Overcoming Cybercrime in Ukraine (Cyberterrorism)

Andrey Pravdiuk[1], Larysa Gerasymenko[2], Olena Tykhonova[3],
a.pravd4449@gmail.com
lora-gera@ukr.net
fin_bezpeka@ukr.net
[1]Vinnytsia National Agrarian University, Vinnytsia, Ukraine
[2,3]National Academy of Internal Affairs, Kyiv, Ukraine

Abstract
Ensuring national security in cyberspace is becoming an increasingly important issue, given the growing number of cybercrimes due to adaptation to new security and protection technologies. The purpose of this article is to study the features of counteracting, preventing, and detecting crimes in the virtual space of Ukraine on the example of cases and analysis of the State Center for Cyber Defense and Countering Cyber Threats CERT-UA and the Cyber Police Department of the National Police of Ukraine. The research methodology is based on the method of analysis and study of cases of crime detection in the virtual environment of the State Center for Cyber Defense and Countering Cyber Threats CERT-UA and the Cyber Police Department of the National Police of Ukraine. The results show that the consistent development of the legal framework in 2016-2020 and the development of a cyber-defense strategy for 2021-2025 had a positive impact on the institution-building and detection of cybercrime in Ukraine. Establishing cooperation with developed countries (USA) has helped to combat cybercrime by facilitating investigations by US law enforcement agencies. This means that international experience is effective for developing countries as a way to quickly understand the threats and risks of cybercrime. In Ukraine, the main number of incidents concerns the distribution of malicious software in the public sector. In the private sector, cyber police are largely confronted with the misappropriation of citizens' income through Internet technology. The practical value of this study is to systematize the experience of overcoming cybercrime on the example of cases of crime detection in a virtual environment.

Key words:
Cybercrime, Cyberspace, Cybersecurity, Crimes in Cyberspace, Cybercrime Detection, Incidents in Cyberspace.

1. Introduction

Ensuring national security in cyberspace is becoming an increasingly important issue, given the growing number of cybercrimes due to adaptation to new security and protection technologies [1]. The development of e-democracy in Ukraine, the growth of the number of Internet users, and the development of information and communication infrastructure exacerbate this problem. The share of individuals using the Internet in Ukraine increased from 23.3% of the population in 2010 to 62.55% in 2018 [2], the number of mobile cellular subscriptions per 100 people - from 118 in 2010 to 130 in the 2019 year [3], the number of fixed-broadband subscriptions - from 6.5 per 100 people in 2010 to 16 units in 2019 [4], the number of secure Internet servers (per 1 million people) – from 12, 36 units per 1 million persons to 8955 units per 1 million persons [5]. The growing level of Internet use by Ukrainian citizens requires the protection of personal data from illegal use, dissemination, destruction, fraud, and crimes of the virtual environment. Overcoming cybercrime concerns both the protection of the population from the threats of the digital world and the provision of national security and protection against cyber-attacks by enterprises. For example, only one in three companies has a cybercrime protection program that poses risks such as loss of funds, reputation, brand strength, business and government relations. In 2016, 24% of companies faced cybercrime, in 2018 - 31% [6]. These trends determine the relevance of the study to combat cybercrime in Ukraine, given the lack of an approved cybersecurity strategy in Ukraine. The purpose of the article is to study the features of counteracting, preventing, and detecting crimes in the virtual space of Ukraine on the example of cases and analysis of the State Center for Cyber Defense and Countering Cyber Threats CERT-UA and the Cyber Police Department of the National Police of Ukraine.

2. Literature review

The scientific literature discusses the causes, risks, threats, policies, and strategies for overcoming cybercrime. The rapid spread of personal data and the low level of digital literacy of the population, the anonymity of the online space are the main factors in the widespread of cybercrime, built on the mechanisms of building user trust [7].

Cybercrime is any illegal computer activity that often occurs on global electronic networks [8]. Gordon & Ford described cybercrime as any crime that facilitates or is committed using a computer, network, or hardware device [9]. The computer device may be an agent, facilitator, or object of crime. Gordon & Ford also classified cybercrime into two types: type I - mostly technological in nature and occurs mainly using software, while type II has a more pronounced human element and usually occurs using programs that do not fall under the classification of

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.24

criminal programs [9]. Types of cybercrime can be considered a set of crimes, some of which are characterized by the use of several technological elements, while others can be committed entirely using Internet technologies [10].

