Modern Structural Level and Dynamics of Crimes with The Use of Computers, Automation Systems, Computer Networks and Electric Connection Systems

Sergiy Tkalichenko[1], *Valentyna* Khotskina[1*], *Zhanna* Tsymbal[1], *Victoria* Solovieva[1], and *Olena* Burunova[2]

[1]State University of Economics and Technology, Kryvyi Rih, Ukraine
[2]Science and Business Center ZAK, 96100, Poland

Abstract. Actuality of surveillance the cyber-criminality problem and its impact upon a society is proved out by the rapid increase in a quantity of such crimes and material losses accordingly. The statistical analysis of their number increases and the caused losses is made in the process of cybercrimes studying. It's revealed that besides the catastrophic number growth of such crimes, the relative size of losses is increased too. The analysis of the actual data for the nine years is made, on which basis the indicators' table of the cyber-attacks number, the general losses and the indexes of their dynamics is elaborated. The analysis of the struggle's state with cyber-criminality in our state is made. The recommendations are presented in the limits of the research for the increase of the information protection's reliability.

1 Introduction

The rapid development of the world information-communication technologies, being observed for the last two decades, is accompanied by the dynamic development of crimes in this field. Such development brings the negative phenomena of the new type – cyber-criminality – into our life. Besides the crimes, being specific for it, the cyber-crime presented the new possibilities of the traditional crimes' commitment and creates conditions for the realization of the principally new schemes and methods of the criminal activity. The criminals actually created the black market for the sale of drugs, weapon, the stolen goods, etc. with the help of the Darknet system.

The growth of the cybercrime's provision with the modern computing engineering, the means of the telephone communication with the access to the networks, the specific software form the threat not only for the crossing citizens in particular, but for the national security of the state in general.

2 Background

At present, in the times of information technologies, the identification of the cyber-criminality problem is gaining actuality. Correspondingly, it's necessary to construct the operating system of the cybernetics security guarantee at the state level.

The research materials of the cybersecurity problems are presented in the European Cybercrime Center [12], Norton Cybercrime Report, SecureWorks Cybercrime, FBI IC3Report, Globalstudy.bsa.org and the other sources.

To increase fighting efficiency related to such crimes, it is necessary to synchronize Ukraine's legislation with legislation of the countries, which have achieved considerable successes in combating cyber-criminality. The international rules introduced by ISO/IES 15408 standard, should be implemented into the state's legislation [1].

The different aspects of the problem are lighted up in the works of the leading professionals: the study of the international experience of information security [2, 3]; the information security's audit [4]; the hybrid aggressive threats [5]; the prevention of cyber-criminality [6, 7, 8]; the protection of the critical infrastructure objects [9]; widening of cyber-criminality in different branches (the protection of the data base, banking protection, the protection of the intellectual ownership, the protection from the pornography, electronic swindling, etc.) [10].

2.1 Problem Positing

The EU Commission presented the new Strategy of the EU Security Union on July, 24, 2020 with an emphasis on the protection of the critical infrastructure, the struggle with cyber-criminality, the opposition to the hybrid threats and the organized criminality. Such strategy has become the continuation of the complex measures of the previous years: the first European security strategy of 2003, the European agenda on security of 2015, the Global EU strategy of 2016, where the significant attention was paid to the problems of security.

The domestic realities of the cybersecurity sphere testify to a series of the important problems, preventing from the creation of the efficiently operating system of

*Corresponding author: khotskina_vb@ukr.net

opposition to the threats in the cyberspace. The following ones belong to such problems in the first turn: the terminological uncertainty, the absence of the proper coordination of activity of the corresponding government departments, the Ukraine's dependence on the program and the engineering products of foreign origin, the difficulties with the staff complement of the corresponding structural subdivisions [13]. The official statistics reflects not only the state of the criminality, but the state of its registration in the country. The high delitescence of such type of crimes is observed.

That's why the modern structural level and the dynamics of crimes with the use of computers, automation systems, computer networks and the systems of the electric connection are selected as the subject of the research.

