

Development of the Concept of Cybersecurity of the Organization

Anatolii A. Loishyn, Spartak Hohoniants, Mykola Ya.Tkach,
Maksym H. Tyshchenko, Nataliya M. Tarasenko, Volodymyr S. Kyvliuk

The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

Abstract - The article is of interest to managers and scientists at all levels who deal with combating cyber threats. The study analyzed the security environment and confirmed the rapid growth of malware and cyberattacks. The stages of development of cybercrime are analyzed, and the most significant cyberattacks that have taken place in recent years are identified. Statistics on the number of cyberattacks and their devastating impact on economies are presented. A brief description of the available types of malware and the algorithm of unauthorised entry of cyber attackers into the system is given. The article offers a variant of developing the concept of cybersecurity, defines the range of participants in ensuring the organisation's cybersecurity, and formulates an algorithm for its development and operation.

Keywords – Cybersecurity, Cyberattacks, Cybercrime, Concept of Cybersecurity.

1. Introduction

Today, security in information and cyberspace is becoming increasingly important. There is a rapid trend towards the digitalization of all spheres of human activity.

DOI: 10.18421/TEM103-57

<https://doi.org/10.18421/TEM103-57>

Corresponding author: Anatolii Loishyn,
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Ukraine.


Email: aloishyn@gmail.com

Received: 21 February 2021.

Revised: 12 August 2021.

Accepted: 17 August 2021.

Published: 27 August 2021.

 © 2021 Anatolii Loishyn et al; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at www.temjournal.com

Analysis of trends in science and technology shows the growing dependence of man on digital tools, organizations on databases in networks, banking on digital payments, countries on the management of weapons of strategic importance through computer technology and software.

Every day, groups of experienced cybercriminals seize control of other people's computers and gadgets of all forms of ownership; launch a series of destructive programs against sites. In a matter of seconds, ATMs, companies, telephone lines, and even the presidential sites of the world's powers cease to function. There is a tendency in the world to increase attention to cybersecurity and information resource management.

No one could have predicted that the financial crisis in 2007-2008, which began with the US mortgage crisis, bank failures, and falling stock prices, would lead to a global economic crisis (sometimes called the "Great Recession") [1].

Next, humanity faced an infectious disease that was first detected in humans in December 2019 in China [2]. The disease began as an outbreak that developed into a pandemic. The cause of the disease was the coronavirus SARS-CoV-2 [3], [4]. The disease has dealt a devastating blow not only to human health but to the global economy as a whole.

1.1. Novelty of Research

The disease forced a significant part of the world's population to consider the issue of remote work, educational institutions switched to distance learning, a large number of online conferences, meetings, and business meetings are held every day. This undoubtedly stimulated the trend towards expanding the scope of digital technologies.

Given the above, the financial crisis and infectious diseases like the "black swans" could not have been foreseen in advance to develop appropriate countermeasures [5]. Therefore, one should not deny the possibility of a catastrophic world-class cyberattacks that may take place in the future. Today it is impossible to predict what social, economic, and

political consequences the world will face if the Internet stops even for a day.

Thus, it should be noted that our personal and corporate computer networks and digital processes have to be reliably protected. The actualization of the research topic is confirmed by the need to counter cyberattacks, study them, and analyze the development of the prerequisites for their occurrence and possible countermeasures technologies.

1.2. Setting Objective

The purpose of the article is to develop a variant of the cybersecurity concept for an organization.

1.3. Methodology

To achieve the purpose defined in the study, its decomposition was carried out. So, within the target, the following tasks were performed:

1) It is a description of the security environment (brief statistics of the background of the study, determination of prerequisites for the development of cybercrime, analysis of the largest cyberattacks in the world, statistics on the number of cyberattacks and predicted losses from them, classification of types of cyber threats).

The scientific knowledge methods were used to solve the problem: a systematic approach with careful consideration of environmental safety, analysis in determining the numerical indicators used in the study, synthesis - a combination (grouping) of elements (arrows) of the study.

2) Development of a variant within the concept of cyber defense of the organization (determination of the prerequisites for developing a concept, determining the circle of participants in the development and implementation of the concept, determining the algorithm for developing and implementing the concept).

To solve the set partial task, the methods of scientific knowledge were used: a systematic approach - in describing the functioning of the organization's cyber defense system, analysis and synthesis - in determining the elements of the concept, their grouping, and the like.

