Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 11, 2020

CONTROL OVER CRIME COMMISSION (MATERIALS OF CYBERCRIME CASES)

Samoilenko Olena[1], P. Reznik Nadiia[2], Bielik Larysa[3], Chornous Yuliia[4]

[1]PhD in Law, Associate Professor, Department of Criminalistics, National University Odesa, Ukraine.
[2]Doctor of Economics, Professor, Head of Department of Management named after prof. J.S. Zavadskyi, National University of Life and Environmental Science, Kyiv, Ukraine.
[3]PhD in Law, Associate Professor, Department of Criminalistics, National University "Odesa Law Academy", Odesa, Ukraine.
[4]LLD, Professor of Department of Criminalistics and Forensic Medicine, National Academy of Internal Affairs, Kyiv, Ukraine.

Received: 11.04.2020 ***Revised: 18.05.2020*** ***Accepted: 09.06.2020***

Abstract
Timeliness of the paper's topic is based on the fact that annual increase in data leakage via the Internet creates favorable conditions for the commission of cybercrime trespassing against various legal relationships: from the sector of national security to property relations. The common trait of such crimes is that certain features and characteristics of cyberspace are used to achieve a criminal result; thus it becomes clear that use of uniformed methods and means to investigate this criminal activity is pivotal. Having analyzed the materials of judicial and investigative practice, we may state that control over crime commission is a typical and one of the most effective tactical means used to tackle practical problems of cybercrime investigation in Ukraine.
Control over crime commission is an element of forensic tactics – formats of its optimization are to be identified in the context of performance tactics specificity within the investigation of separate crime group/category. We studied the peculiarities of certain control type selection through the prism of tactical need for this covert investigative (search) action to be performed during the cybercrime investigation.

Keywords: Investigation, Cybercrime, Tactics, Recommendations, Covert Investigative (Search) Actions.

© 2020 by Advance Scientific Research. This is an open-access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)
DOI: http://dx.doi.org/10.31838/jcr.07.11.135

INTRODUCTION

The annual increase in data leakage via the Internet [1] creates favorable conditions for the commission of cybercrime trespassing against various legal relationships: from the sector of national security to property relations.

Cybercrime should also be considered as international crime as it is completely borderless – computers, technical equipment and networks are easily operated to commit crimes without being tied to physical locations which makes it difficult to trace and identify perpetrators using the abovementioned technology. In order to successfully perform the tasks of identification, detection, investigation, prevention of cybercrimes, provisions of international treaties and national legislation regulating the prosecution of cybercrimes must be applied [2, p. 92].

The Convention on Cybercrime (2001) with its Additional Protocol (2003) [3] recognizes the international illegality of offenses against the confidentiality, integrity and availability of computer data and systems: illegal access; illegal interception; data interference; intervention in the system; abuse of devices and other illegal actions which stipulate use of computers, operating networks, relevant information. Prosecution of the outlined offenses is defined in Chapter XVI of the Criminal Code of Ukraine [4].

The common feature of such crimes is that certain features and characteristics of cyberspace are used to achieve a criminal result; thus it becomes clear that use of uniformed methods and means to investigate this criminal activity is pivotal. Having analyzed the materials of judicial and investigative practice, we may state that control over crime commission is a typical and one of the most effective tactical means used to tackle practical problems of cybercrime investigation in Ukraine.

Control over crime commission is an integral part of a certain tactical operation within the investigation cycle and has certain specificity shaped by the tactical tasks of a peculiar criminal activity investigation. Therefore, from a scientific – forensic – point of view ways to optimize the control over crime commission should be determined in the context of a particular crime group/type. That's why we focused intensively on cybercrime.

