CYBER THREAT INTELLIGENCE AS A NEW PHENOMENON: LEGAL ASPECT

Iryna Sopilko
Doctor of Law, Professor, National Aviation University,
1 Lyubomir Guzar Avenue, Kyiv, Ukraine, 03058
https://orcid.org/0000-0002-9594-9280
iryna.sopilko@npp.nau.edu.ua

Abstract. The study gives definitions of cyber threat intelligence and related terms, such as cyber threat, information security, cybersecurity, and others, indicating the purposes, objects, and subjects of the concepts mentioned. The author correspondingly considers the features of the organization of cyber threat intelligence in Ukraine, its types and levels, bodies to operate in the sphere under consideration and identifies their key functions. The studies of Ukrainian and foreign scientists who researched certain aspects of cyber threat intelligence and cybersecurity were analyzed, based on their views practical conclusions were drawn and the conceptual ground of the paper was composed. Separately, the characteristics of the main types of cyber threats in nowadays cyberspace are given, methods for solving the problems arising in this field are introduced, and ways of ensuring the appropriate condition of cybersecurity of the state are marked. Additionally, the concept and features of cyber threat hunting as part of the cyber threat intelligence process were studied as part of the cyber threat intelligence process. Cyber threat intelligence in this scientific research is considered from the point of view of two approaches – as an analytical activity and as an activity of special authorities. Furthermore, the author analyzed the existing regulatory and legal instruments regulating different aspects of the phenomenon under consideration in the USA and Ukraine. The author pointed out the deficiencies of such regulations and provided recommendations for their further improvement. Correspondingly, suggestions are given to develop and improve the national cyber defense system of the country.

Keywords: information security, InfoSec, cyber threat intelligence, cyber threat, cybersecurity, cyberspace

INTRODUCTION

Previously, it was believed that a person can interact in three spaces – air, water, and land. Now there are four such spaces, cybernetic space has been added to the three named. It is in it that modern inhabitants of the Earth spend most of their time. And it is against it that a large number of attacks are directed. According to statistics for the first half of 2020, the number of cyber-attacks increased by 22% compared to the previous six months. Gartner

previously predicted that the global market for data protection software and services from hacking and illegal access will be valued at over $170 billion in 2022 (Cyber threat review 2020: Pandemic result, 2020).

Indeed, the rapid development of information and telecommunication technologies has led to their active implementation in almost every sphere of human life. The World Wide Web, cloud services, and similar systems allow us to transfer various data, hold video conferences, establish connections and build a business in a fraction of the time. This also became the reason for the widespread automation of production and other processes.

We began to be called the information society, that is, one in which there is a free exchange, the production of information, and accordingly we have become much more efficient and successful. However, such digitalization also has quite tangible negative consequences, because the traditional threats to state security have received a new breath and, along with them, completely new challenges and risks appear. Accordingly, under these conditions, the search for new opportunities for ensuring national security in the new cyberspace for us comes to the fore for every state, including Ukraine.

It should be understood that information and communication networks are used everywhere and in various areas of public life, from schools to critical infrastructure facilities. All of these are tidbits for cybercriminals. We should recall that Ukraine has been a victim of aggression by the Russian Federation for 8 years, the enemy is carrying out a hybrid war against our state. Consequently, ensuring the security of information and communication networks responsible for the life support of Ukrainians is very important. In this regard, cybersecurity intelligence is of particular importance.

For Ukraine, the topic of cyber threat intelligence as the basis for ensuring the country's cyber security and its legal regulation is relatively fresh and still little developed. There are few comprehensive studies on this subject matter, but there are considerations of specific categories and issues of cybersecurity in general and cyberthreats in particular.