2.2 Presentation of Materials and Results

The available classifications of the notion "cybercrime" from the position of the scientific understanding are various enough.

The growth dynamics of cybercrimes, according to the statistics of the Internet Crime Complaint Center [11, 14, 15, 16, 17], is presented in the Table 1, in fig.1.

According to the calculations of the professionals, the quantity's jump of all the cybercrimes took place in 2017. After that the quantity of the cybercrimes received the tendency to the sharp rise. Thus, according to the data of the cyber-police in Ukraine, it's fixed: 1795 cases in 2017, 1023 cases – in 2018, 2826 – in 2018, already 4263 cybercrimes – in 2019. Let's present some general-world tendencies. We consider it to be opportune, if we present the analytical indicators of the investigated process (Table 2, Fig. 2).

As the visual analysis shows, the growth dynamics of the crimes' number and their cost have the different character.

Let's use the methods of the index analysis for the more detailed analysis.

$$Ipg = \frac{\sum p_1 g_1}{\sum p_0 g_0},\ Ip = \frac{\sum p_1 g_1}{\sum p_0 g_1},\ Ig = \frac{\sum p_0 g_1}{\sum p_0 g_0}$$

where p1, p0 – the average cost of one crime (current and previous period), q1, q0 – the quantity of crimes (current and previous period), Ipq – the general index of losses, Ip – the general index of losses, due to the increase of the crime's average cost, Iq – the general index of losses, due to the number increase of crimes (Table. 3, Fig. 3).

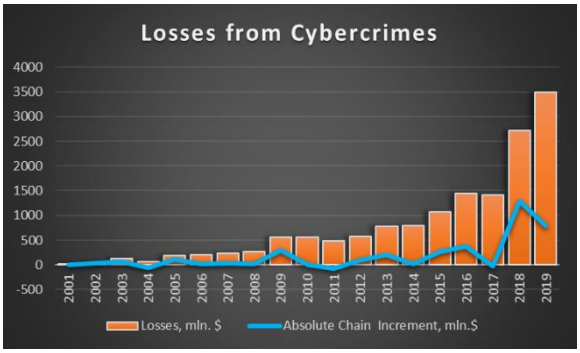

Fig. 1. Growth Dynamics of Losses from Cybercrimes

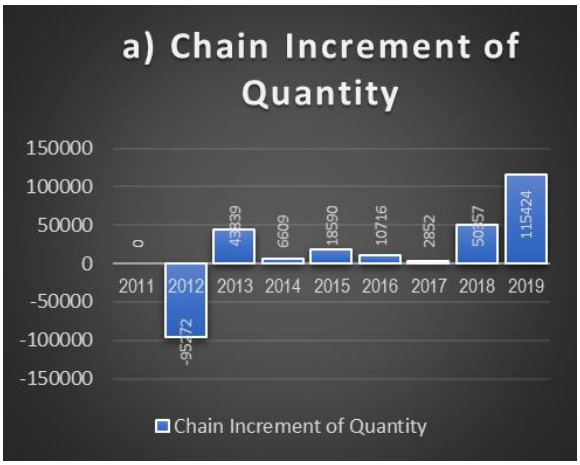

Fig. 2. Dynamics Indicators of Quantity Cybercrime (a)

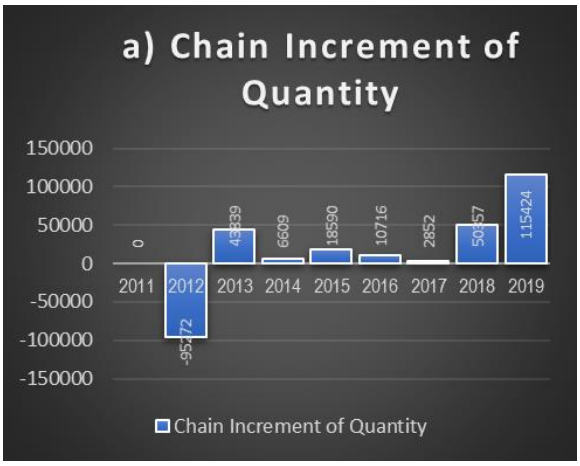

Fig. 2. Dynamics Indicators, Average Cost of One Cybercrime (b)

