UDC 004.63
DOI: 10.31891/CSIT-2021-3-8

SERGIY TKALICHENKO, VALENTYNA KHOTSKINA, VICTORIA SOLOVIEVA
State University of Economics and Technology

CYBERCRIME: THE COMPARATIVE ANALYSIS OF THE MODERN INFORMATION SPACE

The burning problem of modern society - cybercrime, was considered in the article. In the process of studying cybercrimes and the mechanisms of protection against information security threats, the concept of cybercrime classification was carried out. The comparative analysis between the number of registered cyberattacks and losses from them was performed. The analysis of factual data was carried out, on the basis of which the table of cyberattacks quantity indicators, general losses was developed, and the cost of cyberattacks was calculated. The study provides recommendations for improving the reliability of information protection.

Keywords: ICT - information and communication technologies, information security, cybersecurity, cyberattack, neural networks.

СЕРГІЙ ТКАЛІЧЕНКО, ВАЛЕНТИНА ХОЦКІНА, ВІКТОРІЯ СОЛОВЙОВА
Державний університет економіки і технологій, Кривий Ріг, Україна

КІБЕРЗЛОЧИННІСТЬ: ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Міжнародними експертами з кібербезпеки Cybersecurity Ventures підраховано, що в 2019 році в світі кібератаки відбуваються кожні 14 секунд. У звіті говориться про те, що через хакерів світова економіка втратила не менше $ 1 трлн, або трохи більше 1% глобального ВВП, що складає більше ніж на 50% порівняно з 2018 роком. Тому актуальність теми попередження, обліку, аналізу та своєчасного реагування на такого виду виклики безсумнівна.

У процесі вивчення кіберзлочинів та механізмів захисту від загроз інформаційної безпеки здійснено класифікацію поняття кіберзлочин. Проведено порівняльну характеристику між кількістю зареєстрованих кібератак та збитками від них. Здійснено аналіз фактичних даних, на основі чого розроблено таблицю показників кількості кібератак, загальних збитків, та розраховано вартість кібератак, а також побудовано регресійну модель росту такої вартості. Виявлено категорії кіберзлочинів, які найбільш динамічно розвиваються останніми роками та структурний аналіз впливу кіберкриміналу на галузі соціальної та економічної сфери.

В дослідженні використані статистичні методи аналізу динаміки росту кількості кіберзлочинів, метод агрегатних індексів для виявлення питомої ваги кількості злочинів та їх вартості в загальних втратах. У межах дослідження надано рекомендації для підвищення надійності захисту інформації. Запропоновано більш сучасний та перспективний підхід до прогнозування та аналізу стану кіберзлочинності на основі сучасних математичних моделей, зокрема на основі штучної нейронної мережі прямого поширення.

Ключові слова: ІКТ – інформаційно-комунікаційні технології, інформаційна безпека, кібербезпека, кібератака, нейронні мережі.

Introduction

The rapid development of global information and communication technologies, which we have observed over the past two decades, is accompanied by the dynamic development of crime in this sphere. This development brings a new type of negative phenomena into our lives - cybercrime. Cyber criminality, in addition to its specific criminal activities, has provided new opportunities for traditional crimes and creates conditions for the implementation of fundamentally new schemes and methods of criminal activity. With the help of Darknet, criminals have effectively created a black market for drugs, weapons, stolen goods, etc.

The growing provision of cyber criminality with modern computers, telephone communication means with access to networks, specific software poses a threat not only to ordinary citizens in particular, but also to the national security of the state in general.

The analysis of recent research and publications

Nowadays, in the age of informatization, it is becoming more important to clarify the problem of cybercrime from the standpoint of the threat to the modern information society. Accordingly, it is necessary to build an effective system of cyber security at the state level.

The materials for research on cybersecurity issues are presented in the European cybercrime center [19], Norton Cybercrime Report, SecureWorks Cybercrime, FBI IC3Report, Globalstudy.bsa.org and other sources.

The effectiveness of the fight against cybercrime lies primarily in the presence of the appropriate harmonized legislative bases of the leading European countries and, accordingly, the availability of information security specialists. Adaptation of the fight against cybercrime according to international standards is characterized by introduction ISO / IEC 15408 standard [1].

