УДК 004.056.005(73)

Цитування:
Sarancha V., Shabunina V., Tur O. (2023). Information Security Management: American Experience. Library Science. Record Studies. Informology, 3, 89–98 [in Ukrainian].

Саранча В. І., Шабуніна В. В., Тур О. М. Управління інформаційною безпекою: американський досвід. *Бібліотекознавство. Документознавство. Інформологія*. 2023. № 3. С. 89–98.

Sarancha Viktor,
Candidate of Historical Sciences,
Associate Professor,
Associate Professor at the Department
of Humanities, Culture and Art
Kremenchuk Mykhailo Ostrohradskyi
National University
https://orcid.org/0000-0001-9435-0615
visar73@ukr.net

Shabunina Viktoriia,
Candidate of Philology, Associate Professor,
Associate Professor at the Department
of Humanities, Culture and Art
Kremenchuk Mykhailo Ostrohradskyi
National University
https://orcid.org/0000-0001-7957-3378
shabuninaviktoria@gmail.com

Tur Oksana,
Doctor of Science in Social Communications,
Professor, Professor at the Department
of Humanities, Culture and Art
Kremenchuk Mykhailo Ostrohradskyi
National University
https://orcid.org/0000-0002-8094-687X
oktur@ukr.net

INFORMATION SECURITY MANAGEMENT: AMERICAN EXPERIENCE

The purpose of the article *is a comprehensive analysis of the American concept of threats to information security and determination of priority areas of the US's activity in creating a secure national cyberspace.* ***The methodological basis*** *of the study is general scientific and special methods of cognition, in particular, systemic approach, analysis, synthesis, and logical method. Methods of content analysis, comparative and analytical monitoring of Internet resources of US government bodies responsible for information security are also used.* ***The scientific novelty*** *of the study consists in the expansion of ideas about theoretical aspects in the field of information security and the systematic analysis of instrumental, conceptual foundations and practical aspects of information security in the United States.* ***Conclusions.*** *The globalisation of information systems has created a completely new situation in the security field. In cyberspace the main threat to the US national security comes from states and intermediaries acting in their interests. They have the necessary skills and technologies to carry out destructive cyberattacks for military and political purposes, and also effectively use cyberespionage methods, which not only entails economic losses, but also causes great damage to strategically important industries for the US. The American concept covers such three key levels of cyber security as the state, private business and individual users. There are such defence priorities for the United States as ensuring the protection of critical infrastructure, information networks and systems; quality control of used IT equipment; formation of effective mechanisms of interlevel communication and raising awareness at all levels. An important component of the US National Cyber Strategy is international cooperation on information security issues. In this regard, at the international level the United States seeks to implement such opportunities*

© *Sarancha V., 2023*
© *Shabunina V., 2023*
© *Tur O., 2023*

as to encourage countries to increase responsibility for ensuring the security of information systems and networks at the national and global level; to create the legal regime necessary to ensure cross-border access to information; to form a regime of collective cyber defence within the framework of NATO and other bilateral and multilateral agreements with strategic partners; to preserve the maximum possible freedom of action in cyberspace in order to conduct all types of information operations both during military conflicts and in peacetime.

Keywords: *cyberspace, information threat, information war, information security, information management, informatisation, ICT.*

Саранча Віктор Іванович,
кандидат історичних наук, доцент,
доцент кафедри гуманітарних наук, культури і мистецтва
Кременчуцького національного університету імені Михайла Остроградського

Шабуніна Вікторія Валентинівна,
кандидат філологічних наук, доцент,
доцент кафедри гуманітарних наук, культури і мистецтва
Кременчуцького національного університету імені Михайла Остроградського

Тур Оксана Миколаївна,
доктор наук із соціальних комунікацій, професор,
професор кафедри гуманітарних наук, культури і мистецтва
Кременчуцького національного університету імені Михайла Остроградського