LITERATURE REVIEW

Ukrainian long-standing practice of operative-search activity proved that controlled supply / controlled and operative procurement of goods, items and substances are highly efficient in the process of crime combating. Many researchers working in the area of operative-search activity and criminal procedure contributed significantly to resolution of problems related to the implementation of the abovementioned measures and use of relevant results in criminal proceedings, namely S. Albul, O. Antonechko, M. Gribov, O. Dolzhenkov, I. Demidov, A. Ishchenko, I. Kozachenko, S. Kudinov, D. Nykyforchuk, S. Nikolaiuk, V. Nekrasov, A. Onofreichuk, M. Pohoretskyi, O. Podobnyi, D. Serheieva, Y. Skulysh, S. Tahiiev, M. Shumylo etc.

Amendment introduced to the applicable criminal procedure legislation (combining controlled supply / controlled and operative procurement as well as newly introduced forms of covert activity in the form of a special investigative experiment and simulation of criminal environment into one independent covert investigative (search) action - control over crime commission) has intensified the forensic research in this area. After all, having defined four independent forms of control over crime commission: 1) controlled supply; 2) controlled and operative procurement; 3) special investigative experiment; 4) simulation of the crime circumstances in Article 271 of the Criminal Procedure Code of Ukraine [5], legislator had not introduced legislative criteria to distinguish these forms of investigative activity, resulting in purely subjective choice of one of the forms of control over crime commission made by the initiator in specific situations; that is why V. Bernaz, R. Blahuta, A. Volobuiev, M. Dzhyha, A. Ishchenko, V. Lysenko, S. Tahiiev, Y. Shepitko, Y. Shynkarenko and other scholars pay considerable

attention to the tactics of performing the specific types of control over crime commission.

For example, debates still take place among the experts in the area of operative-search activity and criminal procedure regarding the separation of investigative experiment from imitation (simulation) of the criminal environment. M. Bahrii considers the perpetrator's identification a criterion the abovementioned division (special investigative experiment is performed concerning certain subject, imitation – both identified and unidentified subjects) [6]; V. Dintu – aim and environment where these forms of control over crime commission are carried out [7]. M. Hribov mentions the relative criteria of distinguishing the abovementioned forms of control over the crime commission. The author confirms the existence of certain features common for special investigative experiment and the simulation of the crime situation as different forms of control over crime commission and proves the inconsistency of their division in the current criminal procedure legislation [8]. Each scholar provides arguments for individual opinion which, without any doubt, deserves attention.

Any investigative (search) action, including covert ones, is a practical means of achieving tactical objectives during the investigation of a crime, a means of forensic tactics. A tactical task is a contextually determined complex issue (problem) that arises at a certain point in the investigation process with a limited, fully localized scope of implementation, of an intermediate nature, designed to identify the separate facts about individual elements or circumstances of the crime by using purely tactical solutions [9, p. 16]. In this sense, tactical tasks defined within the investigation of a particular crime group play a key role in the tactics of investigative (search) actions, in particular control over crime commission. Thus, the choice of specific form of control over crime commission is shaped by actual tactical conditionality.

RESEARCH METHODOLOGY

In order to determine the organizational and tactical peculiarities of control over cybercrime commission and formulate practical recommendations for the organization of this investigative (search) action during the investigation of cybercrime authors used systemic, structural, aristotelian, statistical, formal-legal and logical-legal research methods. The statistical method was chosen as a basis for collecting and developing an empirical research foundation - interviewing law enforcement practitioners; processing questionnaire materials, materials of criminal proceedings collected within the territory of Ukraine.

RESULTS

According to the analysis of the materials of domestic investigative and judicial practice, a special investigative experiment is the most common form of control over cybercrime commission (65% of criminal proceedings materials). It stipulates creation of appropriate conditions in a situation as close as possible to the real one by investigative and operational unit in order to verify the real intentions of a person whose actions are indicative of a serious or especially serious crime commission along with monitoring of one's behavior and certain decisions made concerning the crime [10].

Crimes committed in cyberspace are usually very sophisticated and seldom limited to a single episode [11]. Taking the abovementioned into account, investigator should focus on the moment of actual criminal activity fixing. Facts being obtained at this stage must confirm the connection between several crimes. This connection can be traced back to the beginning - motive of the crime. It is the motive that is fused in the causal link between the criminal consequence and criminal act – due to motive certain goals of criminal activity are achieved. The tactical purpose of conducting a special investigative experiment during the investigation of most cybercrime types is to establish the ultimate motive for criminal activity in cyberspace.

