UDC 351:343.85 (477)
DOI: https://doi.org/10.32689/2617-2224-2019-17-2-296-306

Ostrovoy Aleksey Vladimirovich,
Applicant of Ph.D. in Public Administration, Donetsk State University of Management, 87513, Mariupol, Str. Karpinsky, 58, tel.: (050) 426 07 70, e-mail: ostrovalexsey@icloud.com
ORCID: 0000-0002-7704-5149

Островий Олексій Володимирович,
здобувач наукового ступеня кандидата наук з державного управління, Донецький державний університет управління, 87513, м. Маріуполь, вул. Карпинського, 58, тел.: (050) 426 07 70, e-mail: ostrovalexsey@icloud.com
ORCID: 0000-0002-7704-5149

Островой Алексей Владимирович,
соискатель ученой степени кандидата наук по государственному управлению, Донецкий государственный университет управления, 87513, г. Мариуполь, ул. Карпинского, 58, тел.: (050) 426 07 70, e-mail: ostrovalexsey@icloud.com
ORCID: 0000-0002-7704-5149

ANALYSIS OF THE CONDITIONS FOR THE STATE POLICY FORMATION TO ENSURE KIBERNETIC SECURITY IN UKRAINE

Abstract. The article summarizes the main tendencies, features and problems that have a direct impact on the state policy formation for ensuring cybernetic security. The present state of cybercrime in the world has been analyzed and its global distribution has been proved. The potential of cyberattacks in Ukraine has been investigated and its increase was determined by such tendencies in the activity of enterprises and business as the growth of the number of computer equipment, increase of access to the Internet, and also increase of the level of use of information and communication technologies in their activity. The tendency to increase the number of crimes in the sphere of the use of electronic computers, systems and computer networks and telecommunication networks in Ukraine, as well as an increase in their share in the total number of crimes in Ukraine has been revealed. The main factors that contributed to the increase in the number of cybercrime in Ukraine, including technical and structural unwillingness of the

existing system of management of law enforcement agencies, and imperfection of the state policy, have beend generalized. On the basis of the analysis of crimes in the field of the use of electronic computers (after the investigation by criminal proceedings) a “portrait” of a cybercriminator has been formed and it has been proved that its main feature is a high qualification level. It has been revealed that among the positive trends in the field of combating cybercrime in Ukraine today it is possible to observe the introduction of modern methods of detection, fixation and research of digital evidence into practical activity; signing agreements on cooperation in the field of combating cybercrime with organizations from different countries of the world; establishing effective interaction with the world's most famous social networks.

Keywords: state policy, cybernetic security, cybercrime, cyberattack, information and communication technologies.

АНАЛІЗ УМОВ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ

Анотація. Узагальнюються основні тенденції, особливості та проблеми, які мають безпосередній вплив на формування державної політики забезпечення кібернетичної безпеки. Проаналізовано сучасний стан кіберзлочинності у світі та доведено її глобальний характер розповсюдження. Досліджено потенціал кібератак в Україні та виявлено, що його підвищення обумовлено такими тенденціями у діяльності підприємств та бізнесу, як зростання кількості комп’ютерної техніки, підвищення доступу до мережі Інтернет, а також збільшення рівня використання інформаційно-комунікаційних технологій у своїй діяльності. Виявлено постійно зростаючу тенденцію до збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку в Україні, а також збільшення їх питомої ваги у загальній кількості злочинів в Україні. Узагальнено основні фактори, які сприяли зростанню кількості кіберзлочинів в Україні, серед яких як технічна та структурна неготовність існуючої системи управління правоохоронних органів, так і недосконаліть державної політики. На підставі аналізу злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів) (за закінченими розслідуваннями у кримінальних провадженнях) сформовано “портрет” кіберзлочинця та доведено, що основною його рисою є високий кваліфікаційний рівень. Виявлено, що серед позитивних тенденцій у сфері боротьби із кіберзлочинністю в Україні на сьогодні можна спостерігати впровадження у практичну діяльність сучасних методик виявлення, фіксації і дослідження цифрових доказів; підписання договорів про взаємодію у сфері боротьби з кіберзлочинністю з організаціями різних країн світу; налагодження ефективної взаємодії зі світовими соціальними мережами.

Ключові слова: державна політика, кібернетична безпека, кіберзлочин, кібератака, інформаційно-комунікаційні технології.