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: АМЕРИКАНСЬКИЙ ДОСВІД

Мета статті – *аналіз американської концепції загроз інформаційній безпеці та з'ясування пріоритетних напрямів діяльності держави у створенні безпечного національного кіберпростору*. ***Методологічну основу*** *дослідження склали загальнонаукові та спеціальні методи пізнання, як-от: термінологічний, системний підхід, аналіз, синтез та логічний метод. Також використано методи контент-аналізу, порівняльний та аналітичний моніторинг інтернет-ресурсів органів державної влади США, що відповідають за інформаційну безпеку.* ***Наукова новизна*** *статті полягає в розширенні уявлень про теоретичні аспекти в галузі інформаційної безпеки та системному аналізі інструментальних, концептуальних основ і практичних аспектів інформаційної безпеки США.* ***Висновки.*** *Глобалізація інформаційних систем кардинально вплинула на ситуацію у сфері безпеки. Головна загроза національній безпеці США в кіберпросторі походить від держав і посередників, які діють в їхніх інтересах. Вони володіють необхідними навичками й технологіями для проведення деструктивних кібератак у військових і політичних цілях, а також ефективно використовують методи кібершпигунства, що не тільки спричиняє значні економічні втрати, але й завдає великої шкоди стратегічно важливим для США галузям промисловості. Американська концепція охоплює такі три ключові рівні кібербезпеки, як держава, приватний бізнес та індивідуальні користувачі. Сполучені Штати ведуть боротьбу з кібератаками за кількома напрямами, як-от: забезпечення захисту критичної інфраструктури, інформаційних мереж і систем; контроль за якістю використовуваного IT-обладнання; формування ефективних механізмів міжрівневої комунікації та підвищення поінформованості на всіх рівнях. Важливою складовою національної кіберстратегії США є міжнародна співпраця з питань гарантування інформаційної безпеки. На міжнародному рівні США прагнуть спонукати інші країни до підвищення відповідальності за гарантування безпеки інформаційних систем і мереж на національному та глобальному рівнях; створити правовий режим, необхідний для забезпечення транскордонного доступу до інформації; сформувати режим колективного кіберзахисту в межах НАТО та інших двосторонніх і багатосторонніх угод зі стратегічними партнерами; зберегти максимально можливу свободу дій у кіберпросторі з метою проведення всіх видів інформаційних операцій як під час військових конфліктів, так і в мирний час.*

Ключові слова: *кіберпростір, інформаційна загроза, інформаційна війна, інформаційна безпека, інформаційний менеджмент, інформатизація, ІКТ.*

The relevance of the research. Today's current problems in the socio-economic sphere, in particular the full-scale aggression of the Russian Federation and the deterioration of the economic situation in the country, digitalisation of social life, intensifying competition with foreign manufacturers in the domestic market, etc., encourage domestic entrepreneurs to master the methods and tools of information management. Despite the significant theoretical developments of domestic and foreign scientists in this field, information management is a relatively new scientific direction. In the context of this direction, the information policy of the modern period of the development of the Ukrainian state in the conditions of globalisation and Ukraine's entry into civilised communities is being formed.

In the modern sense, information management should perform such types of work as research of the enterprise as an object of management; formation of information resources of the enterprise as a management base; creation of information products as a means of management. An integral component of information management is the management of information security of the institution, the region and the country as a whole.

Analysis of recent research and publications. Problems of threats to information security are of interest to many Ukrainian and foreign researchers. Thus, A. Nashynets-Naumova [4], O. Frolova [8], M. R. Fazlida, Said Jamaliah [15], K. Fokina-Mezentseva [7] and many others have paid special attention to global information security. At the same time, K. Zakharenko [3] has studied information security as a basic component of information management within the framework of modern world markets and processes of digital transformation of the economy. A number of scientists, in particular V. Dubnytskyi and N. Naumenko [2], Yogesh K. Dwivedi, D. Laurie Hughes at al. [14], Zahoor Ahmed Soomro, Mahmood Hussain Shah and Javed Ahmed [20] have considered the problem of information security from the point of view of the need to develop a company's information management model based on leadership technology in conditions of digitalisation of the economy. O. Tur and V. Shabunina have analysed the impact of negative media content on a personality [5] and negative practices as a reaction to destructive content [6].

Such scientists as I. Khanin [9], I. Hrabar, R. Hryshchuk and K. Molodetska [1] have analysed the information management of economic entities and regions, as well as the effectiveness of information security in the conditions of information management not only at various levels of the economy, but also in cybernetic and information space.

The purpose of the work is a comprehensive analysis of the American concept of threats to information security and determination of priority areas of activity of the state in creating a secure national cyberspace. The research methodology consists of general scientific and special methods of cognition, in particular, systemic approach, analysis, synthesis, and logical method. Methods of content analysis, comparative and analytical monitoring of Internet resources of the US government bodies responsible for information security were also used.

