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

Sergiy Tkalichenko¹, Valentyna Khotskina*¹, Zhanna Tsymbal¹, Victoria Solovieva¹, and Olena Burunova²

¹State University of Economics and Technology, Kryvyi Rih, Ukraine
²Science 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.

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).
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.

\[
I_{pg} = \frac{\sum p_1 g_1}{\sum p_0 g_0}, \quad I_p = \frac{\sum p_1 g_1}{\sum p_0 g_0}, \quad I_g = \frac{\sum p_0 g_1}{\sum p_0 g_0}
\]

where \( p_1, p_0 \) – the average cost of one crime (current and previous period), \( q_1, q_0 \) – the quantity of crimes (current and previous period), \( I_{pq} \) – the general index of losses, \( I_p \) – the general index of losses, due to the increase of the crime’s average cost, \( I_q \) – the general index of losses, due to the number increase of crimes (Table. 3, Fig. 3).
Table 1. Growth Dynamics of Losses from Cybercrimes.

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses, mln. $</th>
<th>Absolute Chain Increment, mln. $</th>
<th>Year</th>
<th>Losses, mln. $</th>
<th>Absolute Chain Increment, mln. $</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>17,8</td>
<td>0</td>
<td>2011</td>
<td>485,2</td>
<td>-78</td>
</tr>
<tr>
<td>2002</td>
<td>54</td>
<td>36,2</td>
<td>2012</td>
<td>581,4</td>
<td>96,2</td>
</tr>
<tr>
<td>2003</td>
<td>125,6</td>
<td>71,6</td>
<td>2013</td>
<td>781,8</td>
<td>200,4</td>
</tr>
<tr>
<td>2004</td>
<td>68,1</td>
<td>-57,5</td>
<td>2014</td>
<td>800,4</td>
<td>18,6</td>
</tr>
<tr>
<td>2005</td>
<td>183,1</td>
<td>115</td>
<td>2015</td>
<td>1070,7</td>
<td>270,3</td>
</tr>
<tr>
<td>2006</td>
<td>198,4</td>
<td>15,3</td>
<td>2016</td>
<td>1450,7</td>
<td>380</td>
</tr>
<tr>
<td>2007</td>
<td>239,1</td>
<td>40,7</td>
<td>2017</td>
<td>1418,7</td>
<td>-32</td>
</tr>
<tr>
<td>2008</td>
<td>264,6</td>
<td>25,5</td>
<td>2018</td>
<td>2710</td>
<td>1291,3</td>
</tr>
<tr>
<td>2009</td>
<td>559,7</td>
<td>295,1</td>
<td>2019</td>
<td>3500</td>
<td>790</td>
</tr>
<tr>
<td>2010</td>
<td>563,2</td>
<td>3,5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

Table 3. Index Analysis of Cybercrimes Structure.

<table>
<thead>
<tr>
<th>Year</th>
<th>Quantity</th>
<th>Losses, $</th>
<th>Average Losses, due to One Cybercrime</th>
<th>Ip</th>
<th>Iq</th>
<th>Ipq</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>314246</td>
<td>485253871</td>
<td>1544,18</td>
<td>1,05539328</td>
<td>0,696824</td>
<td>1,082817</td>
</tr>
<tr>
<td>2012</td>
<td>218974</td>
<td>525441110</td>
<td>2399,56</td>
<td>1,2397681</td>
<td>1,200202</td>
<td>1,487972</td>
</tr>
<tr>
<td>2013</td>
<td>262813</td>
<td>781841611</td>
<td>2974,90</td>
<td>1,09987391</td>
<td>1,025147</td>
<td>1,023855</td>
</tr>
<tr>
<td>2014</td>
<td>269422</td>
<td>800492073</td>
<td>2971,15</td>
<td>1,2512322</td>
<td>1,069</td>
<td>1,337567</td>
</tr>
<tr>
<td>2015</td>
<td>288012</td>
<td>1070711522</td>
<td>3717,59</td>
<td>1,3062906</td>
<td>1,037207</td>
<td>1,354893</td>
</tr>
<tr>
<td>2016</td>
<td>298728</td>
<td>1450700000</td>
<td>4856,26</td>
<td>1,096996</td>
<td>1,009547</td>
<td>0,97922</td>
</tr>
<tr>
<td>2017</td>
<td>301580</td>
<td>1420555000</td>
<td>4710,38</td>
<td>1,632569</td>
<td>1,166977</td>
<td>1,905171</td>
</tr>
<tr>
<td>2018</td>
<td>351937</td>
<td>2706400000</td>
<td>7690,01</td>
<td>0,973842</td>
<td>1,327968</td>
<td>1,293231</td>
</tr>
</tbody>
</table>

Thus, the aggregate index of the general growth of losses is \( I_{pq} = 1,308 \) (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 \( (I_q = 1,066) \) and the sharp rise of the average cost of one crime – by 24% \( (I_p = 1) \).

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

*Corresponding author: khotskina_vb@ukr.net
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 4. Indexes of the Most Dynamic Quantitative Types of Cybercrimes.

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

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.

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

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 Gryncak, 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].

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...
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>
<thead>
<tr>
<th>Year</th>
<th>Number of Offences</th>
<th>Message on Suspicion is Delivered</th>
<th>Investigation is Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Quantity</td>
<td>%</td>
</tr>
<tr>
<td>2013</td>
<td>595</td>
<td>256</td>
<td>331</td>
</tr>
<tr>
<td>2014</td>
<td>443</td>
<td>207</td>
<td>237</td>
</tr>
<tr>
<td>2015</td>
<td>598</td>
<td>263</td>
<td>411</td>
</tr>
<tr>
<td>2016</td>
<td>865</td>
<td>472</td>
<td>420</td>
</tr>
<tr>
<td>2017</td>
<td>2573</td>
<td>1272</td>
<td>605</td>
</tr>
<tr>
<td>2018</td>
<td>2301</td>
<td>1608</td>
<td>169</td>
</tr>
<tr>
<td>2019</td>
<td>2204</td>
<td>1481</td>
<td>182</td>
</tr>
<tr>
<td>2020</td>
<td>2498</td>
<td>1675</td>
<td>51</td>
</tr>
</tbody>
</table>

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 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 Martynehuk (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 mlн. 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-
demanded, 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
000/2489/Ittrf_Home/PubliclyAvailableStandards.h
tm
2. D. Gavlovsky, To the Problem of Counter-Action
to the Use of Harmful Software Struggle with
Organized Criminality and Corruption (Theory
and Practice) I, 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: Textbook 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/ ponyattyta-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 I (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


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


23. Staff of Special Agents for Opposition to Cyber-Swinding Will Be Increased, URL: https://www.ukrinform.ua/rubric-economy/2805152-v-ukrani-zbilsit-stat-specagentiv-dla-protidii-kibersahrajstvu.html. Date of address: 31.01.2021


30. State of National Cybersecurity for the Last Three Months, NCCC at CNSD of Ukraine, URL: https://www.radiosvoboda.org/a/details/29031166.html. Date of address: 31.01.2021