АНАЛИЗ УСЛОВИЙ ФОРМИРОВАНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ В УКРАИНЕ

Аннотация. Обобщаются основные тенденции, особенности и проблемы, которые имеют непосредственное влияние на формирование государственной политики обеспечения кибернетической безопасности. Проанализировано современное состояние киберпреступности в мире и доказан глобальный характер ее распространения. Исследован потенциал кибератак в Украине и обнаружено, что его повышение обуславлено такими тенденциями в деятельности предприятий и бизнеса, как рост количества компьютерной техники, повышение доступа к сети Интернет, а также увеличение уровня использования информационно-коммуникационных технологий в своей деятельности. Выявлена постоянно растущая тенденция к увеличению количества преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи в Украине, а также увеличение их удельного веса в общем количестве преступлений в Украине. Обобщены основные факторы, которые способствовали росту числа киберпреступлений в Украине, среди которых как техническая и структурная неготовность существующей системы управления правоохранительных органов, так и несовершенство государственной политики. На основании анализа преступлений в сфере использования электронно-вычислительных машин (компьютеров) (по законченным расследованиям в уголовных производствах) сформирован "портрет" киберпреступника и доказано, что основной его чертой является высокий квалификационный уровень. Выявлено, что среди положительных тенденций в сфере борьбы с киберпреступностью в Украине на сегодняшний день можно наблюдать внедрение в практическую деятельность современных методик выявления, фиксации и исследования цифровых доказательств; подписание договоров о взаимодействии в сфере борьбы с киберпреступностью с организациями разных стран мира; налаживание эффективного взаимодействия с известными мировыми социальными сетями.

Ключевые слова: государственная политика, кибернетическая безопасность, киберпреступность, кибератака, информационно-коммуникационные технологии.

Statement of problem in general. The rapid development of information and communication technologies promoted the increase in the world quantity index of Internet users to 4,021 billion people (55,6 %) of the total world population, along with which the increased use of social media and increase in number of Internet users is observed, in particular, the number of users in Ukraine is more than 25 million people or 60,7 % of the population. It should

be noted that increase in level of penetration, use of the Internet and social media by individuals and companies around the world, in turn, promotes the development of Internet business. However, the relationship between business models and operating activities not only provides the opportunities for development of new spheres of activity, but also creates threats due to increased vulnerability in computer networks and increased risk of cyber incidents. These tendencies directly influence the formation and implementation of the state policy for ensuring cybersecurity, so their tracking and permanent analysis becomes extremely important for ensuring national security at this time.

Analysis of recent studies and publications. A number of scientific studies of such authors as A. Babenko, Yu. Baturin, P. Bilenchuk, V. Butuzov, V. Viehov, V. Havlovskyi, V. Holubev, D. Dubov, O. Knyzhenko, M. Kravtsova [4], V. Nomokonov, V. Petrov, M. Pohoretskyi, I. Riazantseva, N. Savchuk, V. Shelomentsev and others is devoted to the problem of ensuring cybersecurity. The leading international organizations and companies such as KPMG International [1], Norton by Symantec [2] and others have also made a significant contribution to the study of this problem. However, currently, there is a clear need for integration of theoretical background with relevant analytical data in this rapidly developing and transforming sphere in order to formulate the effective state policy for ensuring cybersecurity.

The purpose of the article is to substantiate the main conditions directly influencing the formation of the state policy for ensuring cybersecurity in Ukraine.

Statement of main study material. The cybercrime has long been a global phenomenon and problem, as demonstrated particularly by the study of American company Norton [2], according to which 978 million adults in 20 countries (where the study was conducted) in 2017 faced the global cybercrime, which is 44 % of online users. As a result, the consumers, who became victims of cybercrime, lost 172 billion dollars in total (at average 142 dollars per victim). Among the most widespread noted cybercrimes, the following should be noted:

- availability of the device infected with virus or other security threat (53 %);
- problems with debit or credit cards (38 %);
- removal of account password (34 %)
- unauthorized access or hacking of e-mail or social media account (34 %);
- online purchase that was fraudulent (33 %);
- clicking the fraudulent e-mail or provision of confidential (personal/financial) information in response to fraud with e-mail (32 %).