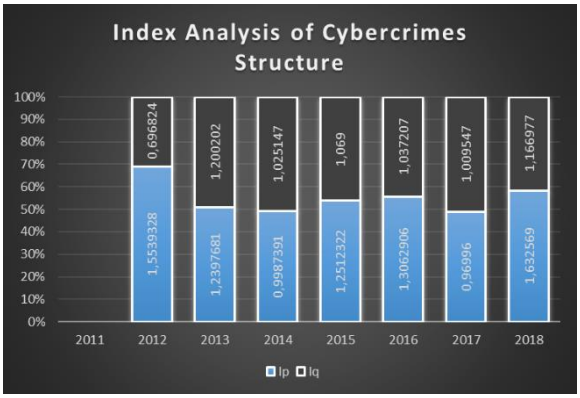

Fig. 3. Correlation of General Losses from Cybercrimes, due to Quantity and Average Cost of One Crime

Table 1. Growth Dynamics of Losses from Cybercrimes.

Year	Losses, mln. $	Absolute Chain Increment, mln. $	Year	Losses, mln. $	Absolute Chain Increment, mln. $
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			

Table 2. Dynamics Indicators of Cybercrimes' Quantity and the Average Cost of One Crime.

Year	Quantity	Losses, $	Average Losses, due to One Cybercrime	Chain Increment of Quantity	Chain Increment of Crime Price, $
2011	314246	485253871,00	1544,18	-	-
2012	218974	525441110,00	2399,56	-95272,00	855,37
2013	262813	781841611,00	2974,90	43839,00	575,34
2014	269422	800492073,00	2971,15	6609,00	-3,75
2015	288012	1070711522,00	3717,59	18590,00	746,45
2016	298728	1450700000,00	4856,26	10716,00	1138,66
2017	301580	1420555000,00	4710,38	2852,00	-145,88
2018	351937	2706400000,00	7690,01	50357,00	2979,64
2019	467361	3500000000,00	7488,86	115424,00	-201,16

Table 3. Index Analysis of Cybercrimes Structure.

Year	Quantity	Losses,$	Average Losses, due to One Cybercrime	Ip	Iq	Ipq
2011	314246	485253871	1544,18			
2012	218974	525441110	2399,56	1,5539328	0,696824	1,082817
2013	262813	781841611	2974,90	1,2397681	1,200202	1,487972
2014	269422	800492073	2971,15	0,9987391	1,025147	1,023855
2015	288012	1070711522	3717,59	1,2512322	1,069	1,337567
2016	298728	1450700000	4856,26	1,3062906	1,037207	1,354893
2017	301580	1420555000	4710,38	0,96996	1,009547	0,97922
2018	351937	2706400000	7690,01	1,632569	1,166977	1,905171
2019	467361	3500000000	7488,86	0,973842	1,327968	1,293231

Thus, the aggregate index of the general growth of losses is Ipq=1,308 (i.e., 30,8% in the average per one year). Such a growth is explained by the average increase (by 6,6%) of the crimes' quantity (Iq=1,066) and the sharp rise of the average cost of one crime – by 24% (Ip=1).

In order to fight efficiently with the cybercrimes, it's necessary to segment their demonstrations and to reveal the crimes, to which it's necessary to pay the maximal attention urgently, and to create the corresponding methods of struggle with them. The most dynamic types of the quantity of such violations, being revealed by the method of the index analysis, are represented in the Table 4.

*Corresponding author: khotskina_vb@ukr.net

Table 4. Indexes of the Most Dynamic Quantitative Types of Cybercrimes.