N.N. Panteleeva and L. Romanovska (2019) analyzed cyber threats in the digital economy, during which the theoretical positions of the understanding of the concept of cybersecurity according to the system and subject-object approach were summarized. Scientists have also identified the multidimensional essence of digital technologies in terms of vulnerability, stability, and capacity to counter cyber threats. V.V. Filinovych (2020) revealed the essence of cyber threats and basic concepts in the field of information and cyber security, paying special attention to the guarantees of the latter as a factor in the information security of a sovereign state. The researcher, among other things, pointed out that various leaks of personal data, violation of the secrecy of correspondence, as well as the provision of distorted or biased information to Ukrainian citizens, is a threat to the entire country. She also notes the need to develop and adopt a special law on information security in Ukraine. L. Belkin and J. Iurynets J. (2021) presented conceptual approaches concerning the implementation of state policy in the field of information security of the Ukrainian state. Also, scholars have proposed effective amendments to the current national legislation. V. L. Buryachok, V. B. Tolubko, and others (2015) paid special attention to cyberspace and cybersecurity as the main components of a new information civilization. They, among other things, indicated the measures of state ensuring the cybersecurity of the national infosphere and counteracting the manifestations

of cybercrime. The problems of introducing new standards of cybernetic and information security in his work were documented by S.L. Gnatyuk (2018).

Furthermore, certain aspects of the legal regulation of ensuring information and cyber security as a field for the manifestation of appropriate threats were studied by such legal scholars as V. Kaletnik (2021), V. Moroz (2021), B. Leonov and S. Lykhova (2021), Yu. Kunev (2021), M. Novikov (2021) and others.

Thus, active opposition to the raid of the Russian Federation against Ukraine should include, among other things, adequate reaction and response to cyberattacks by the aggressor country. It is equally important to recognize the appropriate cyber threats in time and prevent them from transforming into incidents and attacks. That is why it is important to understand how cyber threat intelligence works, who carries it out, and what legal acts regulate such issues. All mentioned will be discussed in this scientific study.

The object of study of this paper is public relations regulated by law that arise in connection with the provision of cyber security and the implementation of cyber threat intelligence functions at its core. The subject matter of the study is cyber threat intelligence as one of the methods for ensuring the cybersecurity of Ukraine.

The purpose of this scientific research is to define the legal basis for the implementation of cybersecurity in general, and cyber threat intelligence in particular, to identify shortcomings in such legal regulation, determine the main actors in its implementation and provide recommendations for improving the current state of affairs in this aspect in connection with the aggression of Russian Federation in course ow hybrid war against Ukraine.

MATERIALS AND METHODS

The methodological basis of this scientific study was the generally recognized criteria of scientific objectivity, as well as general scientific methods of cognition, thanks to which a thorough analysis of cyber threat intelligence was made as a key method for ensuring cyber security in Ukraine. The author of the paper applied a systematic method, because of which it was possible to establish a tie between cyber threats and the national security of the state, as well as between other conceptual phenomena. In the process of working on the scientific research, the formal-logical method was also used to deepen the conceptual base of the study, the historical method was used to periodize the sources of legal regulation of emerging legal relations in the field of cybersecurity and directly carrying out cyber threat intelligence, as well as the method of classification and grouping – to determine subjects of these legal relations, their objects and subject matter.

The methods of analysis and synthesis, as well as synergy, helped the author to achieve the desired results in a comprehensive study of problematic aspects in regulating the direct activities of cyber threat intelligence and cyber security bodies in general. The applied comparative legal method made it possible to clarify the problematic issues of law enforcement in this field and to compare the procedure and features of the implementation of methods for maintaining the cyber security of the state. The author also used the modeling method, which helped her to develop recommendations for improving the current legal support for cyber threat intelligence in Ukraine. The study is based on a detailed breakdown and analysis by the author of Ukrainian regulations, and US legislation on cybersecurity, and cyber threat intelligence.

RESULTS AND DISCUSSION

The problem of cyber threats is more relevant today than ever, especially for the Ukrainian state, whose territory was treacherously invaded by the Russian Federation. That is why intelligence operations in this area have acquired special significance in the light of the hybrid war being waged against Ukraine. The legal aspects of cyber threat intelligence in this regard require particularly close study.