In the course of special investigative experiment, when the actual motive of criminal activity performed by particular person is not clear, the investigator or operative staff on one's behalf creates informational environment in cyberspace imitating the crime scene and relevant conditions, expressing interest in a particular outcome of the criminal's actions.

Concerning the organizational and tactical aspects – investigative or operative unit, acting on behalf of the investigator, draws up a plan or several plans during its step-by-step implementation, determining the purpose of a particular (tactical or organizational) measure to control the crime commission, participants, procedure, imitation tools selected for use under Article 273 of the riminal Procedure Code of Ukraine, in particular cash, payment cards, etc. It is important to comply with the information security procedures; in accordance with Article 8(1(4)) of the Law of Ukraine "On State Secret" it covers information on the results of inspections carried out in conformity with the law by the prosecutor, with proper supervision of legislative compliance, and the content of operative and investigative activities, pre-trial investigation and proceedings related to areas mentioned in the article [12]. In European states information security procedures are also enshrined in the law [13]. Special investigative experiment usually stipulates combination of cybercrime fixation with individual audio and videocontrol in the course of tactical operation as identification of motives stimulating certain subjects to communicate is of utmost importance.

Imitation of the criminal environment is not a common form of control over cybercrime commission (only 5% of proceedings). Specific actions are taken by the investigator, the authorized person, using imitation means that will promote others to "immerse" into the criminal environment in order to prevent it and expose an identified or unknown person(-s) who planned or ordered the commission of this crime [10]. Having analyzed the investigative practice we've come to a conclusion that simulation of a crime is limited to the performance of active fake actions by the investigator or operative staff instructed to take action with aim to recreate the event thus conveying the impression of its commission (including the offender). It usually happens at the stage and in cases when the offender is trying to complete a previously initiated crime (he/she has already taken active steps to find the objects for crime commission, the preparation of the crime scene, etc.). The specifics of cybercrimes detection and investigation determine the importance of recording all communication sessions of specific subscribers, which makes it possible to pre-identify a particular perpetrator, as well as to specify the motive of the latter. Therefore, the fixation of the moment when previously commenced cybercrime has been completed occurs only if there is a need to establish the requestor of the cybercrime (unfortunately, judicial practice rarely mentions the existence of such subjects). Such crime will be duly prevented by law enforcement officers. This will be a typical tactical purpose of monitoring the cybercrime commission process through simulation of a crime scene.

Controlled supply /controlled and operative procurement are typically carried out during the investigation of violated procedures for circulation of certain items committed by criminal networks (groups). The purpose is to neutralize the means of conspiracy during commission of crimes in simulated cyberspace environment (trafficking in weapons, ammunition or explosives, narcotic drugs, psychotropic substances or their analogues and precursors).

It should be noted that, in fact, Ukrainian law enforcement agencies currently have lost these forms of activity as a tactical tool for minor crimes investigation, including wide range of

multi-episode cybercrimes. After all, most crimes, detection and cessation of which are attributed to the tasks of NPU Cyber Police Department, are not grave. Part 2 of Article 246 of the Criminal Procedure Code of Ukraine provides for control over the crime commission exclusively in criminal proceedings for serious or particularly serious crimes. Cybercrimes related to serious and especially serious crimes and committed by members of an organized criminal group (90% of materials). In addition, the tactical task of overcoming the conspiracy means used by members of a criminal network arises when information about their activities is identified in the course of preliminary operative and investigative actions.