Presentation of the main material. Today, the intensive informatisation of all spheres of society's life activity is one of the determining global factors of further socio-economic, intellectual and spiritual development of mankind. At the same time, the world community is entering a new stage of its history, which has every reason to characterise it as an era of information wars. So, the information component is a key element of the Russian Federation's hybrid war against our state. This creates real threats to the national security of Ukraine, since the domestic information infrastructure in the temporarily occupied territories is purposefully destroyed, cyber-attacks are carried out against Ukraine, and channels for the dissemination of relevant information about the country's current socio-political situation are blocked. In addition, destructive information operations are conducted against the background of the deployment of a powerful propaganda campaign against Ukraine, aimed, in particular, at preventing the realisation of the civilisational choice of Ukrainian society. Therefore, in the conditions of the rapid development of the Ukraine's information society and the global information space, as well as the wide use of information and communication technologies in all spheres of life, the problems of information security acquire special importance. At the same time, Ukraine considers the creation of an integrated system of information threat assessment and prompt response to them to be one of the strategic priorities of ensuring information security.

Technological breakthrough of the 1970s led to a deep transformation of all spheres of life in society and the state. The emergence and active development of information and communication technologies initiated the formation of an information society, which means the transition from a production to a service economy, where theoretical knowledge, technologies and information are considered to be mass consumer goods. The USA, along with the countries of Western Europe and Japan, were the first to make the transition to the information society. In the early 1970s, the majority of the workforce (more than 70%) in these countries was concentrated in the service sector and consisted of so-called information workers.

Today, information and communication technologies form the basis of the information

society, which is rapidly acquiring global features. The global Internet network covers about 2.5 billion people (approximately 35% of the entire population of the Earth) [17]. The Internet of things is actively developing, connecting not only people, but also networks, computer devices, household appliances and other objects.

R. Backstrom, the former president of the Corporation for the Management of Domain Names and IP Addresses, has formulated three key principles regarding the Internet:

1. Everything that has access to the Internet can be "hacked";

2. Everything has access to the Internet;

3. So, everything becomes vulnerable. The world is entering a phase of endless struggle against cyber threats, which are constantly updated [10].

Obviously, technologically more developed countries are at the same time more vulnerable in the information space. In the conditions of wide network integration, the interconnection and interdependence of the information spaces of states is growing. That is why the issue of countering threats in the information sphere has both a national and a global dimension.

It is important to note that the international community has not yet come to a common understanding of key terms in the field of information security. Countries interpret and define its boundaries in different ways. In general, two main approaches to defining information security can be distinguished – broad and narrow. According to a broad understanding, the concept of information security includes both information-technical and information-psychological aspects. This approach corresponds to the vision of the countries in the post-Soviet space, China and a number of other states. They define information security as a state of protection of individuals, society and the state and their interests from threats, destructive and other negative influences in the information space.

At the same time, the US takes a narrower approach. It limits the term "information security" to technological aspects and defines it as the protection of information and information systems and networks from unauthorised access, use, disclosure, damage, modification or destruction in order to ensure its integrity, confidentiality and availability [16].

Therefore, information security issues, from the US point of view, do not include content and its management. Cybersecurity is a priority for the United States, where "cyber" is the global space within the information domain that encompasses the interdependent networks of information technology infrastructure and the data contained therein, including the Internet, telecommunications networks, computer systems, and embedded processors and control systems [12].

The United States, a leader in the field of ICT, was one of the first to face the negative consequences of the information revolution. Today, the experience of the United States in the field of ensuring information security is advanced. In 1976, the American analyst T. Ron pointed out that the information infrastructure was a key component of the economy and at the same time one of the most vulnerable targets in both wartime and peacetime [19].

Today, the economy and national security of the USA are completely dependent on information technologies and information infrastructure. Network technologies support critical US infrastructure in such sectors as energy, transportation, banking and finance, information and telecommunications, health care, emergency services, agriculture, food, water, military, industrial, chemical, and hazardous materials, mail and delivery services. Considering this, the main concern of the US leadership is caused by organised cyber-attacks, as a result of which damage may be caused to the national critical infrastructure, economy or national security [23].

The number of incidents related to computer systems and networks is constantly growing in the country. According to the US Computer Incident Response Centre (US-CERT), the growth of cyber incidents was 782% from 2006 to 2012. At the same time, according to information of the US Department of Homeland Security (DHS), the number of reports of computer incidents related to the country's critical infrastructure increased by 83% from 2011 to 2013. The majority of cyberattacks were directed against enterprises in the energy sector, as well as the transport, water supply, chemical and nuclear industries. It is worth noting that in 2013, in the annual report of the US intelligence community "Global Threat Assessment", cyber threats ranked first in the list of national security threats, overtaking terrorism as the biggest threat of the last decade [26].