Before proceeding directly to the above, it is important to study and analyze the main terminology used in this research paper. It's worth starting with the concept of a cyber threat or cybersecurity threat. So, according to the University of North Dakota, we are talking about any possible malicious attack to gain illegal access to certain data, damage information, as well as any other violation of digital operations. Most often, such threats are created by hackers, terrorists, crime syndicates, and, as in the case of Ukraine, hostile states (7 types of cyber security threats, n.d.). An even broader definition of cyber threats is provided by the Oxford Dictionary, which indicates that this term should be understood as the possibility of intentionally damaging or disrupting a computer network or computer system. To which K. Brisco declares the need to supplement this definition with attempts to damage and steal data, as well as, as in the case of the University of North Dakota, violations of digital operations (Brisco, 2021).

One of the leaders in the field of cybersecurity, Imperva, defines cybersecurity threats as actions that are committed by entities with malicious intent, and such actions are aimed at stealing data, disrupting the normal functioning of computing systems, or causing damage. And this includes malware, various cyberattacks such as DoS, MitM, and by injection, as well as social engineering. In this case, the source of the problem is usually terrorist groups, hostile countries, as well as individuals such as dissatisfied employees, contractors, and the like (Cyber security threats: Types & sources, n.d.).

As for the regulatory framework, according to the Minimum Security Requirements for Federal Information and Information Systems, adopted by the U.S. Department of Commerce and the National Institute of Standards and Technology, a threat is a circumstance or occasion that, through an information system, can adversely affect the operation of an organization, its employees and assets. Such an undesirable impact may be obtained by an improper person of unauthorized access to information, its disclosure, modification, and destruction. There is also a threat that a particular vulnerability of an information system may subsequently be exploited in another way by attackers (National Institute of Standards and Technology, 2006).

As for the national legislation of Ukraine, according to the Law On the basic principles of cybersecurity in Ukraine No. 2163-VIII of October 5, 2017, namely, clause 6 of Article 1, a cyber threat is comprehended as potentially possible, as well as quite real phenomena, factors, – for which the vital national interests of the state in cybernetic space may suffer, as well as which negatively affect the state of Ukrainian cybersecurity and the cybernetic protection of objects in our country (On the basic principles of cybersecurity in Ukraine, 2021).

Accordingly, as we see the threat in most cases is defined precisely as an opportunity. However, among cybersecurity experts, this concept is more associated with the subject of

implementation, with adversaries whose objective is to gain access to the information and communication system. Also, a threat can be identified by the damage that will result from such a menace, as well as by the tactics used and the strategy for conducting a wrongful act.

As a rule, a malicious actor tries to get confidential data of an individual or an entire organization, he tries to gain access to the financial assets of the victim, or create conditions for the victim's systems to be significantly damaged for other malicious purposes. And if the attack is somewhat "virtual", intangible in nature, but the intent of the cybercriminal is a very real objective to harm and has a potential impact. Accordingly, a cyber attack is not just a nuisance, but a very real threat to both the stability of the system and the lives of people, especially when it comes to information warfare against entire states. Consequently, today the term cyber threat is inextricably linked with the phenomenon of information security and cybersecurity.

It is important to understand what a cyberattack is. In paragraph 4 of Article 1 of the previously mentioned Law of Ukraine on Cybersecurity, this term refers to conscious actions taken in cybernetic space by a malicious entity using electronic communications and other technical or technological devices and means, carried out to violate the information security of data and the system as a whole by infringing their availability, confidentiality, or integrity, as well as gaining access to such objects, creating hindrances in the stable mode of their operation, as well as using such systems and resources to conduct cyberattacks on other objects of cybernetic protection (On the basic principles of cybersecurity in Ukraine, 2021).

The information security mentioned above, in the context of Ukraine, is a state of special protection of the country's information domain, it is thanks to this condition that Ukrainian society, as an integral information subject, can freely develop in terms of information and not worry about the possibility of infringement of its information rights and freedoms on the background of internal and external threats. At the same time, in addition to the societies themselves, the information subjects should also include the state as a whole, in our case – Ukraine, which operates in the information field through the system of state bodies, as well as social and other groups that are entrusted with the functions of ensuring information security and each individually taken Ukrainian. The object composition, in this case, is information and communication systems, critical infrastructure objects, information assets, and, directly, the consciousness of individuals, groups, and society as a whole (Sopilko, 2021).