2. Results

2.1 The general trend towards an increase in the number of cyber threats, in turn, leads to a sharp increase in the costs of business and government agencies for data protection. So, according to forecasts by Cybersecurity Ventures, over the next four years, global spending on cybersecurity will amount to about \$ 1 trillion. However, the damage from cybercrime will also increase significantly [6].

So, in 2015, the cost of reimbursing global damage for attacks using ransomware amounted to \$ 325 million. In 2017, according to preliminary estimates, these costs will exceed \$ 5 billion, and by 2021 the figure will exceed the \$ 6 trillion bar. Global cybercrime spending is expected to grow by 15 per cent per year, reaching 10.5 billion by 2025. Combined, this exceeds the damage caused by natural disasters per year and will be more profitable than the global illicit drugs trade together [7].

When comparing computer viruses and biological viruses, we will find many similarities. As a rule, the disease causes a runny nose in a person, and along with a runny nose comes sneezing, the particles of which, falling on another person, can infect him. Cybercriminals use a similar technique, and it is called "spam". By sending thousands of infected emails, they infect many computers. The flu virus has mutated since it uses the body of an infected person to spread the virus. It is also not enough for a computer virus to infect only one computer; it tends to spread over a large area. Severe virus attacks can kill a computer or damage the system very badly, just like biological viruses. Many viruses can remain in the body of an infected person for a long time, up to several weeks until he finds out that he is sick.

Furthermore, during such an incubation period, a person can infect other people. The same goes for computer viruses. Computer viruses can go unnoticed until a hacker works remotely and launches them.

Additionally, the number of cyber extortion (ransomware) cases is proliferating [8]. Ransomware is defined as malicious software that blocks users' access to their devices or blocks access to files until an amount of money or a ransom is paid. Ransomware causes downtime, data loss, the potential for theft of intellectual property, and in some industries, the attack is considered a data breach. From 1989 to the present, this type of cyberattack has a general upward trend. In 1989, the first-ever ransomware virus was created that was transmitted on floppy disks. The drives contained malicious code that hid file directories, blocked filenames, and required victims to send \$ 189 to Panama if they wanted their data back. This case was the impetus for the development of this type of threat. Cyber extortion is a significant problem today. It is predicted that in 2021 there will be an attack with organization requirements every 11 seconds, up from every 40 seconds in 2016 [9].

To confirm the importance of research, one should stop and give examples of the largest cyberattacks that have taken place over the past years (Table 1).

Table 1. Known cyberattacks were carried out between 1999 and 2020.

Year	Ref.	The purpose of the attack	Brief description
1999	[10]	International Space Station	The teenager hacked the NASA server.
1999	[11], [12]	Infection of computers based on Windows operating systems	A virus has been created that infects Windows computers (Melissa). The virus modified critical files causing the system to crash. Approximately 20% of computers running Windows were infected.
2007	[13]	Hacker attack on Estonia	Cybercriminals create groups and carry out attacks across the country.
2010	[14]	Attack on Iran's nuclear program	Infected equipment at manufacturers' factories got into a protected system.
2011	[15]	Hacking Sony PlayStation Client Database	The Lulzsec hacker group hacked into the player database.
2013	[16], [17], [18]	Attack on Spamhaus	The largest DDOS attack in the history of the Internet. The blow was so powerful that it slowed down the entire Internet on the planet, in some countries it led to a network outage for several hours.
2014	[19]	Mt.Gox exchange hacked by hackers	\$ 470 Million Crypto Coins Stolen
2014	[20]	Hackers hacked digital protection of US military bases.	Blueprints for 20 of the latest weapon systems have been stolen.
2017	[21], [22]	"Petya" virus attack on computer systems in Ukraine	Government sites and businesses, banks, institutions, media and private sites were affected.
2018	[23]	Hacking Brazilian Ministry of Defense Server	The damage was not disclosed.
2020	[24]	Hack Nintendo	Cybercriminals gained access to Nintendo Network IDs (NNIDs). The attack affected 300,000 people.

Analysis of the information presented in the table (Table 1) allows us to trace a clear trend - hacker methods are increasingly modelling the corporate hierarchy. Cybercriminals unite in online communities (such as Red Hacker Alliance [25], Anonymous [26] Red Hack [27], which allows them to attack objects together. As indicated in the table, the target of cyberattacks can be: government organizations, commercial organizations, banking institutions, private accounts and accounts. The profile and methods of activity of hacker attacks can have not only economic goals, but also political ones, which in turn equates cybercriminals with cyberterrorists.