Type of Cybercrime	Average Index
Swindling with the Enquiry of Personal Data	2,230
Demanding of Illegal Profit by Intimidation	1,713
Forgery of Goods and Services	1,656
Lottery/Totalizator	1,390
Swindling in the Sphere of Medicine	1,293
Games of Chance	1,274
Breaking-Up of E-Mail, Accounts, etc.	1,257
Trust Abuse of Investors	1,228
Violation and Forgery of Copyrights	1,203
Confidentiality Violation of Personal Data	1,171
Computer Blocking by Attacks	1,159
Abuse on Confidence	1,106
Crimes on the Basis of Technical Support at Remote Access	1,090

The types of the cybercrimes, according to the "hardness" (which lead to the most losses) are also presented in the Table 5.

Table 5. Indexes of the Most Harmful Types of Cybercrimes.

Type of Cybercrime	Average Index
Swindling by Presenting Himself (Herself) as the State Official	2,700
Demanding of Illegal Profit by Intimidation	2,568
Swindling in the Field of Medicine	2,005
Crimes on the Basis of Technical Support at Remote Access	1,969
Terrorism	1,830
Swindling in Social Networks	1,821
Swindling with Real Estate	1,771
Computer Blocking by Attacks	1,744

All the key "classical" cybercrimes, committed with the help of the computer and the telecommunication technologies, which number grows every year, are present now in Ukraine in the whole scope.

As Oleksandr Grynchak, the first deputy head of the Ukraine cyber-police department, states, the most spread types of such actions in Ukraine are the following: the illegal access, the illegal catching, the interference into data, the abuse by devices, the swindling, connected with computers; the violations, connected with the children's pornography, etc. The swindlers create the sites and sell the not existent product more often. There are many crimes, concerning the defrauding of information from the cards and the online-crediting [18, 29].

According to [21], 4263 cybercrimes were registered in Ukraine in 2019, which caused losses for the sum of 28 mln.UHA, 17 mln.UHA of them were recompensed. The main part of such crimes is the following:

- crimes in the application sphere of computers, systems and computer networks, i.e. viruses, attacks and others – 1494;
- E-Commerce – 744;
- crimes, connected with the payment systems – 1641;
- lawless contents – 332.

The presented quantity of the revealed cybercrimes is scanty, compared with the European statistics. Let's state that the trustworthy statistics is almost absent, but the available one causes doubts.

The information of NCCC at CNSD of Ukraine [30], concerning the quantity of the cyber-incidents (Table 6), cannot but cause the amazement in the background of the insignificant number of the officially registered cybercrimes.

Table 6. Quantity of Fixed Cyber-Incidents (the 9-th of September – the 6-th of December, 2020).

Type of Cyber-Incident	Quantity
Scanning of Resources	15449264
BRUTEFORCE	4028226
Network Attacks	1184980
WEB-Attacks	1033221
Harmful Software	275981
Not-Sanctioned Access	83384
Spam	79261
HARVEST-ATTACK	18858
Exploits	2771
Fishing Attacks	813
DDOS Attacks	68

Thus, the very significant delitescence exists in the sphere of cybercrimes. The most part of cyber-incidents are not registered as crimes.

According to the data of the Ukraine's state statistics, the specific weight of the young people (aged to 30), convicted for the crimes in the application sphere of the electronic-computing machines (computers), the systems and the computer networks, was equal to the following: in 2010 – 55,1%, 2012 – 45,0%, 2013 – 36,7%, 2014 – 43,2%, 2015 – 41,9%, 2016 – 41,7%, 2017 – 40,5% [19]. To our mind, such statistics is not grounded enough. The National Agency on Struggle with Criminality (NCA) in Great Britain launched the #CyberChoices campaign for the cybercrime warning. The statistics pushed the NCA to such step: the average age of a cybercriminal reduced from 24 to 17 years old [22]. The age reduction of a cybercriminal was caused by the accessibility of the highly-technological means of communication for the youth and the availability of the mobile access to the

networks.

The swindling with the services' use of the mobile communication operators, including the SMS-messages, has become traditional. It's reasonably to divide the offences with the use of the mobile telephone into the following groups: hooliganism (including the telephone terrorism; various types of swindling, aimed against the operators and the subscribers of the mobile communication and others).