Cybersecurity, according to paragraph 5 of Law No. 2163-VIII, is the protection of the vital interests of individuals and citizens, Ukrainian society, and Ukraine as a state in the course of operating in cyberspace, and such protection ensures the sustainable development of both the information society (which Ukrainian society is recognized as), and digital communication environment, as well as timely detection, deterrence and neutralization of actual and probable threats to Ukrainian national security in cybernetic space (On the basic principles of cybersecurity in Ukraine, 2021). At the same time, as V. Filinovych remarks, it is not worth equating information security with cybernetic security, since the former aims to ensure the security of information and knowledge in any form, and the latter protects precisely digital information. Cyber security also extends its action to critical infrastructures, networks, cloud platforms, applications, the Internet of things (IoT), and the like (Filinovych,

2020).

Having defined the conceptual apparatus of this scientific research, we should describe the main types of cyber threats in nowadays cyberspace:

- malware – both programs and individual files that can disrupt or otherwise harm a system or digital device. Commonly dealt with such malware as trojans (a program that masquerades as legitimate software that starts a negative impact when turned on), remote access trojans, RATs (they give the offender remote access and administrative control on the system), worms, and viruses (malicious code which "injects" into the system without the knowledge of users), botnets (infect many devices connected to the Network at once), spyware (performs illegal monitoring of actions on the victim's device and collects data about her), ransomware (it encrypts data on the affected device (in the system) and subsequently requires payment for decryption) ;
- domain name system poisoning attacks – with their help, assaulters redirect web users to malicious sites without hacking vulnerable web resources;
- DDoS attacks – they fill servers and networks with Internet traffic to exhaust the resource and system bandwidth;
- formjacking – it inserts malicious JavaScript code into forms for making online payments to steal information from payment cards;
- backdoors – they give attackers remote access to systems or devices (Roy, 2021).

But this list of cyber threats should not be considered exhaustive, as cybercriminals are constantly developing their illegal skills, inventing more and more illicit cyber schemes. Consequently, it is important that the relevant authorities, whose responsibilities include ensuring information and cybersecurity, constantly keep their finger on the pulse and learn about new threats in time to counteract them qualitatively and promptly and identify such problems beforehand. Therefore, we have come to an understanding of the essence of cyber threat intelligence.

Threat intelligence can be considered from the point of view of two approaches – as an analytical activity and as an activity of special authorities.

Concerning the first approach, Cyber Threat Intelligence (CTI) is regarded as the process of gathering, processing, and studying data about opponents in cyberspace. Based on the results of such activities, operational information on cyber threats will subsequently be developed and disseminated. By conducting CTI, responsible persons can sort out a portrait of the enemy, understand his motives, plans, and methods, and, accordingly, develop for themselves a course of action to prevent threats or mitigate their consequences.

Information about cyber threats is necessary for both individuals and enterprises, and the entire state as a whole since this is a matter of national security in Ukraine. For our country, in recent years, the events of 2017 were especially remembered, when the proper functioning of critical infrastructure facilities was seriously affected by the dominance of the Petya virus. Also tangible was the massive attack in February 2022, when as a result of a DDoS attack on the 23rd, the websites of the Verkhovna Rada of Ukraine, the Cabinet of Ministers, the Security Service, the National Police, and the Ministry of Foreign Affairs were downed. Earlier in the month, the websites of Oschadbank and Privatbank, the state's largest financial institutions, and the web resource of the Ministry of Defense were subjected to a

cyberattack (New large-scale cyber attack: Key government sites "laid down" again, 2022).

The detection of such threats, although carried out by the authorities very scrupulously, can be difficult, as previously mentioned, due to the constant improvement of cybercriminals and their methods of work. Therefore, it is important for potential victims to constantly upgrade, improve their analytical and operational security tools, improve the skills of their staff, and increase their resource base to keep up with the changing threat landscape.

