Advances in Economics, Business and Management Research, volume 129
III International Scientific Congress Society of Ambient Intelligence 2020 (ISC-SAI 2020)

Cyber-Criminality: Protection's Aspects of Modern Information Space

Sergiy Tkalichenko[1] Valentyna Khotskina[1,*] Zhanna Tsymbal[1]

[1] *Kryvyi Rih Economic Institute of Kyiv National Economic University named after Vadym Hetman, Kryvyi Rih, Ukraine*
[*] *Corresponding author: Email: khotskina_vb@ukr.net*

ABSTRACT
The actual problem of the modern society – cyber-criminality –is examined in the article. The classification of the "cyber-crime" notion is realized in the process of study of the cyber-crimes and the mechanisms of protection from the information security's threats. The list of the hardest cyber-crimes is composed, according to the presented classification. The comparative characteristics between the number of the registered cyber-attacks and the losses from them is carried out. The analysis of the actual data for five years is exercised, on the basis of which the quantity indicators' table of cyber-attacks, general losses is elaborated and the cost of the cyber-attacks is calculated. The recommendations for the reliability's increase of the information protection are presented in the limits of the research.
Keywords: *ICT – information-communication technologies, information security, cyber-security, cyber-attacks, authentication*

1. INTRODUCTION

The accelerated development of the calculation engineering and the information-communication technologies (ICT) occurs in XXI century.
The problems, connected with ICT, have been in the interests' sphere of the narrow circle of the professionals still a decade ago. The events of the last years demonstrated: the actuality of the cyber-attacks grows. The threat of the access to information and the interference into it appear in the result of any activity, connected with the formation, creation, transformation, transmission, use and storage of information. Namely, due to the interaction of people, the software, the Internet-services with the help of the technological devices and the net connections. The problem of the information security appears with the ICT development in the information space, on the basis of which is – the activity of the information protection – the guarantee of its confidentiality, accessibility and completeness.

1. Literature Review:

At present, in the times of the society's information, the ventilation of the cyber-criminality's problem gains the actuality from the position of the threat to the modern information society. According to that, it's necessary to construct the efficient system of the cyber-security's guarantee at the state level.
The materials of the cyber-security problems' researches are represented in the Norton Cybercrime Report, SecureWorks Cybercrime, FBI IC3Report, Globalstudy.bsa.org and the other sources.
The decision "On Cyber-Security's Strategy of Ukraine" was adopted on January, 27, 2016 by the Council of the national security and defense of Ukraine, but the corresponding law was approved in 2017[1]. This problem happened to be especially urgent during the hybrid aggression of Russia.
The efficiency of the struggle with the cyber-criminality lies, firstly, in the presence of the corresponding coordinated legislation's base of the leading countries of Europe and, correspondingly, the presence of the professionals in information security.
The problems of the international experience's study of the information security are lighted up in the investigations of Gavrylovsky D., Sidak V.S., Artemov V.Yu. [16, 20], the training's state of the professional specialists is revealed by Orlov O.V.[17]. The adaptation of the international standards is characterized by the introduction of ISO/IEC 15408 standard [18].
The aspects of the information security and cyber-criminality have been investigated for ten years by the domestic scientists: the cyber-security and the protection of the Ukraine's information space (Buryachok V.L., Gnatyuk S.O., Korchenko O.G., Butuzov V.M. and others) [12, 13, 14, 15]; the audit of the information security (Romaka V.A., Lagun A. E., Garasym Yu.R. [19]); the hybrid aggressive threats (Dubov D.V. [21, 24]); the prevention of the cyber-criminality (Kravtsova M.O. [22], Buryachok V.L. [23], Melnyk S.V. [25], Diorditsa I.V. [26]); the protection of the critical infrastructure's objects (Honchar S.F. [27]). The cyber-criminality gains the widening in different branches (the protection of data bases, the banking protection, the protection of the

Copyright © 2020 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

intellectual ownership, the defense from pornography, electronic swindling, etc. [28]).