Various aspects of the problem are highlighted in the works of the leading experts: the study of the information security international experience [2, 3, 4]; cybersecurity and protection of Ukraine’s information space [5, 6, 7, 8]; information security audit [9]; hybrid aggressive threats [10, 11]; cybercrime prevention [12, 13, 14, 15]; protection of crucial infrastructure objects [16]; the spread of cybercrime in various fields (databases protection, banking protection, intellectual property protection, protection against pornography, electronic fraud, etc. [17].

The problem statement

The state of computer or cybercrime is significantly affected by the rapid development of information technology and the expansion of their scope. According to OSCE experts, cybercrime involving the use of information technologies, computer systems and networks can create chaos that is close in scale to the economic crisis [30]. The scale and the level of socially dangerous consequences of cybercrime necessitate the introduction of adequate approaches to improve the criminal legislation against cybercrime.

Presentation of the main material

Cybersecurity means protection of vital interests of the man, a society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace [1].

In the scientific literature there is a significant number of definitions of "cyber threat", "cybercrime", "cyber-attack". But the most fully these terms are defined in the International Standard electronic resource [1].

The most serious cybercrimes according to this classification are the crimes against the state and strategic objects. To confirm the above, we present the following data for 2014-2017 [4]: DDoS-attacks and hacking of the CEC website during the presidential election, as a result of which erroneous results appeared on the website (2014); cyber espionage malware (Turla / Uroburos /Snake,RedOctober, MiniDuke and NetTraveler) (2014); disconnection of about 30 substations of Prykarpattiaoblenerho, in connection with which more than 200,000 residents of Ivano-Frankivsk region were left without electricity for the period from one to five hours. At the same time, attacks on Kyivoblenerho and Chernivtsioblenerho took place (2015); "Hacker attack" on the internal telecommunications networks of the Ministry of Finance, the State Treasury, the Pension Fund. This damaged computers and destroyed critical databases, which caused delaying budget payments at UAH hundreds of millions (2015); DDOS-attack on the Ukrzaliznytsia website, which resulted blocking completely its work during the day. The attack was aimed at passenger traffic data theft (2016); A cyberattack on the Ukrenergo "North" substation led to a failure in the control automation, due to which the districts of the northern part of the right-bank Kyiv and the adjacent districts of the Region remained without power supply for more than an hour (2016).

The year 2017 became even more dangerous for Ukraine. An attack has been launched on the Ukrainian public and commercial sectors using the Petya Ransomware malware file encryption virus.

The Ukrainian agencies and companies turned out unprepared. A large number of critical infrastructure facilities were affected: the Government of Ukraine, the Chornobyl NPP, Ukrposhta, the Kyiv Metro, Boryspil International Airport, and many media outlets, banks, and commercial entities. Besides our state, there is a number of countries that have suffered at most from this attack: Italy, Israel, Serbia, Hungary, Romania, Poland, Argentina, the Czech Republic and Germany. Only crimes that can be called as crimes against the state and that cause enormous losses are listed here.

Table 1 and Figure 1 represent the dynamics of cybercrime growth according to the statistics of the Internet Crime Complaint Center [20, 21, 22, 23, 24].

Table 1

Dynamics of losses growth caused by cybercrimes

Year	Losses, $ million	Absolute chain growth, $ million	Year	Losses, $ million	Absolute chain growth, $ million
2001	17,8	0	2011	485,2	-78
2002	54	36,2	2012	581,4	96,2
2003	125,6	71,6	2013	781,8	200,4
2004	68,1	-57,5	2014	800,4	18,6
2005	183,1	115	2015	1070,7	270,3
2006	198,4	15,3	2016	1450,7	380
2007	239,1	40,7	2017	1418,7	-32
2008	264,6	25,5	2018	2710	1291,3
2009	559,7	295,1	2019	3500	790
2010	563,2	3,5	2020	4500	1000

Here are some examples of cyber incidents in recent years [18]. In January 2019, an archive containing about 773 million unique email addresses and 22 million passwords collected from various sources was discovered in the MEGA cloud service. Collection # 1, the array that stored the data, included 12,000 files of 87 GB data. In the same month, the 845 GB Collection # 2-5 archive, which included 25 billion records, appeared on hacker forums.