As R. Roy notes, cyber threat analytics will allow organizations to extract useful information through the analysis of situational and contextual risks, and then adapt the resulting body of knowledge to a specific threat landscape, even for the entire industry. It is CTI as an extended process that can provide effective cyber threat management and prevent negative consequences during a cyber attack. It also provides situational awareness of the cyber threat landscape, which means that security professionals will be able to anticipate who specifically is interested in attacking their environment. During the implementation of CTI, the history of incidents will be analyzed, based on which an understanding of the internal environment will be derived, and then potential targets for a cyber attack will be determined (Roy, 2021).

In Western countries, the so-called cyber threat hunting has also become famous. It is proactive work – the search for threats that have bypassed the existing cybersecurity solutions in information and communication networks. An interesting feature of this method is the manual collection of potentially dangerous information by the analyst, and its subsequent study using his skills and knowledge, process automation, of course, takes place, but usually only partially. But even in this case, the specialist will use special software to study user and entity behavior analytics, which will help him learn about potential risks in advance. Further, the specialist should study such potential risks by monitoring questionable behavior in networks. Additionally, the analyst also uses machine learning in the process of cyber threat hunting (Kassner, 2016).

Thus, we should not perceive cyber threat intelligence as a predictor of the future, this procedure (process) helps to monitor the events taking place in the world and, based on the knowledge gained, develop an effective action plan to protect the company or organization. For example, businesses often use the results of threat intelligence to prioritize technology investments.

E. Mastaliarchuk points out that when analyzing potential cyber threats, it is important to take into account the so-called "triad of actors" – that is, their intentions and capabilities, taking into account tactics, techniques, and procedures (TTP), their motivation, and level of access to objectives set for themselves. Therefore, the scientist proposes a model for constructing a pyramid of cyber threat analysis levels, consisting of the following levels:

1. Operational. This type of intelligence evaluates specific potential cyber incidents and provides data that can navigate and support response processes. This level involves the use of highly specialized, technically focused intelligence to direct and support the response to specific cyber incidents.
2. Tactical. It involves event evaluation as well as real-time investigations and is the basis for day-to-day operational support.
3. Strategic. This level is the highest, here it is supposed to evaluate heterogeneous

fragments of information to form integrated ideas. At this level, the processed information will be transferred to those who are responsible for making decisions. It is this level that provides a timely warning about threats, since based on the analysis of the cyber threat strategy, an opinion is created about the intentions and capabilities of destructive cyber threats, including participants, tools, goals, tactics – and all this is done by identifying tendencies and patterns, identifying new risks. Thus, work will be carried out on the lead (Mastaliarchuk, 2021, p. 107).

Among cyber threat intelligence platforms, IBM X-Force Exchange, Anomali ThreatStream, and Palo Alto Networks AutoFocus have gained particular popularity and recognition.

In the United States, as the nation with the highest standards and level of cybersecurity enforcement, CTI is addressed in the Cybersecurity Information Sharing Act of 2015. Its norms have encouraged the sharing of cyber threat intelligence data between government institutions and private organizations. The regulation charged the federal government of the state to contribute in every possible way to achieve the 4 goals of CTI in the form of data exchange on threats of varying degrees of secrecy with state governments, tribal and local governments, private entities, the public, other organizations at risk of cybersecurity, with small businesses (To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes., 2015). A year later, the National Institute of Standards and Technology (also known as NIST) released the NIST SP 800-150 standard, which also advocated the benefits of sharing cyberthreat data.

As for Ukraine, there is no separate document on cyber threat intelligence, but a detailed provision of cybersecurity aspects in the country is regulated by the above-mentioned Law On the basic principles of cybersecurity in Ukraine No. 2163-VIII (2017). Also, many related issues are considered in the following Ukrainian regulatory documents:

- Constitution (1996);
- laws: "On the National Security of Ukraine" 2469-VIII (2018), "On Information" No. 2657-XII (1992), "On Electronic Communications 1089-IX (2020), "On the Protection of Information in Information and Communication Systems" No. 80 /94-BP (1994) and others;
- Convention on Cybercrime (ratified by Ukraine by the Law N 2824-IV (2824-15) dated 07.09.2005) and other international treaties binding per the decision of the Verkhovna Rada;
- Decrees of the President, including No. 447/2021 on the entry into force of the decision of the National Security and Defense Council dated May 14, 2021 "On the Cyber Security Strategy of Ukraine" and the approval of the updated version of such a Strategy;
- acts of the Cabinet of Ministers and other documents in force.