It is can also cite the following facts analyzing the targeted use of cyber weapons in international and domestic politics. One of the first large-scale applications of cyber weapons occurred in Iran in 2009-2010. Unlike common malware running on popular operating systems, the Stuxnet virus used against Iran was explicitly designed to infiltrate industrial computers. This virus paralyzed Iran's nuclear program, due to which the production of uranium in this country was reduced by 20%. As a result of several disclosures and information leaks, it can be argued that specialists developed this virus from the United States and Israel [28].

Analyses of the activities of organized cybercrime require defining the main significant events that accompanied its origin and development (Table 2).

Table 2. The activities of organized cybercrime require defining the main significant events that accompanied its origin and development

Period	The content of the event
1960s	The first computer hackers were from the Massachusetts Institute of Technology (USA). Some members of the group used the new university computers for their purposes to manipulate programs [29].
1970s	Hacking local and international phone networks to make calls for free
1980s	Hacker groups began to form. The first was Legion of Doom in the US and Chaos Computer Club in Germany.
1983	The first film about hackers "War Games"
1984	Publishing of the hacker magazine "2600".
1986	For the first time in its history, the US Congress passed the Computer Fraud and Abuse Act, making computer hacking a crime [30].
1988	A self-replicating program called the Morris Worm disabled about 6,000 university and government computers across America, causing massive damage estimated at about \$ 96.5 million [31].
1993	The famous NCSA Mosaic web browser appeared.

The subjects of the commission of computer crimes can be both internal users (persons who are in labour relations with the enterprise where the crime was committed) and external users (persons who are not in labour relations with the enterprise where the crime was committed). The generalized data of forensic practice show that internal users commit 94% of crimes, while external users - only 6%, while 70% are users of the computer system, and 24% are service personnel [32].

The number of cyberattacks is growing every day due to the rapid scientific and technological progress of digital technologies and an increase in the proportion of remote execution of tasks due to the world's problematic epidemiological situation. Experts estimate a 600% rise in cybercrime due to COVID-19. Figure 1 depicts how the total number of computer malware infections has increased in recent years [33], [34]. Unfortunately, accurate data on the number of cyberattacks in 2019 and 2020 in 2020 Cyber Security Statistics (the Ultimate List of Stats, Data & Trends), is not listed.

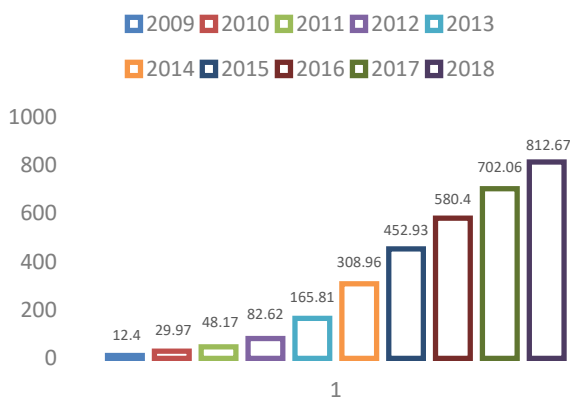


Figure 1. Total malware infection Grows Rare (in Millions).

To understand the information presented, it is necessary to bring the general structure of cyber threats, which currently occur (Table 3).

Table 3. The general structure of cyber threats.

<i>trojan software</i>	Malicious software performs unauthorized destruction of files of both system and regular applications.
<i>computer viruses</i>	Programs inject malicious instructions into any user software.
<i>worms</i>	A malicious code uses network resources during its distribution.
<i>spyware</i>	Programs unauthorized and purposefully collects information about the user.
<i>phishing attack</i>	It is a type of social engineering in which data is "fished out" from the user.
<i>rootkits</i>	It is utilities used to mask suspicious

	activity on the user's device.
<i>ransomware programs</i>	Software when it enters the device of an ordinary user encrypts files valuable to him.
<i>cryptojacking</i>	Programs begin to exploit the resources of his computer for mining cryptocurrency.
<i>hoax- programs</i>	Software that forces the user to buy another product by deception.
<i>spam</i>	Unsolicited correspondence.

The presence of the threats indicated in the table allows us to state that it is possible to satisfy any unlawful needs with the help of cyberattacks by stealing (transferring) funds, obtaining various information, blackmail, disclosing personal information, hacking and appropriating accounts and accounts.

In our opinion, when the world is in a problematic epidemiological situation, the demand for the opportunity to work remotely has increased. Employees of organizations receive office computers, or remote access to perform the necessary work remotely, conduct online conferences, exchange service information. Remote work outside the office, especially at a computer that is not reliably protected, leads to the ingress of harmful software products into the corporate system due to disruption of the functioning of service information in the general system of the organization.