Despite the importance of ensuring information security and countering threats in this area, the United States has not adopted a single concept of information threats. No official US document at the level of national strategy contains a list of threats in this area and their definitions. In American analytical and research materials, you can find different approaches to the classification of threats in the field of information security. From the point of view of the properties of information that are violated, as well as information systems and networks, destructive actions in the information space are aimed at:

- violation of confidentiality (by obtaining unauthorised access to information stored in the information system);

- breach of integrity (using unauthorised modifications and changes to information systems

and data stored in them);

- violation of accessibility (by creating obstacles for malicious purposes for access to information systems and information) [21].

According to the nature of information security threats, they are divided into natural and anthropogenic.

Natural threats include:

- threats of a natural nature (related to natural phenomena and natural disasters, including earthquakes, floods, fires, hurricanes, etc.);

- man-made threats (related to problems in equipment and technology).

There are intentional and unintentional threats of an anthropogenic nature associated with human actions in relation to information, computer systems and networks. At the same time, threats of an intentional nature include both targeted attacks (when the target of the attack is a certain information system or a critical infrastructure object) and non-targeted ones (without a specific goal, for example, in cases of using malicious programmes) [11].

The increase in the number of means and methods of carrying out destructive actions in the network causes the fact that the human factor is becoming the main threat to information security. Sources of threats to information security are considered to be numerous entities that possess the necessary knowledge or capabilities to carry out destructive actions in the information space.

Based on the data of the US General Accounting Office [22] and the Computer Incident Response Centre, different group of sources of cyber threats related to industrial control systems can be distinguished (*Table 1*).

Table 1

The sources of cyber threats

A source of cyber threats	**The main features of the source of cyber threats**
business competitors	such companies seek to acquire information about a competing company in order to gain advantages in various areas (pricing, production, product development, etc.);
states	they use cyber tools to gather information and perform intelligence activities, including economic espionage, with the aim of obtaining political, military and economic advantage. In addition, a number of states conduct developments in the field of information warfare with the aim of reducing the space for the adversary to make decisions, gain a strategic advantage and destroy specific targets, in particular, supporting communications and economic infrastructure that provide the country's military power;
criminal groups	they carry out cyber-attacks with the aim of obtaining monetary profit. Organised crime groups use spam, phishing or malware as tools to carry out identity theft, internet theft and computer extortion;
international corporate spies	they carry out economic and industrial espionage, theft of large sums of money, and also closely interact with hackers, providing them with the necessary conditions for potential development;
botnet operators	they use a network (botnet) of hacked and remotely controlled systems in order to carry out coordinated attacks, spread phishing schemes, spam, etc.;
creators of surveillance programmes and malicious programmes	individuals or organisations create and use tracking programmes and various malicious programmes against users for criminal purposes;
creators of phishing	they create phishing schemes with the aim of stealing personal data and obtaining financial profit;
company employees / insiders	with knowledge of the company's computer systems, they are free to access them and cause damage or steal data. Additionally, contractors hired by companies, as well as careless or poorly trained employees, can inadvertently infect a system with malware;
spammers	they distribute electronic messages containing hidden or false information about the sale of any product, use phishing schemes, distribute spyware and virus programmes, or conduct computer attacks such as DDoS;
terrorists	they aim to destroy, disable critical infrastructure, or interfere with its functioning, which is a threat to national security and can lead to mass casualties, weakening the economy, or undermining the morale of the population. Terrorists may use phishing schemes, spyware or malware to obtain sensitive information or financial resources;
hackers	they penetrate into closed information systems and networks for the purpose of obtaining financial benefit or expressing a civic position, self-affirmation, testing their abilities and skills;
hacktivists (politically active hackers)	they attack web pages and mail servers in order to post political texts on them.

The technological capabilities of various sources of information threats also differ significantly. The Scientific Council of the US Defence Department identifies six main categories of cyber threats sources and divides them into three levels depending on the potential of using ICT for destructive purposes [18] (*Table 2*).

Table 2

The categories of the main cyber threats' sources

Categories	The features of the categories
I, II – actors (mainly individuals)	These actors have basic knowledge and the potential to create simple malicious programmes that use existing vulnerabilities. Their activity is considered to be the least dangerous in terms of possible damage.
III – individuals, IV – organised criminal groups and states	These actors possess a certain level of expertise and experience and use a wide range of computer tools to identify new network vulnerabilities and conduct computer attacks.
V – actors (states)	These states have the ability to install malware and modified hardware into computers and computer systems at various stages of their production to further conduct cyber-attacks (including time-delayed attacks). They can overcome the highest degree of network protection.
VI – actors (states)	These states have the potential to conduct a full range of information operations (including operations with the support of the armed forces and the intelligence sector) with the aim of achieving specific results in the political, military and economic spheres. They can overcome the highest degree of network protection.