Forensic aspects concerning the roles of these organized groups' members intersect with the criminological study of network or corporate model serving as reference ones when organized groups are being established, contesting each other [14, p. 81]. The corporate model is characterized by a centralized system with distinct authoritarian features. Criminal networks, in contrast to corporate entities, are unique for their non-permanent membership and high adaptability to political, economic and social changes occurring in public life, without a centralized control system [15, p. 92-93]. A. Osypenko presents the determining factors for the following groups: 1) flexible management; 2) relative equality of group members, the possibility of changing the status (role) depending on the situation; 3) the ability to quickly change the composition of the group and redistribution of roles; 4) fast restoration of deteriorated criminal ties; 5) ability to perform the same criminal task using a different algorithm of actions [16]. The real number of such groups in cyberspace remains outside the official statistics, because only the analysis of resources chosen by the offender as objects of encroachment and means (methods) of operation will allow to conclude that the latter are not available to a single perpetrator or small cluster, therefore may be committed only by an organized group.

Controlled supply or establishment of control over import, export, transit by road, rail, air, sea and other modes of transport through the territory of Ukraine of any goods, objects, substances (when purchasing weapons, explosives, radioactive substances, valuable cultural artefacts, jewelry, human organs via Internet) are are aimed to determine the composition of a criminal group, members of which use the means of conspiracy thus obstructing the determination of their direct participation (role) in the commission of crimes in cyberspace. This action subsequently presupposes notification of the foreign competent authorities about the transportation of encroachment objects through their territory in case of conventional cybercrimes commission, organization of further cooperation in order to expose the full scope of activities performed by the criminal group. Under these conditions, the investigation of cybercrime should stipulate implementation of international cooperation measures which can be described as the activities of the competent authorities, regulated by provisions of international and national law, carried out within criminal proceedings and aimed at achieving its objectives [17, p. 244].

In general, it should be borne in mind that interstate cooperation as an element of fight against crimes of international significance, which include cybercrime due to established international relations, can be defined as the set of activities performed by states, their competent authorities, international organizations based on provisions of international and national law and is aimed at the investigation, prosecution, judicial consideration and prevention of crimes of international significance with relevant obligations of states enshrined in various international treaties [2, p. 229].

Operative procurement stipulates simulation of the purchase or receipt, in particular free of charge, goods, the circulation of which is limited or prohibited by applicable law from individuals and legal entities, regardless of ownership form, in order to expose and record the crime and identify the perpetrator. The criterion used to distinguish between controlled and operative procurement seems obvious – the subject of its performance: for controlled procurement usually it is a product circulating freely; for operative – goods circulating with certain limitations or fully prohibited by law. Therefore, the legislator's consolidation of these two forms into one is not entirely justified.

At the preparation stage investigator evaluates the situation, specifies the tasks (identification and neutralization of the conspiracy means), decides whether it is sufficient to perform this action, initiates (for the prosecution) and justifies the need to launch the case with relevant facts and materials.

After all, its implementation is often associated with the need to use special equipment as a means of control and fixation of moving objects, and, secondly, these forms of control over crime commission are accompanied by covert organizational and tactical techniques of a covert nature, which still remain outside the competence of many low-level (district) police investigators. Therefore, investigators take an active part only at the planning stage, can on a daily or step-by-step basis monitor the fixation results from the operatives and adjust the tactics of subsequent investigative (search) actions.

Techniques and methods of controlled supply, controlled and operative procurement are determined by the characteristics of its implementation subject. For crimes committed in cyberspace, the latter is a prerequisite for the encroachment object to emerge and therefore, controlled supply, controlled and operative procurement are accompanied by another covert investigative (search) action – the removal of information from transmitting telecommunications networks, including extraction from communication channels. The use of such investigative (search) actions algorithm allows the investigator to expand the time limits of documentary crime commission support, to record not only the acquisition, receipt or movement of prohibited or restricted goods, but also, as justified by the analysis of practice, the circumstances of its manufacturing, use, copying, distribution in other way (use of certain computer technology), etc.