In order to access the information system of any organization, a cybercriminal has to perform several interrelated steps (steps), which are:

- 1) Collecting information about the object of the cyberattack;
- 2) Identification of weaknesses in defence;
- 3) The choice of cyberattack tools;
- 4) Infiltration of malicious content into the system;
- 5) Unauthorized entry into the system;
- 6) Deployment of covert criminal activity;
- 7) Software control and management;
- 8) Achieving a specific criminal goal;
- 9) Destruction of the facts of presence.

In our opinion, one of the most vulnerable places for a cyberattack in the protection of any system is e-mail boxes, software applications, and automated telephone exchanges. Mailboxes are the input and output channels for the circulation of all information both within and outside the organization. This vulnerability needs to be neutralized by clearly separating the ways of communication between staff within the organization and obtaining information from external consumers. Many modern services combine internal and external document management to organize the circulation of information within the organization in the software market. In general, it is necessary to consider creating a gateway in the

organization, which will accumulate incoming documents to the address of the organization, and after careful inspection to be delivered to the structural units for internal use.

All of the above confirms the need to implement appropriate tools to counter threats in cyberspace. Every organization needs to build an appropriate system to counter cyberattacks.

The study's result is the development of the author's version of building a system of concepts within cybersecurity of the organization with the development of an appropriate concept. This concept aims to a holistic perception of cyber threats by management and staff, and it develops an appropriate model of how the system protection works. The concept covers all processes in the organization to prevent cyber threats.

The primary purpose of the concept is to minimize internal and external cyber threats, including:

1) Internal threats: information leakage, malware distribution, unauthorized access, and conflict of interest.

2) External threats: intelligence of competitors, unauthorized access of external users, theft of information, distortion of information, blackmail (extortion), and financial fraud.

It should be noted that the list of external and internal threats is much broader and identified threats can have both internal and external features (characteristics).

The starting point in the development of the concept is the study of institution's security department and prerequisites for its construction. As of today, the prerequisites for building a reliable system to combat cyber threats are:

- 1) The general tendency to increase cyberattacks;
- 2) Infiltration into the malware system;
- 3) Rapid development of digital technologies;
- 4) The use of electronic document management in the organization;
- 5) Increasing the complexity of data processing;
- 6) Increasing the requirements of national and international legislation to combat cyber threats.

Also, the prerequisites for the development of the concept should include proposals from other departments of the institution:

Compliance unit – on the compliance of the organization's cybersecurity system with the relevant legislation, requirements of international (domestic) standards (if necessary);

Internal control unit – on identified risks in cybersecurity and the need to develop appropriate countermeasures.

Next, the security unit analyzes the security environment and analyzes external and internal

factors that affect the institution's security system. The result of this work is a draft concept of cybersecurity of the organization, which includes some interrelated elements:

- 1) Description of the security environment;
- 2) Purpose, goals of the concept;
- 3) Participants and powers;
- 4) Resource provision;
- 5) Contractors (suppliers);
- 6) Instructions (instructions for managers; instructions for employees; action protocols; schedule of circulation of documents and information, external and internal).

It should be added that the stated goals and objectives set out in the concept should correspond to the abbreviation widely used in management and project management - SMART (Specific, Measurable, Attainable, Realistic, Time related).

The draft Concept is submitted to the organization's management to ensure the implementation of the security policy function in cybersecurity.

Moreover, the implementation of the policy including comprehensive support of the organization considers the need for appropriate resources and technical means necessary for the implementation of measures to combat cyber threats.

It is necessary to pay attention to the compliance department's activities, which within the implementation of the tasks checks compliance with the law and determines the required level of implementation of requirements in the organization, including compliance with technical requirements for equipment and information protection. These requirements are summarized and submitted to the technical support department to consider the requirements during the draft technical support plan's preparation for the partial implementation of the organization's support policy. The technical support department also provides proposals, if necessary, on the feasibility of attracting external support - IT audit, the need for software maintenance, the name of suppliers of machinery and services, the involvement of other services and equipment necessary for the organization's smooth operation. These tasks have to be performed under the security department's close supervision, as the main body responsible for organizing access and the need to provide it to the organization's systems to both employees and external users.