According to another study conducted by KPMG International, about half of company executives (49 %), among the company executives in different countries [1], underline the possibility of cyberattack not in terms of "if", namely "when". Herewith, USA, Australia and Germany (Figure 1) are top three according to the evaluation of cyberattack as imminent threat to

business carried out on a geographic basis. In sectorial section, the sphere of infrastructure became the most prepared for cyberattack (67%). It should be pointed out that only about half of company executives (51%) determine good preparedness for cyberattacks.

If analyze the potential of cyberattacks in Ukraine separately, first of all, it should be noted that according to the State Statistics Committee of Ukraine [3], increase in number of computer equipment (+2 % in 2017 as compared to 2016), improvement of access to the Internet (+2 % in 2017) and increase in use of information and communication technologies in the activity is observed today at the enterprises, in particular in 2017:

+4 % of enterprises having a website operating on the Internet;

+8 % of enterprises using social media (social networks, enterprise blogs or microblogs, websites with multimedia content, means of knowledge sharing);

+13,6 % of enterprises purchasing the cloud computing services during the year;

+4,5 % of enterprises providing electronic/paper invoices;

+3,7 % of enterprises receiving orders via computer networks for sale of goods or services (except for orders received by e-mail);

+14 % of enterprises purchasing via computer networks of goods or services (except for orders received by e-mail).

The largest part of enterprises having access to the Internet belongs to the wholesale and retail trade; repair of motor vehicles and motorcycles, processing industry and construction.

Among the directions of Internet use, the following should be noted: sending or receiving messages via e-mail; making telephone calls using Internet/VoIP or video conferencing;

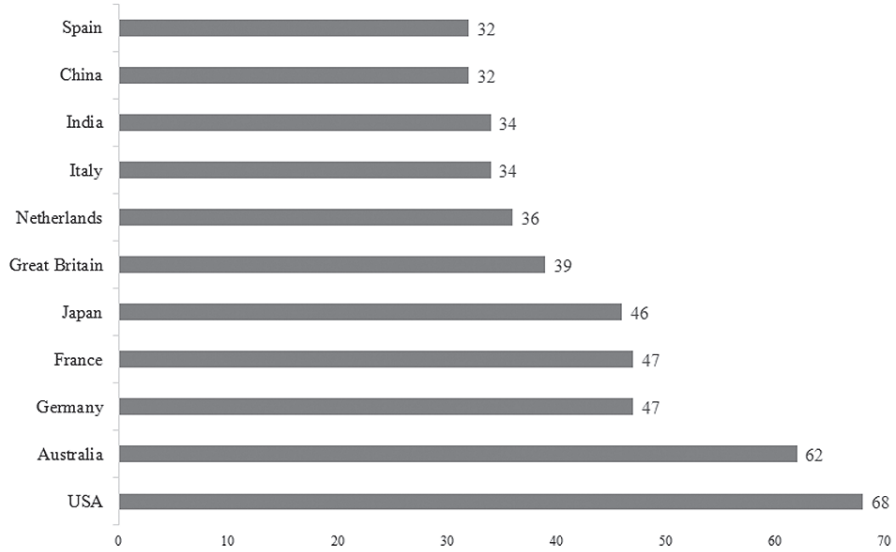

Fig. 1. **Evaluation of cyberattacks as an imminent threat to business**, %
Source: compiled according to [1]

obtaining information on goods and services; use of instant messaging and bulletin board system; obtaining information from state authorities; carrying out various operations with state authorities (except for obtaining information); banking transactions; access to other financial services.

Such tendencies have created not only prerequisites for development of enterprises and national economy in general, but also led to increase in crime rate in the sphere of information and communication technologies.

The information on registered criminal offenses (proceedings) and the results of their investigation are summarized in the reporting form № 1 "Unified Report on Criminal Offenses" that is formed every month by cumulative total from the beginning of reporting period (year) by region of crime commission based on data entered into the National Register of Pre-Trial Investigations by users of the information system, in terms of sections and articles of the Criminal Code of Ukraine; information on persons who committed such crimes is summarized in the reporting form № 2 "Unified Report on Persons Who Committed Criminal Offenses", according to criminal proceedings completed by investigation.

So, let us note that the number of crimes in the sphere of use of electronic computers, systems, computer networks and telecommunication networks have been steadily growing since 2014, reaching 2573 crimes in 2017. The growth rate for 2014–2017 was 480,8 %. In 8 months of 2018, this indicator has already exceeded the level of 2016 by 117,9 %.