So, according to this categorisation, in cyberspace the greatest threat comes from states or interested actors. Depending on the goals and tasks pursued by actors in cyberspace, as well as their potential, the Presidential Commission on Critical Infrastructure Protection has identified three main levels of information security threats and related types of threats. According to this approach, in cyberspace such destructive actions of states as information warfare and cyberespionage are among the most dangerous from the point of view of national security. At the same time, the use of ICT for criminal and terrorist purposes is a threat to both the state and the private sector. Local threats corresponding to the level of individual users and local networks include the actions of hackers. At the same time, the threat of destructive actions by insiders persists at all levels.

The classification clearly demonstrates that ensuring information security requires a set of measures at the level of the state, private companies and individuals. At the same time, in the US, effective countermeasures against these threats at the national level are possible only with close cooperation between the public and private sectors, since a significant part of the country's critical infrastructure and networks is privately owned. Therefore, it is necessary to increase the level of overall responsibility for ensuring security, as well as to establish feedback and to ensure inter-level interaction.

In general, American scientific research institutes and advisory bodies form the national concept of threats to information security and lay the foundations for the activities of federal ministries and departments to ensure information security. At the level of federal institutions, two main approaches to threat identification can be distinguished. The first one is based on destructive actions that pose a threat to information security, the second – on the subjects of the threat. Thus, the US Department of National Security classifies cyber-attacks against the integrity and availability of data and cyber-attacks against physical infrastructure as the highest-level threats to US national security and equates them to the level of hostile attacks [16]. Representatives of the US intelligence service distinguish two groups of cyber threats based on destructive actions:

- cyber-attacks – special offensive operations aimed at achieving a physical effect or influencing information, its distortion and destruction, which can vary from DDoS-attacks on sites to attacks on critical infrastructure objects that can take them out of order for a long time;
- cyberespionage – interference in networks with the aim of gaining access to diplomatic, military or economic information [24].

During discussions on international information security, the US considered such sources of threats to cyber security as criminals, states, terrorists, as well as intermediaries (individuals or groups that carry out malicious network activities on behalf of state or non-state actors for obtaining financial benefits or based on nationalistic or other political motives).

The US Department of Defence conducts activities taking into account four categories of cyber security threats, which include both actors and individual actions [13] (*Fig. 1*).

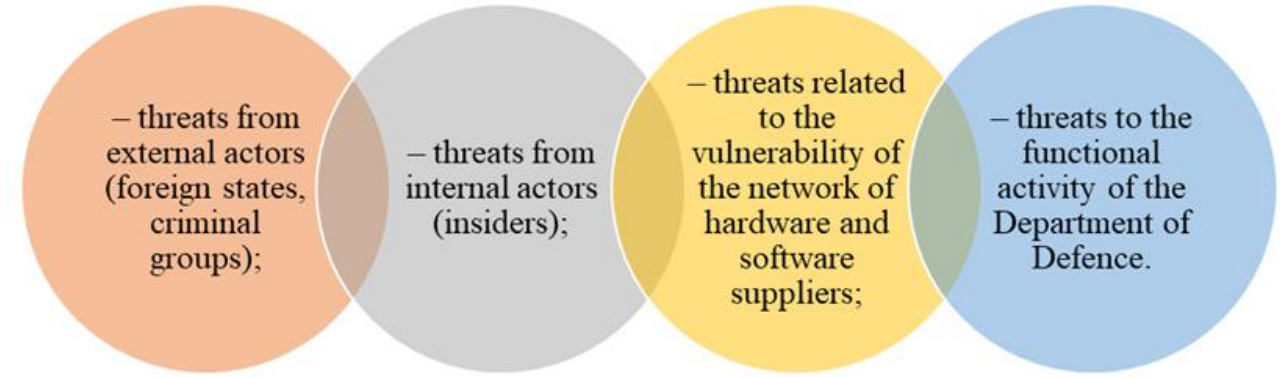

Fig. 1. ***Categories of cyber security threats***

The departmental approach demonstrates that, in practice, the perception of threats to information security is largely determined by the tasks within the competence of one or another federal structure. At the same time, threats from the actions of states, criminals and terrorists belong to the area of responsibility of several ministries and agencies at once, which determines the need to ensure interdepartmental cooperation on information security issues.

The scientific novelty of the study consists in the expansion of ideas about theoretical aspects in the field of information security and the systematic analysis of instrumental, conceptual foundations and practical aspects of information security in the United States.

Conclusions. So, the globalisation of information systems has created a completely different situation in the security sphere. Cyberspace is changing the traditional threats to national security that come from states, as well as non-state actors such as criminals and terrorists who use ICTs for destructive purposes.