2. Problem's Positing

The creation of the modern information space, which outlined the new level of the information protection's problems, was recognized at the meeting of the developed states' representatives in Okinawa in July, 2000. The new notions appeared: cyber-space, cyber-criminality, cyber-attacks, etc. The scales of these phenomena were approved by the research of SUMANTEC (2007), according to which the incomes of the cyber-criminality exceeded the incomes of the drugs trading. By the way, the hundreds of the worldwide known organizations study statistics, analysis and methods of these notions' prevention.
One of the aspects of the outlined problem – the application of the unlicensed software – is lighted up in the article.

3. Presentation of Materials and Results

The cyber-security – is the protection of the vitally important interests of the individual, society and the state in the period of the cyber-space application, due to which the stable development of the information society and the digital communication environment, the timely revealing, prevention and the neutralization of the real and potential threats to the national security of Ukraine in the cyber-space are guaranteed [1].
There is a considerable quantity of the notions' definitions: "cyber-threat", "cyber-crime", "cyber-attack" in the scientific literature. But these terms are defined most completely in [1]. The classification of the "cyber-crime" notion is various enough from the position of the scientific understanding. The most complete classification, in our opinion, is presented in fig. 1.

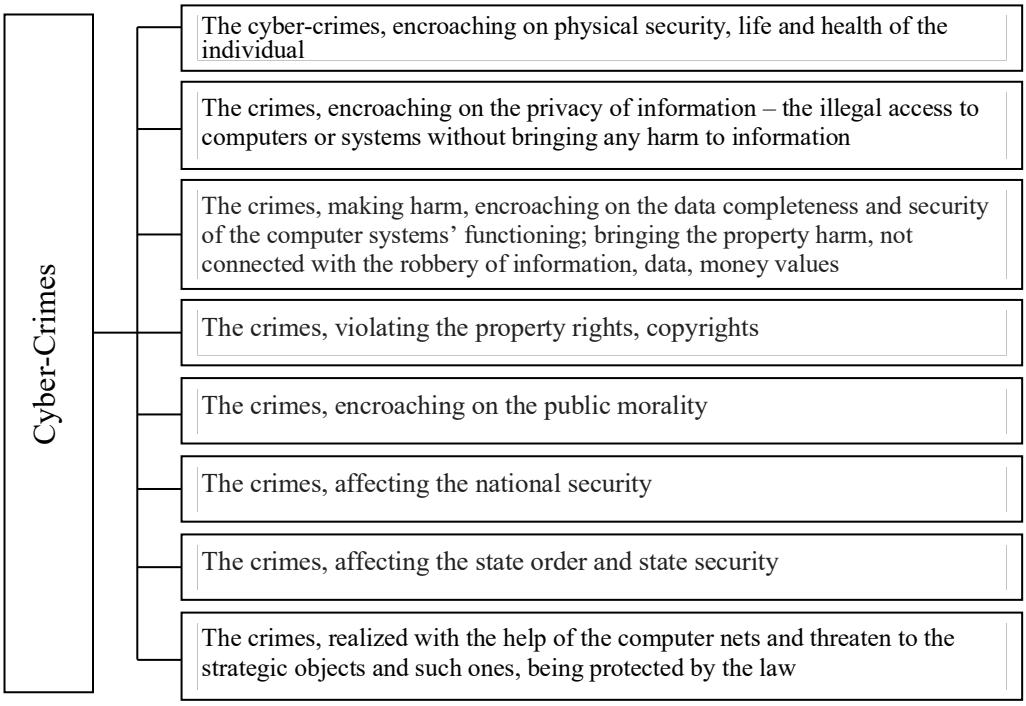

Figure 1 Classification of the "cyber-crime" notion

The hardest cyber-crimes, according to the presented classification, are the crimes against the state and the strategic objects. We'll present such data to confirm the above mentioned [4]:
- The DDOS-attacks and breaking up of the CEC site during the president elections took place on May, 21-25, 2014, in the outcome of which the mistaken results appeared on the site. In spite of the information on the breaking up, the very those data were wired for sound in the news on the Russian First channel as the real results of the elections in Ukraine.