The faster growth of registered cybercrimes affected the increase in their share in total number of crimes in Ukraine, keeping the tendencies of increase from 0,08 % in 2014 to 0,51 in 2018, which is the highest indicator since 2009.

Such tendencies were influenced by a number of factors. The following should be noted as main of them: significant rates of society informatization, technology gap of the law enforcement system and need for its reformation, insufficient level of funding of anti-cybercrime actions.

It should be stated that in 2018 the attention of employees of the cyberpolice was focused on the investigation of crimes committed in the sphere of high information technologies. So, during the year, employees of the Department of Cyberpolice were involved in the investigation of more than 11 thousand criminal proceedings. Their structure is shown in Fig. 2.

At the same time, it should be noted that by regions the largest number of crimes in 2017 was concentrated in the city of Kyiv, Kyiv, Chernivtsi and Lviv Oblasts. According to the results of 2018, the highest criminal activity was observed in the city of Kyiv, as well as in the territories of Cherkasy, Odesa, Mykolaiv and Lviv Oblasts.

The analysis of the structure of cybercrimes in dynamics in the period from 2013 to 2017 allowed to state the largest share of crimes committed under Article 361 of the Criminal Code of Ukraine: unauthorized interference with operation of electronic computers, automated systems, computer networks or telecommunication networks (from 50 to 77 %) (Table 1). In addi-

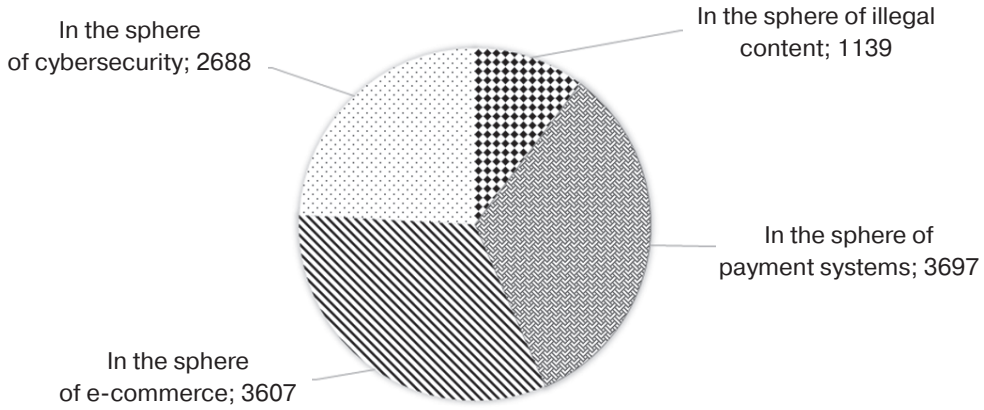

Fig. 2. **Structure of criminal proceedings being investigated by cyberpolice (2018)**, pcs.

Source: compiled according to [5]

Table 1

Structure of cybercrime on the criminal and law basis for 2013–2017 [4]

Criminal offenses reported in the reporting period	2013	2014	2015	2016	2017
Unauthorized interference with operation of electronic computers, automated systems, computer networks or telecommunication networks (Article 361 of the Criminal Code of Ukraine)	408	344	432	494	1795
Creation of malwares and malicious technical means for the purpose of use, distribution or sale, as well as their distribution or sale (Article 361-1 of the Criminal Code of Ukraine)	12	10	21	15	35
Unauthorized distribution of restricted information stored in electronic computers, automated systems, computer networks or on the carriers of such information (Article 361-2 of the Criminal Code of Ukraine)	20	11	59	28	64
Unauthorized actions with information that is processed in electronic computers, automated systems and computer networks or stored on the carriers of such information, committed by a person having the right of access to it (Article 362 of the Criminal Code of Ukraine)	152	73	75	311	670
Violation of the rules of operation of electronic computers, automated systems, computer networks or telecommunication networks or procedure or rules of protection of information processed in them (Article 363 of the Criminal Code of Ukraine)	2	4	9	15	6
Interference with operation of electronic computers, automated systems, computer networks or telecommunication networks by mass messaging (Article 363-1 of the Criminal Code of Ukraine)	1	1	2	2	3
Total	595	443	598	865	2573

tion, there is general increase in cybercrimes in the dynamics due to these crimes.