The primary basis for implementing the above approaches to the organization's cybersecurity is primarily the need to isolate information flows within the processes that take place in the organization. It is achieved by ensuring the circulation of official information only through secure channels in the mandatory absence of employees' possibility to use third-party media. It is also essential to determine the level of access to each employee of the organization. All incoming or outgoing information has to be passed through appropriate security gateways. At the

same time, attention should be paid to the security of the organization's automated telephone exchanges as dangerous sources of cyber threats. Control measures should cover the issues of comprehensive protection of e-mail, channels of connection to the corporate network, and employees' interaction with the Internet.

The general approach to the development and location of the proposed concept of cybersecurity of the organization is shown in the Figure 2.

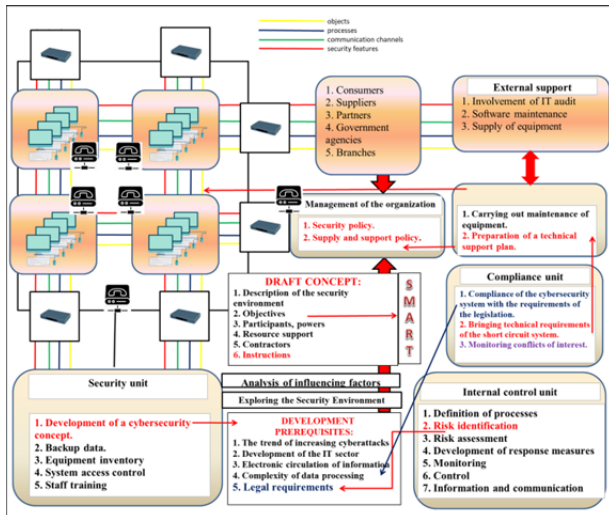


Figure 2. The general approach to the development and location of the proposed concept of cybersecurity of the organization

3. Conclusion

Thus, the study highlights the author's team's results in developing the concept of cybersecurity of the organization. We emphasize that this approach does not override the best cybersecurity practices, but tries to supplement and expand them, taking into account the rapid development of IT technologies and threats.

Given the above, it should be noted that any protection concept may not justify itself almost without the proper perception of its requirements by managers and employees at all levels. Information protection and corporate resistance to information leakage and fraud in all its forms is the key to success and effective functioning of any organization, regardless of type and form of ownership. Only the education of integrity, strengthening corporate ties, instilling respect for the organization in which personnel work, its leadership, and the organization's mission will inevitably be the key to success in combating threats in cyberspace.

Prospects for further research are seen in the practical implementation of the proposed concept with subsequent evaluation of the cybersecurity system's effectiveness and compare it with previous periods.

References

- [1]. Jordà, Ò., Schularick, M., & Taylor, A. M. (2016). The great mortgaging: housing finance, crises and business cycles. *Economic policy*, 31(85), 107-152.
- [2]. Zhao, J. Y., Yan, J. Y., & Qu, J. M. (2020). Interpretations of "diagnosis and treatment protocol for novel coronavirus pneumonia (trial version 7)". *Chinese medical journal*, 133(11), 1347
- [3]. Zhou, H., Chen, X., Hu, T., Li, J., Song, H., Liu, Y., ... & Shi, W. (2020). A novel bat coronavirus closely related to SARS-CoV-2 contains natural insertions at the S1/S2 cleavage site of the spike protein. *Current biology*, 30(11), 2196-2203.
- [4]. Wu, C., Liu, Y., Yang, Y., Zhang, P., Zhong, W., Wang, Y., ... & Li, H. (2020). Analysis of therapeutic targets for SARS-CoV-2 and discovery of potential drugs by computational methods. *Acta Pharmaceutica Sinica B*, 10(5), 766-788.
- [5]. Aven, T. (2013). On the meaning of a black swan in a risk context. *Safety science*, 57, 44-51.
- [6]. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.
- [7]. Morgan, S. (2020). Cybercrime to cost the world \$10.5 Trillion annually by 2025. *Cybercrime Magazine*, 13.
- [8]. Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10.
- [9]. Beard J. (2021, January 21). *Analyze Attacker Behavior, Endpoint Detection Anomalies with Log Rhythm and Carbon Black*. Muck Rack. Retrieved from: <https://logrhythm.com/analyze-attacker-behavior-endpoint-detection-anomalies-with-logrhythm-and-carbon-black/> [accessed: 07 January 2021].
- [10]. Kharin, V.V., & Plotnikova, T.V. (2018). Cybercrime as a threat to international security. *Actual problems of state and law*, 2(8), 96-107.
- [11]. Ahmad, W. (2010). Computer Viruses as a Threat to Home Users. *Int. J. Electr. Comput. Sci. IJECS-IJENS*, 10(3), 29-34.
- [12]. Gil'metdinov, A. D. (2017). Istoriya komp'yuternykh virusov. *Alleya nauki*, 2(9), 871-873. [In Russian].
- [13]. Dunham, K., & Melnick, J. (2008). *Malicious bots: an inside look into the cyber-criminal underground of the internet*. Auerbach Publications. Retrieved January 15, 2020, from <https://doi.org/10.1201/9781420069068>.
- [14]. Romashkina, N. P., & Makhukova, A. V. (2013). Komp'yuternaya vredonosnaya ataka na yademuyu programmu Irana. *Informatsionnyye voyny*, 4, 88-98. [In Russian].
- [15]. Pendergrass, S. & Morris R. (2012). Hackers gone wild: the 2011 spring break of Lulzsec. *Issues in Information Systems*, 13(1), 133-143.