The messages on minelaying acquired a special spreading for the last time. Such crimes lead to the pulling away of the police forces, the operation stoppage of the metro (underground), enterprises, the trade complexes, the educational establishments, the state institutions, resulting in the greatest losses. As they informed in the National police of Ukraine, 3730 anonymous messages on the minelaying of buildings and the infrastructure objects came in 2019. Only 750 similar minelayings were fixed last year. Thus, it may be said of the mining of up to five hundred objects in one message [25]. It's very difficult to follow such calls or messages, because, according to the data of the companies "Kyivstar" and "Vodafone Ukraina", 90–96% of Ukrainians use today the mobile communication anonymously. According to the data of the Inter-Bank association of payment cards, EMA, the ill-intentioned persons stole more than 275 mln UHA from the accounts of Ukrainians with the help of calls and SMS-messages. This figure reached 340 mln UHA in 2018, moreover, 80% of the assets were received by the thieves, who gained the card requisites by fraud over the telephone [24].

Besides the scanty number of the registered cybercrimes, it is worth paying the attention to the insufficient degree of their punishment. The data of the General Public Prosecutor's Office, concerning the investigation of a cybercrime, are presented in the Table 7 [26].

Table 7. Crimes in Application's Sphere of Electronic-Computing Machines (Computers), Systems and Computer Networks and Electric Connection Systems.

Year	Quantity		Investigation is Closed	
	Accounted Offences	Message on Suspicion is Delivered	Quantity	%
2013	595	256	331	55,63%
2014	443	207	237	53,50%
2015	598	263	411	68,73%
2016	865	472	420	48,55%
2017	2573	1272	605	23,51%
2018	2301	1608	169	7,34%
2019	2204	1481	182	8,26%
2020	2498	1675	51	2,04%

We stress on the fact, that besides the significant number of the closed investigations, the quantity statistics of the real punishments is absent.

It's worth emphasizing, that the cyber-criminality reasons are changeless for years. They may be characterized briefly in the following way: for the enterprises – the insufficient quantity of the qualified professionals in cybersecurity; the computer threats of the new type [28]; carelessness and incompetency of the personnel; for the crossing citizens – the excessive trustfulness, poverty (the use of the licensed software, the absence of the anti-virus protection), the Internet-incompetency, carelessness, etc.

Let's indicate that the inefficient struggle is realized with such crimes in Ukraine. For example, the National Bank launched the great program of struggle with the cyber-swindling in 2020. The Anti-crisis center of the business cybernetic protection at the Trade-Industrial Chamber of Ukraine spoke with the proposal to the Ministry of Education and Science that each academic year would begin with the lessons of cyber-hygiene [23]. The cyber-police launched the campaign of knowledge in cybersecurity [27]. The activity of the cyber-police grows every year and the promulgation of the operation results is realized at the professional conferences. As the counter-action to the telephone swindling and terrorism, the petition is located (on October, 19, 2017, on the Official Internet-Representation of Ukraine President) with the demand to oblige the operators of mobile communication to identify all the mobile numbers, according to the owner's documents. The struggle with such type of crimes is only starting.

A special attention is worth being paid to the cybercrimes, aimed at the undermining of the national security, and the global threats, connected with the hacker attacks, which have become the weapon in the hybrid Russian-Ukrainian war.

The demonstrations of such threats are the attacks at the objects of the state's strategic infrastructure, which may be examined as cyber-terrorism. The Ukrainian economy lost $466 mln (or 0,5% of the GDP) only, due to the Petya virus. As Ukraine is faced with the hacker attacks at the state resources every day, the Ukrainian Service of State Security (SSU) has an intention to strengthen its cybersecurity. "The penetration scales into the state information resources strike – the attacks take place almost every day. The conclusions are simple – we need to act immediately and systematically" [20].

The director of the Cisco Representation in Ukraine and the CIS countries for the work with partners and clients, Sergiy Martynchuk (Cyber Defence Congress 2K18) announced that the majority of the great cyber-attacks fulfilled not the economic, but the political and military tasks [20].