A more detailed analysis of the structure of crimes in the sphere of use of electronic computers, systems and computer networks carried out based on statistical reporting for 2017, made it possible to state that, in particular, the largest share of crimes in the sphere of use of electronic computers, systems, computer networks and telecommunication networks is represented by those the responsibility for which is stipulated by Article 361 of the Criminal Code of Ukraine — unauthorized interference with operation of electronic computers, automated systems, computer networks or telecommunication networks (69,8 %). The last place is taken by crimes provided by Article 363-1: interference with operation of electronic computers, automated systems, computer networks or telecommunication networks by mass messaging (0,1 %).

During 2018, 6,000 crimes committed in the sphere of use of high information technologies were detected. At the same time, the most of them were in the sphere of e-commerce (Fig. 3).

The analysis of information on persons who committed crimes in the sphere of use of electronic computers (according to completed investigations in criminal proceedings), based on data of 2017, made it possible to create the "profile" of a cybercriminal. The main part is the persons aged from 18 to 39 years with complete higher and basic higher education that confirms their high qualification level.

According to data of 2018, more than 800 people involved in crimes in the sphere of high information technology were identified. According to statistics, most suspects are men aged 25 to 40 (Table 2).

The investigation of the revealed cybercrimes by articles allowed to state that their main part was committed under Article 190 of the Criminal Code of Ukraine (Table 3).

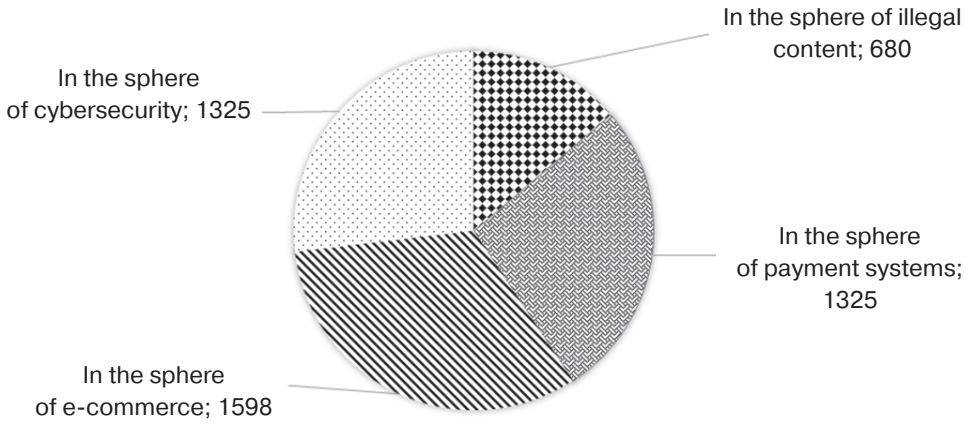

Fig. 3. **Structure of crimes detected in the sphere of high information technologies (2018)**, pcs

Source: compiled according to [5]

Table 2

Distribution of cybercriminals by sex, % (according to data of 2018) [5]

Age	Men	Women
Total, of them:	67	33
Up to 25 years	13	6
25–40c years	39	20
40 and more	15	7

Table 3

Distribution of cybercriminals by gender and articles [5]

	Article of the Criminal Code of Ukraine			
	176	**190**	**361**	**361-1**
Total persons, of them:	37	1019	505	55
men, %	97	67	92	95
women, %	3	33	8	5

The analysis of structure of cybercrimes by species indicates that, at the same time, most users of malware who committed crimes using viruses acquired in DarkNet (Figure 4) were detected in the sphere of cybersecurity.

It should be noted that in order to detect cybercrimes, the Ukrainian cyberpolice develops and introduces modern methods of detection, fixation and examination of digital evidence in practical activities. In particular, during 2018, 5.5 petabytes of information, which was further identified as digital evidence, was examined and analyzed by specialists of cyberpolice. As a result of international cooperation in 2018, 8 transnational hacker groups were revealed and more than 30 international operations were assisted.