To overcome cybercrime, the scientific literature offers models of machine learning based on information, in particular social networks. This is due to the large amount of data disseminated by users in the process of communication in a virtual environment [11]. Models aim to address cyberbullying [11], spam as a threat to user trust and communication infrastructure [12], identity theft, and sexual exploitation of minors [13].

To combat cybercrime, it is important to harmonize legislation, as well as to establish cross-border cooperation and cooperation with private entities, in particular those that provide Internet services [14]. The development of legislation to combat cyberterrorism is characterized by fragmentation in developing countries due to limited resources [10]. Platforms for monitoring public policy to combat crime in cyberspace are characterized by several practical problems [15]. In addition, the lack of international cooperation, new strategies to combat cybercrime is a challenge for law enforcement agencies due to the ineffectiveness of traditional countermeasures [13]. In developing countries, the institutional factor, the state of international relations, and economic development determine the level of cybercrime [16].

Thus, a review of the literature reveals the many challenges of tackling cybercrime, especially in developing countries. Among the main problems: the need to develop the legal framework, lack of policies and strategies to combat, lack of effective monitoring platforms, limited financial resources (funding does not guarantee overcoming crimes in cyberspace), institutional unpreparedness, lack of international relations and cooperation in this area, rapid growth in the number of Internet users and the growth of personal data in need of protection, insufficient level of protection of the private sector from cybercrime.

3. Methodology

This study uses methods of comparative analysis and synthesis to compare the dynamics of change in overcoming cybercrime in Ukraine. For the analysis we used: 1) indicators of the National Cyber Security Index, which assess the effectiveness of combating crimes in cyberspace for 2018-2021 in various areas: policy, threats, education, global contribution to global cybersecurity, digital protection of digital services, essential, ID & TS (e-identification and trust services), personal, CIRC (Cyber incidents response), crisis, police, military; 2) indicators of activity of bodies of counteraction to cybercrime and examples of incidents, system of identification of incidents in cyberspace, namely the state center of cybersecurity and counteraction to cyberthreats CERT-UA; 3) cases of detecting cybercrime in the private and public sectors of the Cyber Police Department of the National Police of Ukraine, which are classified into: criminal schemes of Internet fraud (online stores, ad websites, delivery services, social networks, fraudulent call centers, hacker forums, phishing, sites), unauthorized real estate transactions of officials, unauthorized interference of Internet providers, creation of a network of special fictitious business entities.

4. Results

In Ukraine, since 2008, the legislative framework for combating cybercrime has been actively developing, and a draft Cyber Security Strategy of Ukraine has been developed. In 2016-2020, the formation and development of the national cybersecurity system took place. To institutionalize the system, the Law of Ukraine “On Basic Principles of Ensuring Cyber Security of Ukraine” of 2018 was adopted, which formed the principles of development of the cybersecurity system and implementation of tasks by crime prevention entities. During this period, the legal support of critical infrastructure is developing, requirements for cyber defense are formed, and cybersecurity centers are established (in the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Ministry of Infrastructure of Ukraine, the National Bank of Ukraine, the Ministry of Defense of Ukraine). In Ukraine, there are secure data processing centers (data centers), the National Telecommunication Network has been developed, the National Center for Reserving State Information Resources has been established, and a system for detecting vulnerabilities and responding to cyber incidents and cyberattacks has been launched. In the period 2021-2025, it is planned to establish a National Coordination Center for Cyber Security to coordinate and unite institutions to combat cybercrime.

Despite the development of the legal framework and institutions, cybercrime remains an important problem in Ukraine. Indicators of the National Cyber Security Index (see Fig. 1) show the following main problems in combating cybercrime in Ukraine: insufficient policy coordination, lack of security strategy in cyberspace, lack of strategic plan implementation, lack of public reports on threats and cybercrime, lack of site security, low level of initial competence and secondary education in the use of the virtual environment, low quality of cybersecurity programs at the bachelor's and master's level, lack of cybersecurity associations, lack of cooperation and participation of Ukraine at the international level, inability to form “Cybersecurity capacity”.