In 2020, through the fault of the third-party software developers, 540 million records with data from Facebook users, including comments, preferences, logins, and IDs, were merged into the network.

In October 2019, WhatsApp sued the NSO Group (software developer) for allowing Israeli intelligence to "hack" the phones of more than 1,400 users throughout the world, including diplomats, oppositionists, and journalists.

In the same year, an unsecured MongoDB server was detected in the network, which stored a 4.1 GB database called "GNCTD". The archive contained confidential information about 458,388 residents of Delhi.

A 4TB database and 1.2 billion records have been made public, including data from the profiles of hundreds of millions of Facebook, Twitter, LinkedIn and GitHub users, including 50 million phone numbers, 622 million email addresses and employment history.

Google was noted for the scandal. It turned out that they, along with other companies, were running a secret project - the collection and analysis of medical data of millions of Americans.

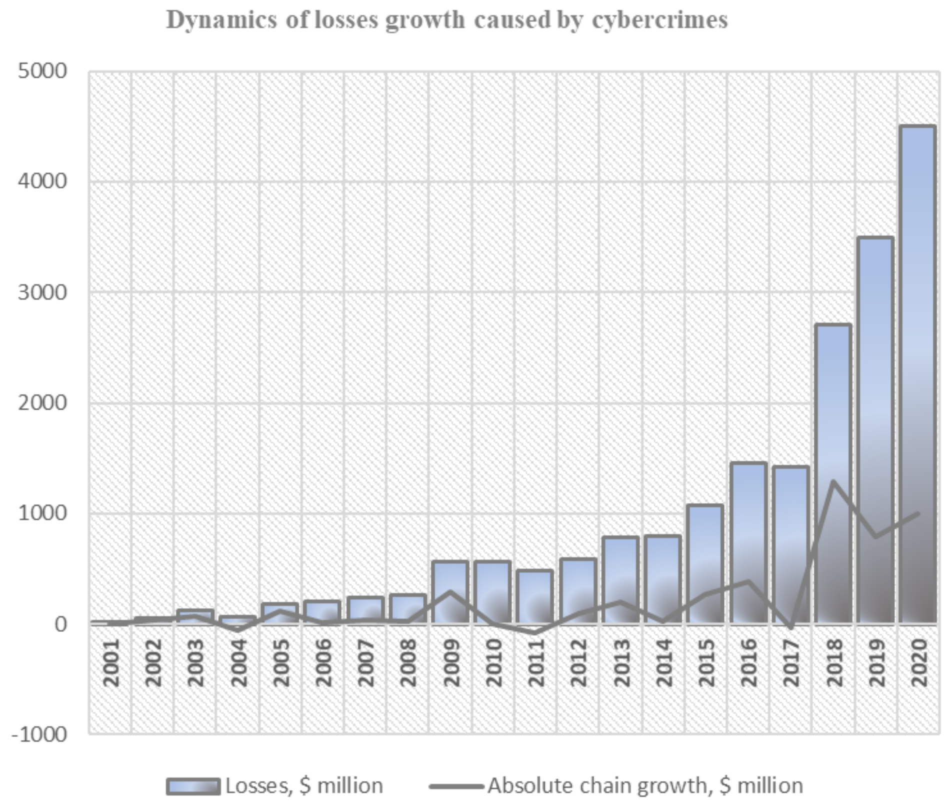


Fig.1. Dynamics of losses growth caused by cybercrimes

Among the incidents directly related to the financial and industrial spheres, the most well-known is the Norsk Hydro ASA shutdown, a Norwegian oil and gas and metallurgical company, due to the LockerGoga attack. The Company’s losses from the incident were estimated at about $ 35-41 million and the "hacking" (for the third time in three years) of the South Korean exchange Bithumb, which lost about $ 20 million in cryptocurrency, and in May 2019 cryptocurrency exchange Binance: hackers hacked " hot "wallet service and brought out more than 7,000 bitcoins (about $ 41 million).