In addition, in 2018 the agreements on anti-cybercrime cooperation with

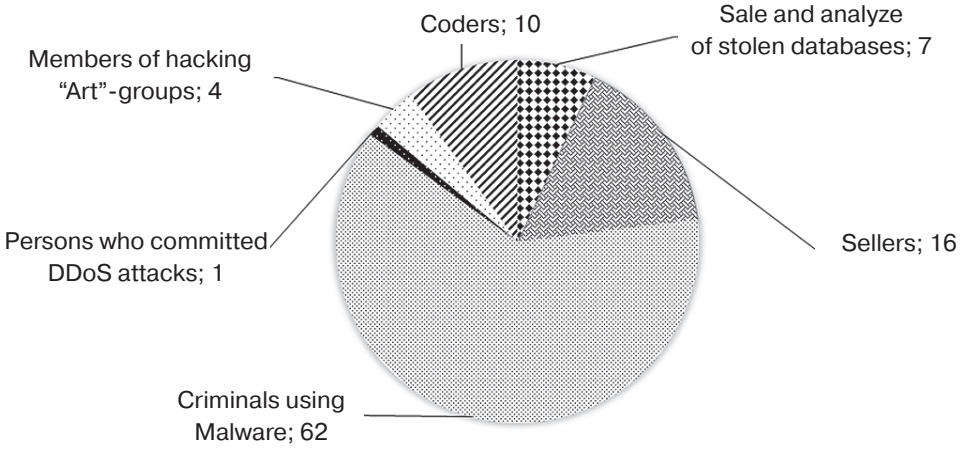

Fig. 4. **Structure of detected cybercrimes by species (according to data of 2018)**, %
Source: compiled according to [5]

organizations of state and private sector were signed. Among them are representatives of international companies in the sphere of information security and IT companies, police of Australia, Singapore, Qatar and other countries. In addition, the effective interaction with the world's most famous social networks was established.

Conclusions and perspectives of further studies. The growth of informatization in the world both opens up new ways for further world development, and promotes emergence of new threats, such as, in particular, cyberattacks. At the same time, the role of the state and corresponding state regulation in solving this problem also grows, considering that the policy of national security, sustainable development, digitization of economy, etc. is determined by the state itself. The analysis showed that the number of cybercrimes in Ukraine grows at high rates, while the law enforcement system was technically not ready for their prevention. Thus, the problem of attracting and optimizing the technical, financial and organizational and managerial resources necessary for effective overcoming cybercrimes in Ukraine today becomes one of the main tasks of the state policy for ensuring cybersecurity and is an integral part of the national security policy. In further studies it is expedient to substantiate the relevant mechanisms of the state policy for ensuring cybersecurity in Ukraine.

REFERENCES

1. Growing pains: 2018 Global CEO Outlook. (2019). kpmg.com. Retrieved from https://home.kpmg/qm/en/home/insights/2018/05/growing-pains-2018-global-ceo-outlook.html [in English].
2. Norton Cyber Security Insights Report. Global Results 2017. (2018). www.symantec.com. Retrieved from https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf [in English].
3. *Karmazina O. O.* (Eds.). (2016). Vykorystannia informatsiino-komunikatsiinykh tekhnolohii na pidpryiemstvakh Ukrainy [Use of information and communication technologies in Ukraine]. Kyiv : Derzhavna sluzhba statystyky Ukrainy. Retrieved from https://ukrstat.org/uk/druk/publicat/kat_u/2016/bl/07/bl_vikt_15pdf.zip [in Ukrainian].
4. *Kravtsova M. O.* (2018). Suchasnyi stan i napriamy protydii kiberzlochynnosti v Ukraini [The current state and strain the counteraction to cybercrime in Ukraine]. Visnyk kryminolohichnoi asotsiatsii Ukrainy – Bulletin of the Criminological Association of Ukraine, 2(19), 155-166. Retrieved from http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y [in Ukrainian].
5. Pidsumky 2018 roku v tsyfrakh [Summary of the Year 2018 In Figures]. cyberpolice.gov.ua. Retrieved from https://cyberpolice.gov.ua/results/2018/ [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Growing pains 2018 Global CEO Outlook, KPMG International. URL: kpmg.com/CEOoutlook

2. Norton Cyber Security Insights Report 2017 Global Results 2017. URL: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
3. Використання інформаційно-комунікаційних технологій на підприємствах України: статистичний бюлетень / відп. за вип. О. О. Кармазіна. — Київ : Держ. служба статистики України, 2015–2018. URL: http://www.ukrstat.gov.ua/
4. *Кравцова М. О.* Сучасний стан і напрями протидії кіберзлочинності в Україні // Вісн. кримінологічної асоціації України. — 2018. — № 2 (19). — С. 155–166. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y
5. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/