– The harmful programs, being engaged in the cyber-spying (Turla/Uroburos/Snake, RedOctober, MiniDuke and NetTraveler) were revealed on the servers of the private companies of Ukraine and NATO countries in June, 2014.
– Nearly 30 substations of the "Pre-Carpathianoblenergo" were put off on December, 23, 2015 with the help of the Throjan program BlackEnergy3, in the use of which the Russian hackers had been noticed before, therefore above 200 thousand residents of the Ivano-Frankovsk region were left without the electric energy for the period of one to five hours. The attacks at "Kyivoblenergo" and "Chernivtsioblenergo" took place at that time too.

– The "hacker attack" at the internal telecommunication nets of the Finance Ministry, the State Exchequer, the Pension Fund took place on December, 6, 2016. It broke down the computers and also destroyed the critically important data bases, leading to the delay of the budgetary payments in hundreds million UAH.
– The Ukrainian hackers, on the order of the undetermined person from Saint-Petersburg, realized the DDOS-attack at the "Ukrzaliznytsya" site on December, 15, 2016, in the result of which its operation was completely blocked for one day-period. The attack was oriented at the data's robbery of passengers-transportation.
– The cyber-attack at the substation "Pivnichna" of the "Ukrenergo" company on December, 17, 2016 led to the breakage in the government's automation, due to which the northern part's regions of the right-bank Kyiv and the adjoining regions of the district were left without any current for above one hour-period.
– The massive cyber-attack started in the first half of the day on June, 27, 2017 at the Ukrainian state and commercial sector with the use of the harmful software – the virus-coder of files Petya Ransomware. The information-telecommunication systems of "Ukrposhta", the "Boryspil" airport, "Ukrenergo", SHEC, many banks, MMI, television channels, ARS and others became its victims.

But the more spread cyber-attacks are those that may destroy, spoil, steal the data, reduce or absolutely prostrate the further efficiency of the computer's operational system, the computer nets, the servers, the information systems [2]. If you deal with the destroying of information, then, the losses, caused by the successful attack, are equal to the cost of the valuable information.

The number of the registered cyber-attacks of such type and the losses from them are presented in fig. 2.

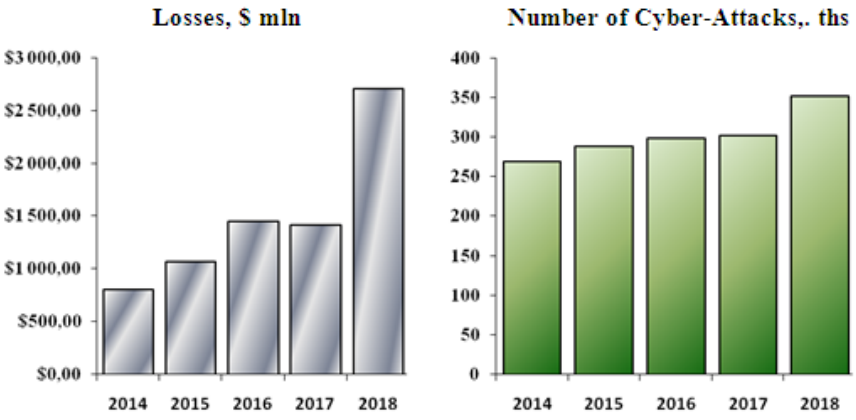

Figure 2 The number of cyber-attacks and losses in 2014–2018 (according to the data of FBI's Internet Crime Complaint Center) [3]

You should mention that the cost of the cyber-attack has considerably grown (table 1 and fig.3): from $2 971,2 in 2014 till $7 689,2 in 2018, except the indicators' growth of both their number and the general losses.

Table 1 Correlation of Cyber-Attacks and General Losses:

Year	Losses, $	Number of Cyber-Attacks	Price of One Cyber-Attack, $
2014	800500000	269422	2971,18
2015	1070700000	288012	3717,55
2016	1450700000	298728	4856,26
2017	1418700000	301580	4704,22
2018	2706400000	351973	7689,23

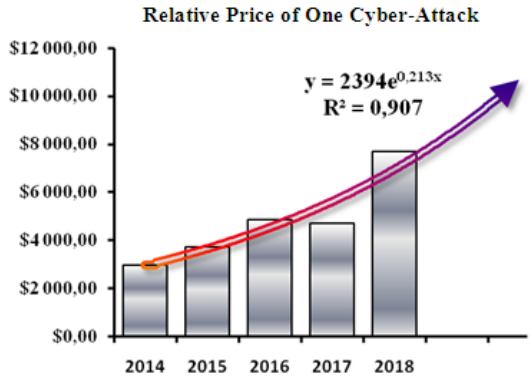

Figure 3 The number of cyber-attacks and losses in 2014–2018 (according to the data of FBI's Internet Crime Complaint Center) [3]