It should be noted, that in addition to the increase in both the number and total losses, the cost of cyberattacks has increased significantly (Table 2 and Fig. 2): from $ 2,971.2 in 2014 to $ 7,689.2 in 2018.

Table 2

Correlation of cyberattacks and total losses

Year	Losses, $ million	Cyberattacks number	One cyberattack cost, $
2014	800,500	269422	2971,18
2015	1070,700	288012	3717,55
2016	1450,700	298728	4856,26
2017	1418,700	301580	4704,22
2018	2706,400	351973	7689,23
2019	35000,000	467361	74888,58
2020	45000,000	791790	56833,25

To effectively combat cybercrimes, it is necessary to segment their demonstrations and identify the crimes that need to be primarily paid attention to in order to create an appropriate method of combating them. Table 3 represents the most dynamic types of such violations, which were identified by the method of index analysis in recent years according to the data given in [19].

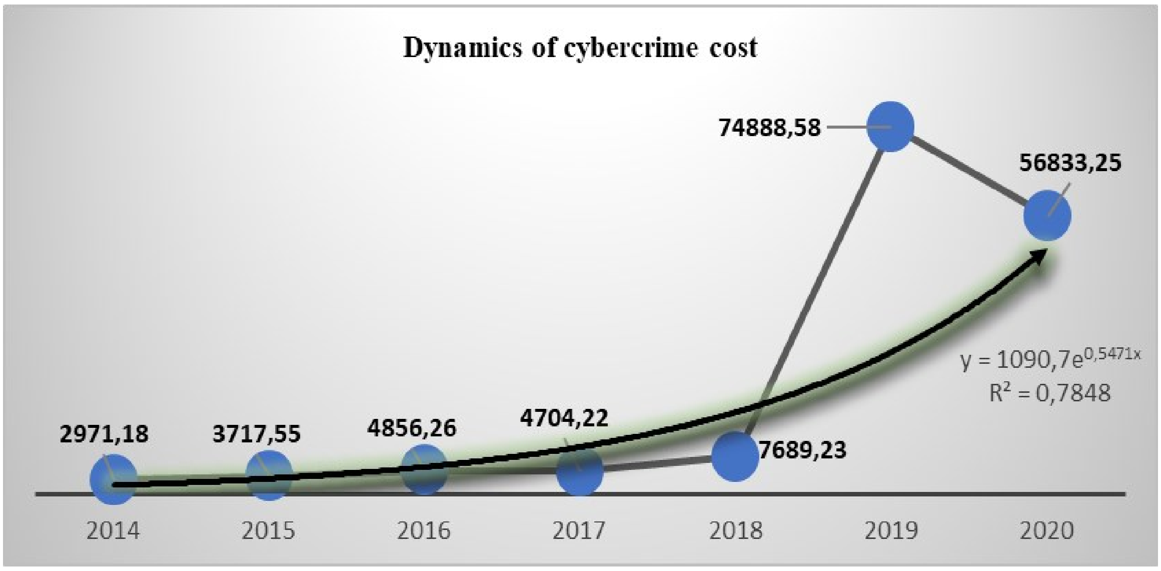


Fig.2. Dynamics of growth of cost of one cybercrime, $.

As we can see, most crimes involve the use of personal data.

At present, all key "classic" cybercrimes committed with the help of computer and telecommunication technologies, the number of which is growing every year, are available in Ukraine at full.

Table 3

Indices of the most dynamic quantitative types of cybercrime

Cybercrime types	Average index
Fraud inquiring personal data	2,230
Counterfeiting of goods and services	1,656
Lottery/Sweepstakes	1,390
Fraud in the sphere of medicine	1,293
Hacking emails, accounts, etc.	1,257
Abuse of investor confidence	1,228
Violation of personal data confidentiality	1,171
Computer blocking with attacks	1,159
Abuse of trust	1,106
Crimes based on technical support with remote access	1,090

As many as 4263 cybercrime cases [25] were registered in Ukraine in 2019. The losses amounted to UAH 28 million, of which UAH 17 million were reimbursed. That is, compared to European statistics, these figures seem unreliable. This is primarily due to the lack of skilled officials in the executive branch, enterprises and organizations that need the necessary protection.