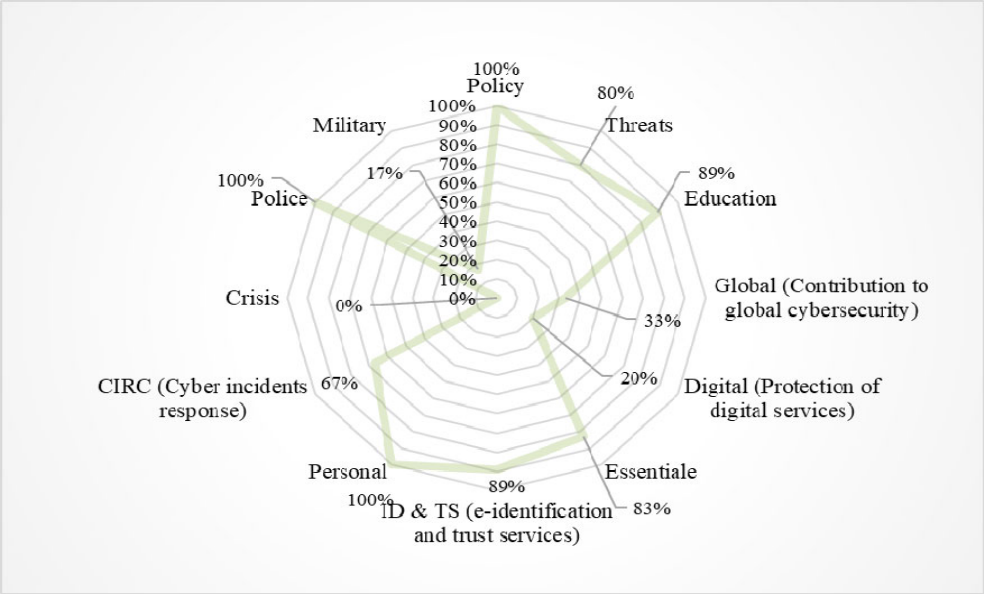

Fig. 1. National Cyber Security Index: general cyber security indicators
Source: National Cyber Security Index [17]

In the field of digital services protection in Ukraine, the following problems are observed: low level of responsibility for the cybersecurity of digital service providers, lack of cybersecurity standards in the public sector, low level of competence of authorities responsible for cybersecurity. In the field of protection of vital services, the following problems have been identified: there is no list of operators of basic digital services, lack of requirements for digital service operators, insufficient level of functioning of competent supervisory authorities, low quality of regular monitoring of security measures. In the field of electronic identification and provision of trust services, problems of permanent identification of a unique nature, lack of requirements for cryptosystems, low quality of electronic identification, and use of electronic digital signature were identified. In the field of personal data protection, the main problem remains the development of legislation. In the area of responding to incidents in cyberspace, there remains a low level of accountability, cybercrime response, and a lack of a single contact point. In the field of cyber crisis management, problems of lack of a crisis response plan, lack of training for crisis management at the national level, low level of participation in international exercises, lack of prompt support of volunteers in case of crisis. In the field of combating cybercrime, the problems of criminalization of cybercrime, low quality of functioning of anti-crime units, and units of digital criminology have been identified. As a result, the National Cyber Security Index in 2018 was 58%, in 2019 - 64%,

Ukraine cooperates with US law enforcement agencies to conduct joint investigations in the field of personal data protection (illegal theft) and other cybercrimes. In Ukraine, according to the OSAC [18] Ukraine 2020 Crime & Safety Report from May 8, 2020, there are several hundred to several thousand cyber-attacks on information portals and government ministries every month. Among the main types of attacks: denial of service (DOS) attacks to prevent connection to the site or server; attacks on critical infrastructure; attacks to worsen publicly available information and service portals for political purposes.

The main actors in combating cybercrime in Ukraine are the government team for responding to computer emergencies, the State Center for Cyber Defense and Countering Cyber Threats CERT-UA, which operates within the State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine and investigates incidents in cyberspace, analyzes vulnerabilities for infrastructure, collects information about threats, monitors the state of infrastructure protection and security [19].

Protection of state information resources within the activities of CERT-UA involves blocking attacks of various kinds, identifying vulnerabilities and responding to incidents, processing cyber incidents. For example, for the period from April 28 to May 4, 2021, the system of secure access of public authorities to the Internet: 42,340 different types of attacks were blocked, which is 23% less than the previous week. The vast majority are application-level network attacks (95%); 5 DDoS attacks were recorded and blocked [20].

The system for detecting vulnerabilities and responding to cyber incidents and cyberattacks at the monitoring facilities recorded 1,067,751 suspicious events (which is 6% more than in the previous week):

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.24

- attempts to obtain user rights - 49%;
- attempts to obtain administrator rights - 21%;
- violations of corporate security policy - 7%;
- suspicious executable code - 11%.