At the same time, in cyberspace the main threat to the US national security comes from states and intermediaries acting in their interests. They have the necessary skills and technologies to carry out destructive cyberattacks for military and political purposes, and also effectively use cyberespionage methods, which not only entails economic losses, but also causes great damage to strategically important industries for the US.

The American concept covers such three key levels of cyber security as the state, private business and individual users (citizens). Given the potential targets of cyberattacks, there are several defence priorities for the United States (*Fig. 2*).

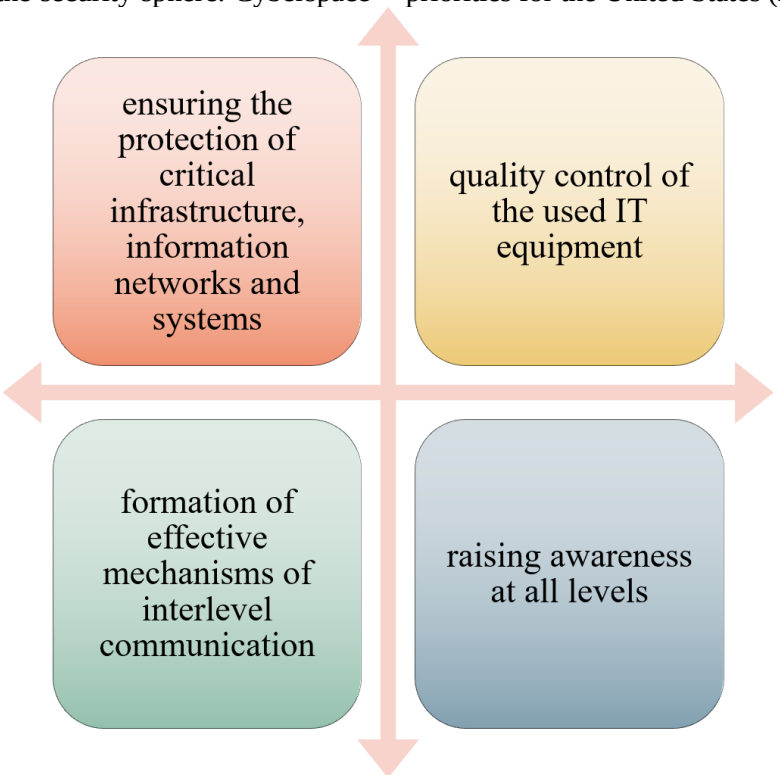

Fig. 2. ***US defence priorities***

When considering threats, a clear distinction can be made between actors, their goals and technological potential. However, despite this, in practice, one of the main cyberspace problems is identifying the source of the attack. The high speed of actions on the Internet, the possibility of maintaining anonymity, as well as the removal of traces of malicious use of ICT make it significantly more difficult to establish discrepancies between the actions of criminals, terrorists and states. In this regard, international cooperation on the entire spectrum of information security threats is of particular importance.

It is worth noting that the United States is one of the world leaders in the field of information security. This primacy concerns both its institutional component and practical implementation. At the same time, the United States recognises the impossibility of ensuring cyber security unilaterally. International cooperation on issues of ensuring information security is an important component of the US National Cyber Strategy. In this regard, the United States seeks to implement the following opportunities at the international level:

1. Encourage countries to increase responsibility for ensuring the security of information systems and networks at the national and global level. In particular, elements of the concept of a global culture of cyber security are aimed at fulfilling this task.

2. Create the legal regime necessary to ensure cross-border access to information, which is an important basis for the activities of both US law enforcement agencies in combating cybercrime, and for US special services.

3. Form a regime of collective cyber defence within the framework of NATO and other bilateral and multilateral agreements with strategic partners.

4. Preserve the maximum possible freedom of action in cyberspace in order to conduct all types of information operations both during military conflicts and in peacetime.

So, the experience of the USA in the field of ensuring reliable information security is valuable for our country, which has been waging a hybrid war with the Russian Federation for almost ten years.

References

1. Hrabar, I. G., Hryschuk, R. V., Molodetska, K. V. (2019). Security synergy: cybernetic and informational aspects: monograph. In general ed. R. V. Hryshchuk. Zhytomyr: ZhNAEU [in Ukrainian].

2. Dubnytskyi, V. I., Naumenko, N. Yu. (2019). Methodological support for the formation of information security in the sphere of economic security of the region. Bulletin of economic science of Ukraine, 1 (36), 35–39 [in Ukrainian].

3. Zakharenko, K. (2018). Theoretical foundations of information security research. International relations, public communications and regional studies, 2(4), 107–116. Retrieved from: https://relint.vnu.edu.ua/index.php/relint/issue/view/7/4 [in Ukrainian].