The Cyber Police, as a structural subdivision of the National Police, was established quite recently on October 5, 2015.

During 2018, the cyber police of Ukraine detained the organizer of the Avalanche bot network, exposed a member of the international hacker group Cobalt, took part in the termination of the international hacking group FIN7, prevention of four mass cyberattacks in Ukraine. They exposed 8 transnational hacker groups and participated in more than 30 international operations within the framework of international cooperation [26].

The Anti-Crisis Center for Cyber Business Protection at the Chamber of Commerce and Industry of Ukraine proposed to the Ministry of Education and Science that each school year should begin with lessons on cyber hygiene [27]. The Cyber Police has launched a cybersecurity awareness campaign [28]. The activity of the Cyber Police is growing from year to year and the results of the work are reported at professional conferences.

And if the work of the cyber police aimed at combating the crimes that threaten the state, especially in a hybrid war, can be considered satisfactory, in any case, the information about the results of such work can be found in the net, (the information about) the crimes against ordinary citizens remains at the initial level. The general situation of cybercrime in Ukraine repeats the European trends with some delay.

Therefore, with some accuracy we can apply the structural analysis (Table 4) of cybercrimes against citizens [29] by using personal data to identify weak points in the protection system and forecasting the development of cybercrime in our country.

Therefore, promising, in our opinion, is a scientific approach to forecasting and analyzing the state of cybercrime based on modern mathematical models.

Table 4

Percentage distribution of cybercrimes by using personal data.

Branches	Malware usage	Social engineering	Account data selection	Hacking	WEB vulnerabilities usage	Others
Public organizations	15,83	16,27	8,62	12,89	25,42	28,24
Finance sector	8,02	9,26	1,72	2,58	0,56	7,06
Industrial companies	11,51	13,14	2,59	5,15	2,82	4,71
Medical institutions	4,83	5,88	12,93	2,06	1,69	2,35
Online services	0,51	0,25	6,03	2,58	12,99	12,94
Service industries	3,19	1,13	7,76	2,06	4,52	0,00
IT-companies	3,49	2,50	9,48	6,70	5,08	8,24
Science and education	6,37	6,88	7,76	4,64	5,08	2,35
Trade	1,95	1,88	2,59	1,03	15,25	0,00
Telecommunication companies	0,82	0,75	1,72	0,52	1,69	4,71
Transport	1,13	1,38	0,86	0,52	1,13	0,00
Block-chain	0,41	0,50	2,59	7,22	1,13	2,35
Others	3,80	3,75	5,17	1,55	5,65	5,88
Without reference to the industry	20,76	13,39	16,38	37,63	14,12	12,94
Private individuals	17,37	23,03	13,79	12,89	2,82	8,24

For example, the quality of the approximation of the malware distribution use, even visually applying the Least Squares Method [LSM] and using neural networks, differs significantly. (Fig.3, Fig.4).