- [16]. Wong, F., & Tan, C. X. (2014). A survey of trends in massive DDoS attacks and cloud-based mitigations. *International Journal of Network Security & Its Applications*, 6(3), 57.
- [17]. Prince, M. (2013). The ddos that knocked spamhaus offline (and how we mitigated it). *Mar, 20*, 06. Retrieved from: <https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-how/>. [accessed: 05 February 2021].
- [18]. van Heerden, R., Leenen, L., & Irwin, B. (2013, November). Automated classification of computer network attacks. In *2013 International Conference on Adaptive Science and Technology* (pp. 1-7). IEEE.
- [19]. Liu, Y., & Tsyvinski, A. (2021). Risks and returns of cryptocurrency. *The Review of Financial Studies*, 34(6), 2689-2727.
- [20]. Harris, S. (2014). *@ War: The rise of the military-internet complex*. Houghton Mifflin Harcourt.
- [21]. Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017, December). Comprehensive survey on petya ransomware attack. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)* (pp. 122-125). IEEE.
- [22]. Aidan, J. S., & Garg, U. (2018, December). Advanced Petya ransomware and mitigation strategies. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 23-28). IEEE.
- [23]. Kardava N. (2018). Kiberprostranstvo kak novaya politicheskaya real'nost': vyzovy i otvety. *Istoriya i sovremennost'*, 1-2(27-28), 152-166. [In Russian].
- [24]. Yang, J. (2013). Post-Lulzsec Cybersecurity. *Insight and Inquiry*, 6(1), 46-64.
- [25]. Henderson, S. J. (2007). *The Dark Visitor: Inside the World Of Chinese Hackers*. Leavenworth, KS: Foreign Military Studies Office.
- [26]. Richards, I., & Wood, M. A. (2018). Hacktivists against terrorism: A cultural criminological analysis of Anonymous' anti-IS campaigns. *International journal of cyber criminology*, 12(1), 187-205.
- [27]. Jarvis, L., MacDonald, S., & Chen, T. M. (2015). *Terrorism Online: Politics, Law and Technology*. Routledge.
- [28]. Shokhnekh, A. V., Mironova, O. A., Moiseeva, L. R., Yakovleva, L. Y., & Evstafieva, A. K. (2019). Provision of innovational and economic security of small business in the internet space of cyber-economy on the platform of cognitive assistants of artificial intelligence. In *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT* (pp. 1023-1029). Springer, Cham.
- [29]. Wall, D. (Ed.). (2003). *Crime and the Internet*. Routledge.
- [30]. Kerr, O. S. (2009). Vagueness Challenges to the Computer Fraud and Abuse Act. *Minn. L. Rev.*, 94, 1561.
- [31]. Nikolaeva, A. B., & Tumbinskaya, M. V. (2014). Cybercrime: a history of development, problems of investigation practice. [in Russian]. Retrieved from: <https://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-%20sorucom-2014/629/> [accessed: 20 January 2021].
- [32]. Bilenchuk, P., & Maliy, M. (2019). Kibersvit u novomu tysyacholitti. Khto vony: kibertzlochynsi, kibershakhrayi, kiberterorysty? *Yurydychnyy Visnyk Ukrainy*, 39, 14-15. [In Ukrainian].
- [33]. Firsch, J. (10). Cyber Security Trends You Can't Ignore In 2021. *PurpleSec*.
- [34]. Mykus, S. A. (2017). The strategy of building functionally stable information-telecommunication systems. *Suchasni informatsiyi tekhnolohiyi u sferi bezpeky ta oborony*, (2), 42-45.