The Minister of the Internal Affairs of Ukraine, Arsen Avakov, stated at the ZOOM-conference "Digital Transformation of the State: Perspectives and Risks of Cybersecurity" (2020) that the number of cybercrimes in the state grew by twice and a half for the last five years. The cyber-police fixes the growth of the following types of crimes: the interference into the

operation of information systems and their intentional damage; the illegal collection, storage, use and spreading of the personal data and information with the limited access; the creation of channels for spreading of weapon and drugs; the illegal financial operations, including the ones with the digital currencies; robbery and swindling in the Internet system; spam and the virus programs [20].

According to [30], the quantity of the cyber-incidents, connected with the critical infrastructure, reached 63505 cases, but with the bodies of the state government – 2938475 - for the three months of 2020.

The state tries to be opposed to such provocations. The experts of the National Coordination Center of Cybersecurity at the Council of National Security and Defense started to elaborate the Strategy of the Ukraine Cybersecurity. The cyber-police of Ukraine plans to increase the staff of the special agents in the sphere of opposition to cybercrimes of such type in 2021 [23].

Thus, the Situational Center of the cybernetic security provision on the basis of the Department of the Counter-Intelligence protection of the state interests in the sphere of the SSU information security, according to the NATO standards, was created in the SSU in 2018 with the support of the foreign partners. It was developed, according to the agreement on the realization of the Ukraine-NATO Trust Fund. More than $1 mln. were allocated for the project. Its key possibilities are revealing and reacting to the various online incidents, which allow prevent the cyber-attacks, determine their origin, analyze for the opposition improvement.

3 Conclusions

Cyber-criminality at present – is the real global threat, which may go out of any country of the world beyond the limits of the definite jurisdiction (in contrast to the other traditional types of economic crimes).

The COVID-19 pandemic promotes to the growth and spreading of cyber-criminality. At the same time, when the online swindling, the demanding and the sexual violence at children in the Internet are aimed at the separate groups of persons, the programs-demanders, in the first turn, undermine the operation of the organizations, including the hospitals.

The distance work increased the number of the potential victims of cyber-criminality. Working online from home, people are subjected to the bigger risk than at the usual mode of operation.

Thus, the introduction of digital technologies at enterprises, information technologies (IT) for information protection, causes the appearance of the new form of counteraction – cyber-insurance.

In the result of the research we have come to the conclusion, that Ukraine fights the above mentioned problems, but organization of such a fight compared to the highly developed countries is at the initial stage. As the necessary conditions for increasing fight efficiency with cyber-criminality can be named the following: the reasoned scientific analysis of such problems, the up-to-date legislative provision, the increasing financial support of appropriate organs for strengthening their personnel and technical potential.

References

1. International Standard, Access Mode ISO/IEChttp://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm
2. D. Gavlovsky, To the Problem of Counter-Action to the Use of Harmful Software Struggle with Organized Criminality and Corruption (Theory and Practice) **1**, 125–130 (2014)
3. O.V. Orlov, State Government of Professionals' Training in the Sphere of Cyber-Security, State Construction. Access Mode: http://kbuapa.kharkov.ua.
4. V.A. Romaka, A.E. Lagun, Yu.R. Garasym and oth.; Audit of Information Security: Texbook 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)
5. D.V. Dubov, Cyber-Space as New Measure of Geo-Political Rivalry. Monograph NISR (2014)
6. M.O. Kravtsova, O. M. Lytvynov, Prevention of Cyber-Criminality in Ukraine: Monograph, Kharkiv Panov (2016)
7. S.V. Melnyk, V.I. Kaschuk, 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., Kyiv NPC NA SS of Ukraine, 5 April 2013
8. I.V Diorditsa, Notion and Contents of Cyber-Security's National System, Access Mode http://goal-int.org/ ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/
9. S.F. Honchar, G.P. Leonenko, O.Yu. Yudin, Methodological Bases of Elaboration and Introduction of Information Protection's Systems in Objects of Critical Infrastructure. Special Telecommunication Systems and Protection of Information **1** (25), 158–163 (2014)
10. Control of Struggle with Cyber-Criminality. Ministry of Internal Affairs of Ukraine. Access Mode http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754
11. Law of Ukraine "On Principal Bases of Ukraine's Cyber-Security Provision" (News of Verhovna Rada (NVR) **45**, (2017)
12. European Cybercrime Center – first year report, URL https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report. Date of address: 29.05.2016).
13. Modern Trends of Cybersecurity Policy: Conclusions for Ukraine. Analytical Note,