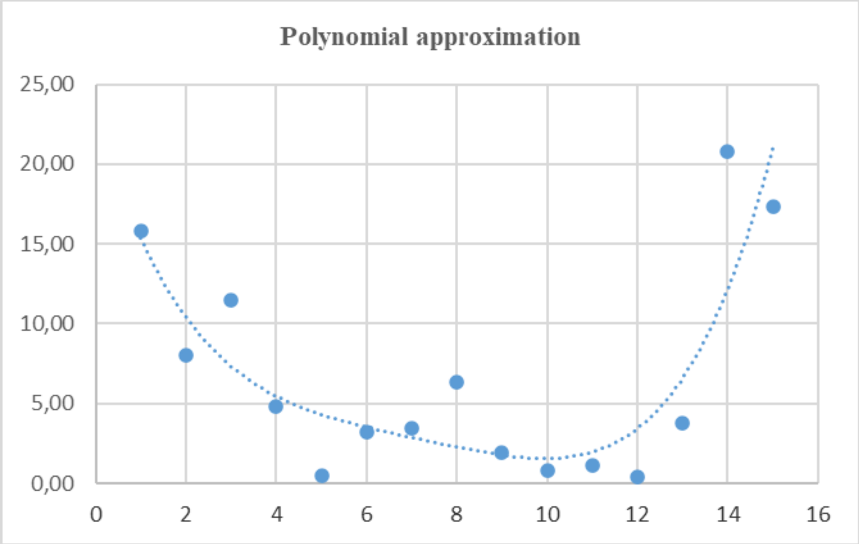
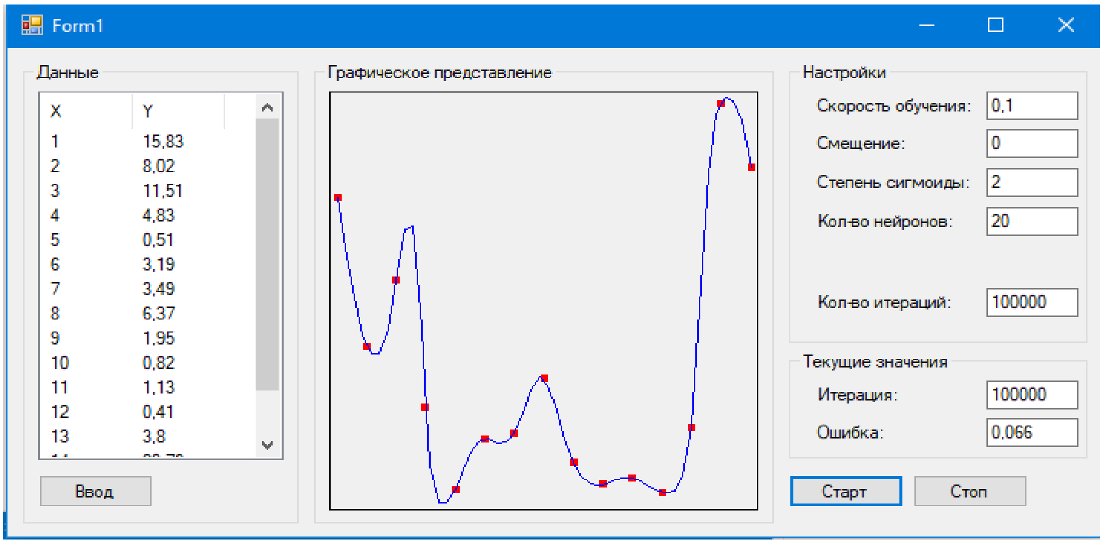


Fig.3. Approximation of the malware distribution use with the help of the Least Squares Method



X	Y
1	15,83
2	8,02
3	11,51
4	4,83
5	0,51
6	3,19
7	3,49
8	6,37
9	1,95
10	0,82
11	1,13
12	0,41
13	3,8

Скорость обучения: 0,1
Смещение: 0
Степень сигмоиды: 2
Кол-во нейронов: 20
Кол-во итераций: 100000

Итерация: 100000
Ошибка: 0,066

Fig.4. Approximation of the malware distribution use with the help of artificial direct distribution neural network (hidden layer 20 neurons, learning 100,000 iterations, learning speed 0.1)

Conclusions

Today, cybercrime is a real global threat that can spread from any country in the world beyond a specific jurisdiction (unlike other traditional types of economic crimes). The introduction of digital technologies at enterprises and in all spheres of activity requires the involvement of information technology (IT) security professionals to protect information. The issues of the information space protection, counteraction of information weapons, development of the information struggle strategy are at the stage of formation and need thorough scientific provision and support.

REFERENCES

1. International Standart – [Electronic Resource]. – Access Mode: ISO/IEChttp://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

2. Gavrylovsky D. To the Problem of Counter-Action to the Use of Harmful Software / D. Gavrylovsky//Struggle with Organized Criminality and Corruption (Theory and Practice). – 2014. – № 1. –P. 125–130.

3. Orlov O.V. State Government of Professionals' Training in the Sphere of Cyber-Security / O.V. Orlov//State Construction. – [Electronic Resource]. – Access Mode: http://kbuapa.kharkov.ua.