4. Nashynets-Naumova, A. Yu. (2017). Information security: issues of legal regulation: monograph. Kyiv: Helvetica Publishing House [in Ukrainian].

5. Tur, O. M., Shabunina, V. V. (28–29.04.2023). Media safety: negative content and its impact on personality. Materials of the International Scientific and Practical Conference "Social Communications: Tools, Technology and Practice". Zaporizhzhia, 2023, 32–33 [in Ukrainian].

6. Tur, O. M., Shabunina, V. V. (02–05.05.2023). Negative practices as a reaction to destructive content. Proceedings of the XVII International Scientific and Practical Conference "System analysis and intelligent systems for management". Turkey, Ankara, 2023, 52–54 [in Ukrainian].

7. Fokina-Mezentseva, K. (2021). Information security in global society. Bulletin of the Kyiv National University of Trade and Economics, 5, 61–71 [in Ukrainian].

8. Frolova, O. M. (2018). The role of the UNO in the system of international information security. International relations. Political sciences, 18–19. Retrieved from: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468/3140 [in Ukrainian].

9. Khanin, I. H. (2015). Formation in the international system of information security: economic guidelines for Ukraine. Efficient economy, 4. Retrieved from: http://www.economy.nayka.com.ua/?op=1&z=4457 [in Ukrainian].

10. Beckstrom, R. Speech at the London Conference on Cyberspace. Retrieved from: https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf [in English].

11. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. Retrieved from: http://www.gao.gov/assets/270/268137.pdf [in English].

12. Department of Defense Dictionary of Military and Associated Terms. Joint Chiefs of Staff. Retrieved from: https://irp.fas.org/doddir/dod/jp1_02.pdf [in English].

13. Department of Defense Strategy for Operating in Cyberspace. Retrieved from: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [in English].

14. Dwivedi Yogesh, K., Hughes D., Laurie, Coombs, Crispin, Constantiou, Ioanna, Duan Yanqing, Edwards John S. et al. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. The International Journal of Information Management. Vol. 15. doi:10.1016/j.ijinfomgt.2020.102211. Retrieved from: https://www.sciencedirect. com/science/article/abs/pii/S026840122031286X [in English].

15. Fazlida, M. R., Jamaliah, Said. (2015). Information Security: Risk, Governance and Implementation Setback. Procedia Economics and Finance, Vol. 28, 243–248. Retrieved from: https://doi.org/10.1016/S2212-5671(15)01106-5 [in English].

16. Federal Information Security Act. 2002. Retrieved from: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf [in English].

17. Internet World Stats. Usage and Population Statistics. Retrieved from: http://www.internetworldstats.com/top20.html [in English].

18. Resilient Military Systems and the Advanced Cyber Threat. Task Force Report. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/ Cyber-081.pdf [in English].

19. Rona Thomas, P. Weapons Systems and Information War. Retrieved from: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf [in English].

20. Soomro Zahoor Ahmed, Shah Mahmood Hussain, Ahmed Javed. Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215–225. Retrieved from: https://ideas.repec.org/a/eee/ininma/v36y2016i2p215-225.html [in English].

21. Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security. Washington: The White House, July, 2011. P. 7. Retrieved from: https://obamawhitehouse.archives.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf [in English].

22. Terrorist Use of the Internet: Information Operations in Cyberspace. Retrieved from: https://sgp.fas.org/crs/terror/R41674.pdf [in English].

23. The National Strategy to Secure Cyberspace. Washington D. C.: The White House. Retrieved from: https://www.boozallen.com/expertise/cybersecurity/national-cyber-strategy.html?gclid=CjwKCAjw8ZKmBhArEiwAspcJ7nmIGzD3DuezFqO4DAai2m8CDPAqRBNKTor9XTzGD1pbqxT9yXcFDRoC5AsQAvD_BwE [in English].

24. The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations. Retrieved from: https://www.files.ethz.ch/isn/178418 /terminology2.pdf [in English].

25. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation / Department of Homeland Security. December 2011. Retrieved from: https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf [in English].

26. Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. Retrieved from: https://www.intelligence. senate.gov/130312/clapper.%20pdf [in English].

Список використаних джерел

1. Грабар І. Г., Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / за заг. ред. Р. В. Грищука. Житомир : ЖНАЕУ, 2019. 280 с.

2. Дубницький В. І., Науменко Н. Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. *Вісник економічної науки України*. 2019. № 1(36). С. 35–39.