The incidents, connected with the cyber-criminality, began to take place more frequently and they regularly appear in the news' headlines, causing much more trouble of the consumers and the leaders of business [6]. In spite of the

vigilant attention to such incidents, the most part of the organizations throughout the world is still hard to comprehend and to govern the appearing cyber-risks in the complex digital environment. Paying attention to the fact that the digital environment complicates every day and our dependence on the data and the interaction in the net grows, the development of the stability to the cyber-threats – the wide-scale events with the ruining results, being developed, according to the cascade principle, - has never been so important.

The General-European Regulation on the protection of personal data became valid on May, 25, 2018 (from Engl., GDPR – General Data Protection Regulation). GDPR coordinates the standards of the data protection in the limits of EU, but the activity of those, who haven't heard the warning to the end, may by broken by the fines of the Council, dealing with the standards of the data security of the payment cards' industry (from Engl., PCI SSC – Payment Card Industry Security Standards Council).

The Cyber-police, as the structural subdivision of the National police, was created on October, 5, 2015. The creation's aim of the Cyber-police in Ukraine is the reformation and development of the Ukraine MIA subdivisions, securing the training and the functioning of the highly-qualified professionals in the expert, operative and the investigating subdivisions of the police, engaged in the counter-action to the cyber-criminality and being capable to use the latest technologies in the operative-official activity at the high professional level. The cyber-police of Ukraine arrested the organizer of the bot-net Avalanche, revealed the participant of the international hacker grouping Cobalt, took part in the activity's stoppage of the international hacker group FIN7, warned four massive cyber-attacks on the territory of Ukraine. Eight transnational hacker groupings were revealed and more than 30 international operations were participated in the limits of the international cooperation [7]. Without any doubt, it's tool little in comparison with the other developed countries.

Ukraine is situated in the zone of the increased cyber-danger. It is connected with the poverty of the citizens, who have to economize on the licensed software. The absence of the operational systems' renovation increases the risk of the possible infection of computers. The presence even of the simple viruses increases the organization's losses in the period of the net's stoppage for the liquidation of viruses. Besides, the installation of the renovations, issued by the official producers of programs, becomes impossible at the use of the pirate software.

The interest analysis of the unlicensed software's application in Ukraine and in the geographically nearest countries is presented in the Table 2, according to the data of the "Microsoft Ukraina" representatives, in accordance with the research of BSA Global Software Survey [8], which is regularly held by the Association of the software's producers.

Table 2 Application of Unlicensed Software, %:

Country	Year				Average Meaning	Absolute Increment, %	Absolute Increment for a year, %	Relative Rate of Reduction for a year, %
	2011	2013	2015	2017				
Moldova	90	90	86	83	87,25	-7	-1,00	0,08
Georgia	91	90	84	81	86,50	-10	-1,43	0,12
Byelorussia	87	86	85	82	85,00	-5	-0,71	0,06
Azerbaijan	87	85	84	81	84,25	-6	-0,86	0,07
Ukraine	84	83	82	80	82,25	-4	-0,57	0,05
Russia	68	65	64	62	64,75	-6	-0,86	0,09
Bosnia	66	65	63	61	63,75	-5	-0,71	0,08
Rumania	63	62	61	59	61,25	-4	-0,57	0,07
Lithuania	54	53	51	50	52,00	-4	-0,57	0,08
Latvia	54	53	49	48	51,00	-6	-0,86	0,12
Poland	53	51	48	46	49,50	-7	-1,00	0,14
Estonia	48	47	42	41	44,50	-7	-1,00	0,16
Hungary	41	39	38	36	38,50	-5	-0,71	0,13
Czech	35	34	33	32	33,50	-3	-0,43	0,09