4. International experience of information security / KK Zakharenko // Modern society. - 2019. - Vip. 1. - P. 95-109. - Access mode: http://nbuv.gov.ua/UJRN/cuc_2019_1_11

5. Buryachok V.L. Formation's Bases of Cybernetic Security's State System: Monograph/V.L. Buryachok. – K.: NAS, 2013. – 432 p.

6. Gnatyuk S.O. Cyber-Terrorism: History of Development, Modern Tendencies and Counter-Measures/S.O. Gnatyuk //Security of Information. – 2013. – V. 19. – №2. – P. 118–129.

7. Korchenko O.G. Cybernetic Security of State: Characteristic Features and Problem Aspects / O.G. Korchenko, V.L. Buryachok, S.O. Gnatyuk//Security of Information. – 2013. – V. 19. – № 1. – P. 40–45.

8. Butuzov V.M. Counter-Action to Computer Criminality in Ukraine (the System-Structural Analysis): Monograph/V.M. Butuzov. – K.: KIT, 2010. – 145 p.

9. Audit of Information Security: Texbook/V.A. Romaka, A.E. Lagun, Yu.R. Garasym and oth.; State Service of Ukraine on Extraordinary Situations: Lviv State University of Life Activity's Safety, NAS of Ukraine, Institute of Applied Problems of Mechanics and Mathematics, named after Ya.S. Pidstryhach. – Lviv: Spolom, 2015. – 363 p.

10. Dubov D.V. Cyber-Space as New Measure of Geo-Political Rivalry: Monograph/D.V. Dubov. – K.: NISR, 2014. – 328 p.

11. Dubov D.V. Cyber-Security: World Tendencies and Challenges for Ukraine. Analytical Report / D.V. Dubov, M.A. Ozhevan. – K.: NISR, 2011. – 30 p.

12. Kravtsova M.O. Prevention of Cyber-Criminality in Ukraine: Monograph/M.O. Kravtsova, O.M. Lytvynov; gen, edit of Dr.of Jurid Sc., prof. O.M. Lytvynov]. – Kharkiv: Panov, 2016.

13. Buryachok V.L. Cybernetic Security – Main Factor of Stable Development of Modern Information Society/A.L. Buryachok//Modern Special Engineering: col. of sc.works. – 2011. – № 3 (26). – P. 104–114.

14. Melnyk S.V. Actual Directions of Violations' Warning in Cyber-Space as Strategy's Component of State's Cybernetic Security. Information Security: Challenges and Threats of Modernity: col. of materials of sc.-pr. conf., April, 5, 2013, Kyiv/S.V. Melnyk, V.I. Kaschuk. – K.: NPC NA SS of Ukraine, 2013. – 416 p.

15. Diorditsa I.V. Notion and Contents of Cyber-Security's National System/I.V. Diorditsa. – [Electronic Resource]. – Access Mode: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

16. Honchar S.F. Methodological Bases of Elaboration and Introduction of Information Protection's Systems in Objects of Critical Infrastructure/S.F. Honchar, G.P. Leonenko, O.Yu. Yudin//Special Telecommunication Systems and Protection of Information. – 2014. – № 1 (25). – P. 158–163.

17. Control of Struggle with Cyber-Criminality//Ministry of Internal Affairs of Ukraine [Electronic Resource]. – Access Mode: http://mvs.gov.ua/mvs/control/main/uk/ publish/article/544754

18. Sergiy Tkalichenko, Valentyna Khotskina, Zhanna Tsymbal. Cyber-criminality: protection's aspects of modern information space//– Advances in Economics, Business and Management Research, – 2020. Vol. 129. – P. 137–143. DOI: 10.2991/aebmr.k.200318.017

19. Sergiy Tkalichenko, Valentyna Khotskina, Zhanna Tsymbal, Victoria Solovieva, and Olena Burunova. Modern Structural Level and Dynamics of Crimes with The Use of Computers, Automation Systems, Computer Networks and Electric Connection Systems. SHS Web of Conferences. 2021. Vol. 100, 01014 https://doi.org/10.1051/shsconf/202110001014

20. Analysis of the regulatory impact of the Draft of the Resolution of Cabinet of Ministers of Ukraine "Some Issues of Carrying out Information Security Independent Audit at the Critical Infrastructure Objects" (State Service of Special Communication and Information Protection). – 2019, URL. [Electronic Resource]. – Access Mode: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=E831D6013C22A4DDC83EB35EEA63A152.app1?showHidden=1&art_id=314821&cat_id=38837&ctime=1576485095838 (Access date: 31.01.2021).