During this period, the government team for responding to computer emergencies in Ukraine CERT-UA registered and processed 2,345 cyber incidents (which is 6% less than the previous week). The vast majority of processed incidents belong to the UACOM domain zone (about 99%). The main number of incidents concerns the distribution of malicious software - 98%, unauthorized access - 1%, phishing - 1% [20]. For example, among the incidents is a large-scale phishing attack on state institutions due to the mass sending of phishing e-mails to the e-mail addresses of state institutions of Ukraine. Another example of incidents is that criminals gain access to specialized software (access to FireEye tools) for use in cyberattacks in Ukraine. This incident poses a major risk to public authorities in critical infrastructure, as the tools contain intelligence automation solutions (simple scripts and large frameworks). To overcome such incidents, CERT-UA uses the following systems: Snort – Open Source Intrusion Prevention System (IPS), YARA – is a tool to assist malware researchers in identifying and classifying malware samples; ClamAV open source antivirus software (GPL).

The Cyber Police Department of the National Police of Ukraine is an interregional territorial body of the National Police of Ukraine, which is part of the criminal police of the National Police and following the legislation of Ukraine, ensures the implementation of state policy in the fight against cybercrime. The Cyber police Department participates in the development and implementation of the state policy of prevention, counteraction, detection, and cessation of criminal violations in the field of cyber defense. Content analysis and analysis of cases of cybercrime detection of the activities of the Department of Cyber police of Ukraine to detect criminal violations shows the following main cybercrimes: Internet fraud through the mechanism of development of online stores, in particular in social networks, to receive income (losses amount to more than 100 thousand UAH); forgery of medical documents and medicines through the interaction of the offender with the use of social networks, websites; mechanism for stealing funds from citizens' bank cards through fraudulent call-centers, hacker forums for purchasing databases of clients of banking institutions using "sip-telephony" technology; mechanism of withdrawal of citizens' funds through phishing sites, which completely copy the design of foreign Internet advertising platforms, and contactless payment systems on phones (the amount of losses is over 1 million UAH); cyberattacks on QNAP devices through a program using a 7-Zip archive to "encrypt" files; sale of counterfeit products through sites of announcements and wholesalers, online stores; unauthorized real estate transactions of officials for the purpose of illegal sale of buildings (changes in the real estate register); illegal sale of enterprise databases by placement on a remote server; creation of phishing resources (fake sites of announcements and delivery services) for misappropriation of means of citizens; unauthorized interference of Internet providers in the work of electronic networks of units of the Joint Forces of Ukraine; creation of a network of special fictitious business entities for conducting non-commodity financial and economic transactions with the involvement of intermediaries for the registration of non-existent enterprises; viral attacks on financial institutions in Europe by modifying malicious software such as encryption viruses, publishing confidential company data when refusing to pay a ransom for decrypting data; misappropriation of incomes of citizens through hacking of social pages on the basis of a method of rough search of passwords (Brute Force attacks).

Thus, in cyberspace, criminals use technology and develop various schemes for misappropriation of income and fraud. The amount of illegally obtained proceeds of crime ranges from 100 thousand UAH to 100 million UAH, depending on the scale of cybercrime. In general, the private sector, in particular citizens, is the least protected subject from cybercrime. The main reason is the low level of digital skills for protection against cybercrime.

Despite several problems in various areas of cybersecurity in Ukraine according to the indicators of the National Cyber Security Index, cases and analysis of the State Center for Cyber Defense and Countering Cyber Threats CERT-UA and the Cyber Police Department of the National Police of Ukraine show rapid development of technologies and systems detection of crimes [17]. It can be expected that the growth of funding for the activities of these bodies and further technological development will provide more effective monitoring to combat cybercrime.

5. Discussion

Legislation in Ukraine regulates a wide range of measures to combat cybercrime, prevent and mitigate the consequences and risks of possible crimes in cyberspace. This practice is common in countries around the world [15]. The measures differ depending on the stated goals, the strategy implementation process, the levels of coercion and the type of interaction between the subjects of overcoming cybercrime and the results. Overcoming cybercrime is difficult to assess in terms of effectiveness, as different types of threats occur at regular intervals in the private, public sectors [15]. Therefore, the policy of counteracting and preventing crimes in Ukraine at the time of writing does not provide the expected results due to the systematic occurrence of crimes. Technical systems for warning and detecting vulnerabilities need to be improved.