3. Захаренко К. Теоретичні засади дослідження інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 2(4). С. 107–116. URL: https://relint.vnu.edu.ua/index.php/relint/issue/view/7/4 (дата звернення: 17.06.2023).

4. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

5. Тур О. М., Шабуніна В. В. Медіабезпека: негативний контент та його вплив на особистість. *Соціальні комунікації: інструменти, технологія і практика* : матеріали Міжнародної науково-практичної конференції (Запоріжжя, 28–29 квітня 2023 р.). Запоріжжя, 2023. С. 32–33.

6. Тур О. М., Шабуніна В. В. Негативні практики як реакція на деструктивний контент. *System analysis and intelligent systems for management* : Proceedings of the XVII International Scientific and Practical Conference (Ankara, May 02–05, 2023). Turkey, Ankara, 2023. P. 52–54.

7. Фокіна-Мезенцева К. Інформаційна безпека у глобальному суспільстві. *Вісник Київського національного торговельно-економічного університету*. 2021. № 5. С. 61–71.

8. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Міжнародні відносини. Політичні науки*. 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468/3140 (дата звернення: 11.06.2023).

9. Ханін І. Г. Формування в міжнародній системі інформаційної безпеки: економічні орієнтири для України. *Ефективна економіка*. 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=4457 (дата звернення: 27.04.2023).

10. Beckstrom R. Speech at the London Conference on Cyberspace. URL: https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf (дата звернення: 15.06.2023).

11. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. URL: http://www.gao.gov/ assets/270/268137.pdf (дата звернення: 12.06.2023).

12. Department of Defense Dictionary of Military and Associated Terms. Joint Chiefs of Staff. URL: https://irp.fas.org/doddir/dod/jp1_02.pdf (дата звернення: 17.05.2023).

13. Department of Defense Strategy for Operating in Cyberspace. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата звернення: 07.06.2023).

14. Dwivedi Yogesh K., Hughes D. Laurie, Coombs Crispin, Constantiou Ioanna, Duan Yanqing, Edwards John S. et al. Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *The International Journal of Information Management*. 2020. Vol. 55. doi:10.1016/j.ijinfomgt.2020.102211. URL: https://www.sciencedirect.com/ science/article/abs/pii/S026840122031286X (дата звернення: 07.04.2023).

15. Fazlida M. R., Jamaliah Said. Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*. 2015. Vol. 28. P. 243–248. URL: https://doi.org/10.1016/S2212-5671(15)01106-5 (дата звернення: 22.06.2023).

16. Federal Information Security Act. 2002. URL: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (дата звернення: 15.06.2023).

17. Internet World Stats. Usage and Population Statistics. URL: http://www.internetworldstats.com/top20.html (дата звернення: 17.04.2023).

18. Resilient Military Systems and the Advanced Cyber Threat. Task Force Report. URL: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/ Cyber-081.pdf (дата звернення: 11.06.2023).

19. Rona Thomas P. Weapons Systems and Information War. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf (дата звернення: 18.06.2023).

20. Soomro Zahoor Ahmed, Shah Mahmood Hussain, Ahmed Javed. Information security management needs more holistic approach: A literature review. International Journal of Information Management. *Elsevier*. Vol. 36(2). P. 215–225. URL: https://ideas.repec.org/a/eee/ininma/v36y2016i2p215-225.html (дата звернення: 17.06.2023).

21. Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security. Washington: The White House, July 2011. P. 7. URL: https://obamawhitehouse.archives.gov/sites/default/files/ Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf (дата звернення: 27.06.2023).

22. Terrorist Use of the Internet: Information Operations in Cyberspace. URL: https://sgp.fas.org/crs/terror/R41674.pdf (дата звернення: 17.06.2023).

23. The National Strategy to Secure Cyberspace. Washington D.C.: The White House. URL: https://www.boozallen.com/expertise/cybersecurity/national-cyber-strategy.html?gclid=CjwKCAjw8ZKmBhArEiwAspcJ7nmIGzD3DuezFqO4DAai2m8CDPAqRBNKTor9XTzGD1pbqxT9yXcFDRoC5AsQAvD_BwE (дата звернення: 12.05.2023).

24. The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations. URL: https://www.files.ethz.ch/isn/178418/terminology2.pdf (дата звернення: 04.06.2023).

25. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation / Department of Homeland Security. December 2011. URL: https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf (дата звернення: 26.06.2023).

26. Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. URL: https://www.intelligence.senate.gov/130312/clapper.%20pdf (дата звернення: 17.05.2023).

Стаття надійшла до редакції 11.07.2023
Отримано після доопрацювання 15.08.2023
Прийнято до друку 23.08.2023