21. Internet Crime Report 2020//FBI's Internet Crime Complaint Center (IC3)//URL: https://pdf.ic3.gov/2017_IC3Report.pdf/ (Access date: 31.01.2021).

22. Internet Crime Report 2017//FBI's Internet Crime Complaint Center (IC3)//URL: https://pdf.ic3.gov/2017_IC3Report.pdf/ (Access date: 31.01.2021).

23. Internet Crime Report 2013//FBI's Internet Crime Complaint Center (IC3)//URL: https://pdf.ic3.gov/2013_IC3Report.pdf/ (Access date: 31.01.2021).

24. Internet Crime Report 2019//FBI's Internet Crime Complaint Center (IC3)//URL: https://pdf.ic3.gov/2019_IC3Report.pdf/ (Access date: 31.01.2021).

25. The REPORT of the Head of the National Police of Ukraine on the results of the work of the department in 2019//URL: [Electronic Resource]. – Access Mode: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu- 2019.pdf/ (Access date: 31.01.2021).

26. The Report of the Head of the National Police of Ukraine S. Knyazev "On the results of the department for 2018". - National Academy of Internal Affairs. - Access mode: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf (Access date: 03.01.2020).

27. Ukraine will increase the staff of special agents to combat cyber fraud//URL: [Electronic Resource]. – Access Mode: https://www.ukrinform.ua/rubric-economy/2805152-v-ukraini-zbilsit-stat-specagentiv-dla-protidii-kibersahrajstvu.html (Access date: 31.01.2021).

28. Cyber Police launched a campaign to raise awareness about cybersecurity//Unified portal of the system of the Ministry of Internal Affairs of Ukraine//URL: [Electronic Resource]. – Access Mode: https://mvs.gov.ua/ua/news/18914_Kiberpoliciya_zapustila_kampaniyu_z_obiznanosti_pro_kiberbezpeku.htm (Access date: 31.01.2021).

29. Internet Crime Report 2013//FBI's Internet Crime Complaint Center (IC3)//URL: [Electronic Resource]. – Access Mode: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf/ (Access date: 31.01.2021).

30. Problems of legal and expert support of law enforcement activity in the field of combating cybercrime. - National Academy of Internal Affairs. - Access mode: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf (Access date: 03.01.2020).

Sergiy Tkalichenko **Сергій Ткаліченко**	PhD, Associate Professor of the Department of Informatics and Applied Software, State University of Economics and Technology, Kryvyi Rih, Ukraine e-mail: tsw1966@ukr.net https://orcid.org/0000-0002-1798-8073	кандидат економічних наук, доцент кафедри інформатики та прикладного програмного забезпечення, Державний університет економіки і технологій, Кривий Ріг, Україна.
Valentyna Khotskina **Валентина Хоцкіна**	PhD, Associate Professor of the Department of Informatics and Applied Software, State University of Economics and Technology, Kryvyi Rih, Ukraine e-mail: khotskina_vb@ukr.net https://orcid.org/0000-0001-8963-4189 Scopus Author ID: 56258837100	кандидат технічних наук, доцент кафедри інформатики та прикладного програмного забезпечення, Державний університет економіки і технологій, Кривий Ріг, Україна.
Victoria Solovieva **Вікторія Соловйова**	PhD, Associate Professor, Head of the Department of Information Technologies and Modeling, State University of Economics and Technology, Kryvyi Rih, Ukraine e-mail: vikasolovieva2027@gmail.com https://orcid.org/0000-0002-8090-9569 Scopus Author ID: 57210109157 https://scholar.google.com/citations?user=y7IlJGUAAAAJ&hl=uk&oi=ao https://dblp.org/pid/249/5121.html	кандидат економічних наук, доцент, завідувач кафедри інформаційних технологій і моделювання, Державний університет економіки і технологій, Кривий Ріг, Україна.