Cybersecurity depends on the technique and technology, the competence of the authorities to counter, overcome and detect, regardless of the availability and implementation of the strategy in the country. Ukraine's experience in overcoming crimes in cyberspace shows that in the absence of a state-approved strategy, the activities of CERT-UA and the Cyberpolice Department ensure the detection of crimes. At the same time, the low level of digital literacy and protection of businesses from fraud indicates a number of problems in the field of cyber security. This state of cybersecurity can be explained by the low level of human development, inaccessibility and inability to use IT security products, limited resources to respond to cybercrime due to their complexity and, as a consequence, the above institutional bottlenecks [16]. The result is that emerging economies such as Ukraine become the main points of the fight against cybercrime, as cybercriminals are displaced from industrialized economies with strict control, regulation and cybersecurity measures. Instead, cybercriminals operate in developing countries and, as the results of case studies show, mostly harm citizens in the form of embezzlement.

Cybercrime in Ukraine, as well as in other developing countries, will remain a problem, because the cases of illegal activities of fraudsters indicate various schemes of misappropriation of income, data, and sale of counterfeit goods. These schemes are valid for 1 to 7 years, providing criminals with income from criminal activities in cyberspace. Therefore, the Government of Ukraine should continue to allocate funds to CERT-UA and the Cyberpolice Department to improve their interoperability, improve cybercrime techniques and technologies, instant accountability and disclosure in various data sources to inform citizens and businesses about potentially dangerous cybercrimes. If Dupont argues for the need to develop platforms for monitoring the effectiveness of public policy, then in this article the authors consider the priority of developing the skills of law enforcement and funding technologies to combat cybercrime [15]. These measures, despite the approval of policy measures and strategies for their implementation, are key in this area. The authors of the article also agree with Barclay “Development and implementation of relevant legislation are principal measures in the management of the growing incidence of cybercrime” [10]. Legislative initiatives are the basis for measures to combat crime, but the introduction of data protection technologies, private and public sector information should be considered a fundamental action. An effective legal framework, civil liberties and institutions determine the proper management of cybercrime.

A review of cases of investigation and detection of crimes in general shows that the police are accountable for exposing cybercrimes in the private sector, which involve embezzlement and misappropriation of funds. The level of reports of violations, where the amount of misappropriated funds ranges from 100 thousand UAH to 1 million UAH and more are less common. Thus, many crimes are not reported. This is also the case in India, where a police-recorded version of crime facts can provide only a limited view of the reality of victimization, and police figures are just the tip of the iceberg [16].

For further understanding and deeper understanding of this issue, it is important to consider primary and secondary victimization (the process or end result of becoming a victim of criminal encroachment). Primary victimization occurs when a person becomes a victim of the crime itself. Some mechanisms involved in primary victimization include physical/psychological suffering or financial loss. Instead, secondary victimization occurs through the actions of the victim's social environment. Key mechanisms involved in secondary victimization include stigmatization, social isolation, or obsessive and derogatory surveys [16]. Secondary victimization also occurs due to incorrect and insensitive practices of journalists in collecting or reporting news or improper actions of the criminal justice system [16]. Therefore, the reluctance of law enforcement agencies to promote a high level of cybercrime reporting can be considered secondary victimization in Ukraine, when police inaction in disseminating information about threats of action in the virtual environment leads to cybercrime. Therefore, the criminal justice system in Ukraine does not fulfill all the defined roles, and victims of cybercrime may be further victimized. For example, in some cases of victimization on the Internet (embezzlement through the provision of bank card information) in response to the offender's actions, the victims themselves are more likely to engage in activities that may be considered a crime. In such cases, the police, lawyers, and courts can blame the victim of the online attack.

6. Conclusion

This study systematizes the issue of overcoming cybercrime in Ukraine as a technology emerging country. In Ukraine, since 2008, the legislative framework for combating cybercrime has been actively developing, and a draft Cyber Security Strategy of Ukraine has been developed. In 2016-2020, the formation and development of the national cybersecurity system took place. Despite the development of the legal framework and institutions, cybercrime remains an important problem in Ukraine. Indicators of the National Cyber Security Index (see Fig. 1) show the following main problems in combating cybercrime in Ukraine: insufficient policy coordination, lack of security strategy in cyberspace, lack of implementation of a strategic plan, lack of public reports on threats and cybercrime, lack of site security, low level of competence of primary and secondary education in the

use of the virtual environment, low quality of cybersecurity programs at the bachelor's and master's level, lack of cybersecurity associations, lack of cooperation and participation of Ukraine at the international level, inability to form "Cybersecurity capacity". In cyberspace, criminals use technology and develop various schemes for misappropriation of income and fraud. The amount of illegally obtained proceeds of crime ranges from 100 thousand UAH to 100 million UAH, depending on the scale of cybercrime. In general, the private sector, in particular citizens, is the least protected subject from cybercrime. The main reason is the low level of digital skills for protection against cybercrime. Cases and analysis of the activities of the State Center for Cyber Defense and Countering Cyber Threats CERT-UA and the Cyber Police Department of the National Police of Ukraine show the rapid development of technologies and systems for combating, preventing, and detecting crimes. It can be expected that the growth of funding for the activities of these bodies and further technological development will provide more effective monitoring to combat cybercrime.