Now it is worth talking about the subjects in the system of state bodies of Ukraine responsible for conducting intelligence on cyber threats. Thus, the Computer Emergency Response Team of Ukraine (also CERT-UA) appeared back in 2007 and is a specialized structural unit of the State Cyber Defense Center of the State Service for Special Communications and Information Protection of Ukraine. The functioning of this state structure is provided for by the Ukrainian laws "On the State Service for Special Communications and Information Protection", "On Telecommunications" and the law on cybersecurity.

The responsibilities of CERT-UA include, among other things:

- accumulation and breakdown of data on cyber incidents and maintenance of an appropriate register;
- development and publication on its official web resource of a set of suggestions for countering cyber threats and attacks;
- practical assistance in detecting and leveling the results of incidents for owners of cyber protection objects;
- educational activities on cyber defense issues for subjects of the national cyber security system;
- interaction with law enforcement agencies, foreign partners, Ukrainian response teams on the issues of reacting to cyber incidents;
- receiving data from Ukrainians about cyber incidents and their subsequent processing, and the like (CERT-UA, n.d.).

The Cyber Police (Cyber Police Department of the National Police) also operates in our state and its duties include ensuring the implementation of state policy in the field of combating cybercrime. This department also manages and carries out operational-search activities. Its main specialization is the deterrence, detection, suppression, and exposure of crimes, whose preparation and commission take place using telecommunication and computer systems, networks, and computer equipment. The tasks of the body are, among other things:

- implementation of state policy in the field of combating cybercrime with the obligatory informing of the people about the appearance of their newest examples;
- combating cybercrime concerning payment systems, e-commerce and economic activity, intellectual property, and directly information security;
- implementation of programs for systematization and study of data on threats, incidents, and offenses in the cyber environment;
- participation in international operations to identify these threats and counter such attacks, as well as real-time cooperation, and the like (Shevchuk, 2019, p. 247-248).

The above-mentioned State Service for Special Communications and Information Protection replaced the Department of Special Telecommunication Systems and Information Protection of the Ukrainian Security Service. Now it is a specialized body of the central executive power in the field of special communications and information security. Also, the State Service for Special Communications is an important body in the defense sector and the main subject of the national cybersecurity system. Its tasks, among other things, include the coordination of activities of other subjects of cybersecurity.

Thus, we can say that the system of cybersecurity and cyber threat intelligence in Ukraine is organized at a fairly high level.

CONCLUSIONS

In the modern world, the number of threats associated with the use of information and communication networks, modern technologies, and digital devices is constantly growing. That is why both individual organizations and entire states use cyber threat intelligence. Such a process plays an important role in countering cyberattacks, which is especially important for the Ukrainian state in light of the hybrid war being waged against it by the Russian Federation. Cyber threat analysis activities are an effective way not only to identify probable risks but also to remove real and potential cyber threats to our country. It is also

a method of forming an enemy profile, and understanding its purposes, tactics, applied procedures, and tools. With the exact picture in front of their eyes and a knowledge of what to expect from the aggressor, the Ukrainian security services can not only detect attacks but also develop effective, timely, and most appropriate response measures.

The legal regulation of relevant issues for Ukraine comprises several legislative acts, including a special Law on Cyber Security, as well as international conventions, presidential decrees, decisions of the National Security and Defense Council, the Cyber Security Strategy, and other documents. As for the organization of conducting reconnaissance of cyber threats, to one extent or another, these functions are assigned to the State Special Communications Service, the Cyber Police, CERT-UA, the National Security and Defense Council, and the Ministry of Defense, as well as other bodies and organizations. In the light of the war waged by the aggressor country of the Russian Federation against Ukraine, the National Security and Defense Council started talking about the need to create special Ukrainian cyber troops (cyber army), because of the objective reality where the national security of the country equally depend on this.