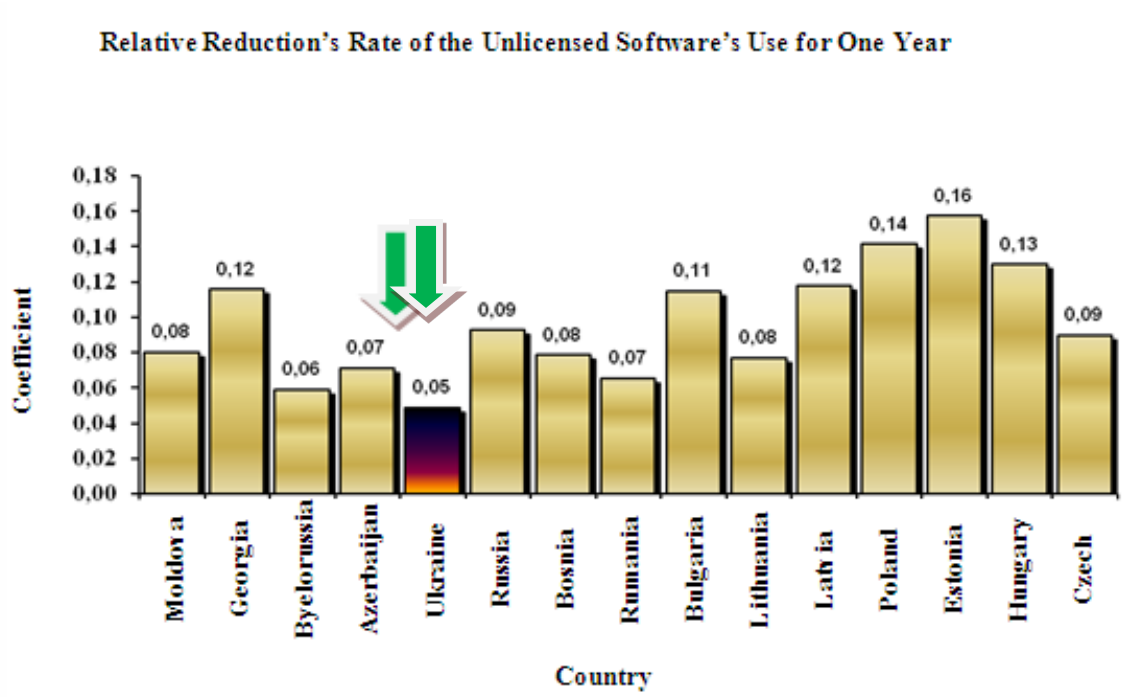

Figure 4 The annual relative reduction's rate of the unlicensed software's use

As we see, Ukraine demonstrates the less relative reduction of the unlicensed software's use among the nearest foreign countries.

The distribution of the programs, being more frequently attacked, didn't almost change during the last years. The appendixes from the Microsoft Office package in this distribution occupy the first place (70%), being by five times more than the browsers, occupying the second one [9].

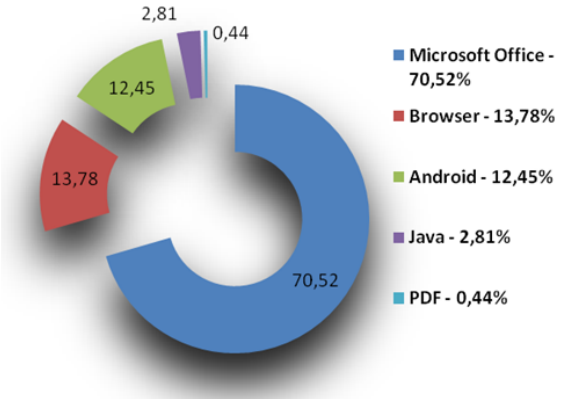

Figure 5 The interest cut of the office programs, being attacked more frequently.

The number of the impressibilities in the decisions of the Microsoft company increased by 110% for the period from 2013 till 2018. In general, more than 700 problems were revealed in 2018. Such data are presented in the BeyondTrust report, devoted to the bugs in Microsoft Software [10].

Let's name the main reasons of the weak cyber-protection of the majority of the organizations and enterprises.

The first reason is – the absence of the qualified specialists in cyber-security. The domestic HEE began the students' enrolment for training on this profession only in the last years.