References

[1] Eddolls, M. "Making cybercrime prevention the highest priority". Network Security, no. 8, pp. 5-8, 2016.

[2] World Bank. Individuals using the Internet (% of population). https://data.worldbank.org/indicator/IT.NET.USER.ZS?view=chart. accessed Dec. 18. 2020.

[3] World Bank. Mobile cellular subscriptions (per 100 people). https://data.worldbank.org/indicator/IT.CEL.SETS.P2?view=chart. accessed Dec. 08. 2020.

[4] World Bank. Fixed broadband subscriptions (per 100 people). https://data.worldbank.org/indicator/IT.NET.BBND.P2?view=chart. accessed Dec. 28. 2020.

[5] World Bank. Secure Internet servers (per 1 million people). https://data.worldbank.org/indicator/IT.NET.SECR.P6?view=chart. accessed Dec. 19. 2020.

[6] PWC. Global Economic Crime and Fraud Survey 2018: Ukrainian findings. https://www.pwc.com/ua/en/survey/2018/pwc-gecs-2018-eng.pdf. accessed Dec. 18. 2020.

[7] Lusthaus, J. "Trust in the world of cybercrime". Global crime, 13(2), pp. 71-94, 2012. DOI: 10.1080/17440572.2012.674183.

[8] Chang, W., Chung, W., Chen, H., & Chou, S. "An international perspective on fighting cybercrime". In International conference on intelligence and security informatics. pp. 379-384. June 2003. Springer, Berlin, Heidelberg.

[9] Gordon, S., & Ford, R. "On the definition and classification of cybercrime". Journal in Computer Virology, 2(1), pp. 13-20, 2006.

[10] Barclay, C. "Using frugal innovations to support cybercrime legislations in small developing states: introducing the cyber-legislation development and implementation process model (CyberLeg-DPM)". Information Technology for Development, 20(2), pp. 165-195, 2014.

[11] Al-Garadi, M. A., Varathan, K. D., & Ravana, S. D. "Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network". Computers in Human Behavior. 63, pp. 433-443, 2016. DOI: 10.1016/j.chb.2016.05.051.

[12] Wall, D. S. "Digital realism and the governance of spam as cybercrime". European journal on criminal policy and research, 10(4), pp. 309-335, 2004.

[13] Reitano, T., Oerting, T., & Hunter, M. "Innovations in international cooperation to counter cybercrime: The joint cybercrime action taskforce". The European Review of Organised Crime, 2(2), pp. 142-154, 2015.

[14] Borko, A., Nehodchenko, V., Volobuieva, O., Kharaberiush, I., & Lohvynenko, Y. S. "Fighting against cybercrime: problems and prospects in Ukraine and the world". http://dspace.univd.edu.ua/xmlui/handle/123456789/5527. accessed Jan. 08. 2021. (in Ukrainian).

[15] Dupont, B. "Enhancing the effectiveness of cybercrime prevention through policy monitoring". Journal of Crime and Justice, 42(5), pp. 500-515, 2019.

[16] Kshetri, N. "Cybercrime and cybersecurity in India: causes, consequences and implications for the future". Crime, Law and Social Change, 66(3), pp. 313-338, 2016

[17] National Cyber Security Index. https://ncsi.ega.ee/country/ua/?pdfReport=1. accessed Jan. 15. 2021.

[18] OSAC. Regional Security Office at the U.S. Embassy in Kyiv. Ukraine 2020 Crime & Safety Report. https://www.osac.gov/Content/Report/cfdde1cb-f15e-4281-96af-1957c70ec6ec. Jan. 27 2021

[19] CERT-UA. https://cert.gov.ua/about-us. accessed Dec. 23. 2020.

[20] State Service for Special Communications and Information Protection of Ukraine. Protection of state information resources for the period from April 28 to May 4, 2021. https://cip.gov.ua/ua/news/zakhist-derzhavnikh-informaciinikh-resursiv-za-period-z-28-kvitnya-po-4-travnya-2021-roku. accessed Dec. 18. 2020. (in Ukrainian).