President of Ukraine V. Zelensky signed a decree on the creation of cyber troops in August 2021. The purpose of this formation is to timely and efficiently respond to threats in cyberspace. Cyber troops creation has many advantages, including tangible savings in state funds, because it will require much fewer people than to form a classic army.

Similar troops have already been created and are operating as part of the German Armed Forces, this is the Cyber and Information Domain Service. In the UK, the National Cyber Force and the National Cyber Security Center function, which carry out offensive operations and cyber defense (respectively).

Consequently, cyber threat intelligence is an important process that will allow taking proactive measures to improve management, reduce risks and realize the cyber defense capabilities of the state and its institutions, as well as private companies. That is why the actions of the relevant authorities must be properly regulated at the legal and also technical levels. After all, relying on a trustworthy cyber threat management structure and the relevant authorized bodies conducting cyber threat analytics, Ukraine will receive important strategic and tactical information that will help prevent and detect potential and real threats and risks.

We also note that, in our opinion, the following should be considered the most promising areas for the development of the national cyber defense system:

- improvement of the legal regulation of the specialization of cyber protection of critical infrastructure objects with the obligatory conduct of an independent audit of information security;
- creation and development of industry-specific centers for responding to cyber incidents;
- development of both local and international cooperation in the relevant field;
- implementation of special training in the field of cybersecurity;
- educating the population and assisting to increase its digital literacy, because even a single individual can affect the system as a whole.

Following these recommendations, as well as active law-making and law enforcement activities will help our state reach a qualitatively new level in ensuring the cyber defense of

the entire Ukrainian society.

REFERENCES

7 types of cyber security threats. (n.d.). University of North Dakota retrieved from: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

Brisco, K. (2021). Cyber threat basics, types of threats, intelligence & best practices. Secureworks: Cybersecurity Leader, Proven Threat Defense. Retrieved from: https://www.secureworks.com/blog/cyber-threat-basics

CERT-UA. (2022). Retrieved from:. https://cert.gov.ua/about-us

Cyber security threats: Types & sources. (2022). Learning Center. Retrieved from: https://www.imperva.com/learn/application-security/cyber-security-threats/

Cyber threat review 2020: Pandemic result. (2020). TechExpert. Retrieved from: https://techexpert.ua/ru/cybersecurity-covid/

Filinovych, V. (2020). Cybersecurity guarantees as a factor of state information security. In Problems Of Implementation Of State Policy In The Field Of Information Security Of Ukraine. Kyiv: Accent Graphics Communications & Publishing.

Kassner, M. (2016). Cyber threat hunting: How this vulnerability detection strategy gives analysts an edge. TechRepublic. Retrieved from: https://www.techrepublic.com/article/cyber-threat-hunting-why-this-active-strategy-gives-analysts-an-edge/

Mastaliarchuk, E. (2021). Cyber threat intelligence systems today. In X International Scientific And Practical Conference Of Young Scientists And Students “Current Tasks Of Modern Technologies” pp. 107–108, Kyiv.

National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems (FIPS PUB 200). Retrieved from: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf

New large-scale cyber attack: Key government sites “laid down” again. (2022). BBC News Ukraine. Retrieved from: https://www.bbc.com/ukrainian/news-60497679

On the basic principles of cybersecurity in Ukraine, Law of Ukraine No. 2163-VIII (2021) Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Roy, R. (2021). What is a cyber threat? Definition, types, hunting, best practices, and examples. Toolbox. Retrieved from: https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-cyber-threat/

Shevchuk, G. (2019). Peculiarities of activities of the cyber police department of the national police of Ukraine. Scientific Bulletin of Public and Private Law, 1(3), 244–249. Retrieved from: http://nvppp.in.ua/vip/2019/3/tom_1/44.pdf

Sopilko, I. (2021). Information security as an object of regulation in the law of Ukraine. Journal of International Legal Communication, 1, 11–22. https://doi.org/10.32612/uw.27201643.2021.1(1).pp.11-22

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes., Bill No. S.754 (2015) (USA). Retrieved from: https://www.congress.gov/bill/114th-congress/senate-bill/754