The second reason lies in the computer threats of the new type. The attack WannaCry Ransomware, which started in spring, 2017, touched over 300000 computers in more than 150 countries. And such threats appear very often. According to the data of the SecureWorks research, held among the companies in the Northern America, Great Britain and Asia in 2016, 36% respondents of b2b segment have already become the victims of such attacks, but 57% of them believe that they will become the aim of the harmful programs-blackmailers in 2017 [11].

The third and, possibly, the most powerful reason is the indifference and illiteracy of the personnel. In fact, 60% of the information security's violations (the research of Cyber Security Intelligence IBM in 2016) was caused directly by the personnel itself. 81% of the critical impressibilities, according to the information from the official bulletins of the Microsoft security for 2018, may be eliminated only by excluding the administrator's rights.

Let's present some recommendations in order to increase the cyber-protection's level of the organizations.

The application of the protection's efficient means: the licensed anti-viruses, the centralized government's means of the Software renovation, the means of the problems' revealing in Software, SIEM-decision, the net screening, the services of anti-DDOs, etc.

The data protection: the regular reserve copying of information, the minimization of the users' rights, the

different accounting records and passwords in different resources, the double-factor authentication (where it's possible), the introduction of the password policy, according to which the severe demands, concerning the length, structure and the terms of the password's action, are introduced.

2. CONCLUSION

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

The introduction of the digital technologies at the enterprises and in all the activity's spheres requires the involvement of the professionals in security of the information technologies (IT) for the protection of information.

According to the new research of the labor resources in the sphere of the global information security, held in 2017, more than 1,8 million vacancies in the sphere of the cyber-security are left unoccupied till 2022.

Basing on the above mentioned, you may come to the conclusion: the problems of the information space's protection, the counter-action to the information weapon, the elaboration of the information struggle's strategy are at the stage of the formation and require the grounded scientific provision and support.

REFERENCES

[1] Law of Ukraine "On Principal Bases of Ukraine's Cyber-Security Provision" (News of the Supreme Rada (NSR). – 2017. – № 45. – art. 403).

[2] Law of Ukraine "On National Security of Ukraine" (News of the Supreme Rada (NSR). – 2018. – № 31. – art. 241).

[3] Federal Bureau of Investigation, FBI. URL – Access Mode : https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219 / (date of address: 03.01.2020).

[4] Analysis of Regular Influence of Decree's Project of the Ukraine's Cabinet of Ministers "Some Problems of Independent Audit's Realization of Information Security in Objects of Critical Infrastructure" (State Service of Special Connection and Protection of Information) – 2019, URL. – 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 (date of address: 03.01.2020)

[5] Federal Bureau of Investigation, FBI. URL: – Access Mode: https://pdf.ic3.gov/2017_IC3Report.pdf / (date of address: 03.01.2020).

[6] The Global State of Information Security® Survey 2018. – Access Mode : https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf (date of address: 03.01.2020).

[7] Report of the Head of Ukraine's National Police, S. Knyazyev "On Results of Department's Operation for the period of 2018". – National Academy of Internal Affairs, Access Mode: https: //www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf (date of address: 03.01.2020).

[8] International Data Corporation. Unlicensed Software and Risks for Cyber-Security. URL: – Access Mode : https://globalstudy.bsa.org/2013/Malware/study_malware_ru.pdf (date of address: 03.01.2020).

[9] Microsoft Ukraina: Weaknesses in Microsoft Program Products. – Access Mode : https://www.microsoft.com/uk-ua; https://cybercalm.org/novyny/vidklyuchennya-prav-administratora-zahystyt-vid-81-urazlyvostej-v-produktah-microsoft (date of address: 06.11.2018).

[10] Beyond trust. Microsoft Vulnerabilities Report 2019. – Access Mode : https://www.beyondtrust.com/de/resources/whitepapers/microsoft-vulnerability-report (date of address: 03.01.2020).

[11] 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)

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

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

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

[19] 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.

[20] Sidak V.S. Provision of Information Security in the Countries of NATO and EU: Ed. Manual / V.S. Sidak, V.Yu. Artemov. –K. : CST, 2007.

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

[22] 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.

[23] 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.

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

[25] 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.

[26] 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/

[27] 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.

[28] 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