National Institute of Ukraine Strategic Research, Access Mode http://old2.niss.gov.ua/articles/294/. Date of address: 31.01.2021)

14. Sergiy Tkalichenko, Valentyna Khotskina, Zhanna Tsymbal, Cyber-Criminality: Protection's Aspects of Modern Information Space. Advances in Economics, Business and Management Research, **129**. 137–143 (2020)
15. Internet Crime Report 2017, FBI's Internet Crime Complaint Center (IC3) URL: https://pdf.ic3.gov/2017_IC3Report.pdf /. Date of address: 31.01.2021)
16. Internet Crime Report 2013, FBI's Internet Crime Complaint Center (IC3) URL: https://pdf.ic3.gov/2013_IC3Report.pdf /. Date of address: 31.01.2021
17. Internet Crime Report 2019, FBI's Internet Crime Complaint Center (IC3), URL: https://pdf.ic3.gov/2019_IC3Report.pdf /. Date of address: 31.01.2021
18. What Do You Need to Know of Cyber-Criminals in Ukraine? URL: https://www.radiosvoboda.org/a/details/29031166.html. Date of address: 31.01.2021
19. Ukraine in Figures in 2017, State Service of Ukraine Statistics, URL:http://www.ukrstat.gov.ua/druk/publicat/kat_u/2018/zb/08/Ukr_cifra_2017_u.pdf. Date of address: 31.01.2021
20. Cyber Defence Congress 2K18, URL: https://itukraine.org.ua/cyber-defence-congress-2k18.html. Date of address: 31.01.2021
21. Report of Ukraine National Police Head on Operation Results of Department in 2019, URL:https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf. Date of address: 31.01.2021
22. Cyber Choices: Helping You Choose the Right and Legal Path, NCA, URL: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices. Date of address: 31.01.2021
23. Staff of Special Agents for Opposition to Cyber-Swindling Will Be Increased, URL: https://www.ukrinform.ua/rubric-economy/2805152-v-ukraini-zbilsit-stat-specagentiv-dla-protidii-kibersahrajstvu.html. Date of address: 31.01.2021
24. Telephone Swindling: How Do They Demand Money from Ukrainians and What to Do with IT? URL: http://chp.com.ua/ua/all-news/item/59212-telefonnoe-moshennichestvo-kak-u-ukraintsev-vymogayut-dengi-i-chto-s-etim-delat. Date of address: 31.01.2021
25. Who and Why "Mines" Massively Public and Administrative Buildings? Deutsche Welle, URL: https://p.dw.com/p/3Mjk3. Date of address: 31.01.2021
26. Report on Criminal Offences in the State, General Public Prosecutor's Office of Ukraine, URL: https://old.gp.gov.ua/ua/statinfo.html. Date of address: 31.01.2021
27. Cyber-Police Launched Campaign on Knowledge of Cybersecurity, United Portal of Ukraine MIA System Bodies, URL: https://mvs.gov.ua/ua/news/18914_Kiberpoliciya_zapustila_kampaniyu_z_obiznanosti_pro_kiberbezpeku.htm. Date of address: 31.01.2021
28. NHS Cyber Attack: Everything You Need to Know about 'Biggest Ransomware' Offensive in History (2017), Access Mode: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive. Date of address: 03.01.2020
29. Global Research of Swindling Problems in Banking Sphere, KPMG International Cooperative, URL: https://assets.kpmg/content/dam/kpmg/ua/pdf/2019/11/Global_Banking_Fraud_Survey.pdf. Date of address: 31.01.2021
30. State of National Cybersecurity for the Last Three Months, NCCC at CNSD of Ukraine, URL: https://www.rnbo.gov.ua/ua/Diialnist/4761.html. Date of address: 31.01.2021