In some cases, control over crime commission in the form of controlled supply, controlled and operative procurement during the investigation of illicit acquisition, sale of narcotic drugs, psychotropic substances or their analogues and precursors related in cyberspace may be carried out to identify sources and channels of narcotic drugs, psychotropic substances and precursors trafficking (Articles 4, 5 of the Law of Ukraine "On measures aimed to combat narcotic drugs, psychotropic substances and precursors trafficking and abuse" [18]). Under such circumstances, the offender is not always immediately arrested at the crime scene. Given the negative prospects of assessing the results of crime commission control as evidence in practice, there are many cases when crime fixation is subject to duplication (after the next episode of criminal activity by carrying out a similar action). In this case, the prospect of assessing the control results seems doubtful because the court may conclude that person was provoked (incited) to commit the following episode of criminal activity.

Provocation - intentional unilateral actions of a person (provocateur), aimed at involving the person being provoked in the crime commission with aim to expose the latter. Moreover, provocation differs from incitement and does not involve accompliceship [19, p. 4]. That is why during the control over crime commission of a it is prohibited to provoke (incite) a person to commit this crime with aim of further exposue, helping the person to commit a crime one would not commit otherwise if an investigator, operative unit staff or a person involved in this action did not contribute to this process, or to influence one's

behavior through violence, threats, blackmail for the same purpose.

To find a solution for this problem we must refer to judicial practice. The Plenum of Superior Specialized Civil and Criminal Court of Ukraine in its resolution №6 (paragraph 16) "On the legal position of the High Specialized Court for Civil and Criminal Cases" of June 3, 2016 which contained certain statements related to provocation during the mentioned procedure noted that in accordance with the practice of European Court of Human Rights, namely in the case "Barannikov v. the Russian Federation" of November 4, 2010, "Veselov and Others v. the Russian Federation" of October 2, 2010, use of special investigative methods - in particular, intelligence methods – basically does not lead to any violation of the person's right to fair trial [20]. The risk of provocation by law enforcement officers stimulated by these methods means that its use must be strictly regulated. To apply these methods, law enforcement agencies must obtain evidence to support the statement regarding person's propensity to commit a crime. The European Court of Human Rights has established, in particular, the following criteria:

- Whether the law enforcement agencies were active, whether there was an incentive on their part to commit a crime, for example, initiating contacts with a person, repeated offers despite the initial refusal of the person, persistent reminders, considerable price boost;
- Whether the crime would have been committed without the intervention of law enforcement agencies;
- Substantiation of reasons for the operative procurement, whether the law enforcement agencies had objective data of person's involvement in criminal activity and significant probability of committing a crime. Any conclusion made concerning the provocation occurrence is not legitimate if circumstances are not analyzed and assessed properly. Such legal opinion is formulated in detail in decision of Superior Specialized Civil and Criminal Court of Ukraine Plenum dd. March 31, 2015 (case № 5-872km15) [21].

Therefore, if the initiative to communicate with a person was expressed by the law enforcement agency, and the moment of person's exposure to crime commission becomes easily predictable due to artificially induced interest in achieving a certain result, then items and documents obtained in this manner can not be used in criminal proceedings. We emphasize that, in fact, the artificiality of criminal environment created intentionally in advance by the operative unit precedes other forms of control over cybercrime commission. This environment is mostly of informative nature (for example, providing information on the sale of goods with restricted/prohibited circulation, on the provision of services for malicious software design, the provision of other information that allows to determine the criminal propensity of a person). Purposeful placement of information by an operative staff pretending to be a regular user in thematic online communities (online stores, bulletin boards, sites distributing, audio/ video products, pornography etc.) essentially contests the legality of the following covert investigative (search) action with crime provoking. In this sense, it is deemed feasible to use special analytical systems [22] and use the practice of EU states police who continuously maintain their presence in Darkweb networks [23].

CONCLUSIONS

Control over crime commission is an element of forensic tactics – formats of its optimization are to be identified in the context of performance tactics specificity within the investigation of separate crime group/category. Peculiarities of certain control type selection, analyzed through the prism of tactical need for this covert investigative (search) action to be performed during the cybercrime investigation, allowed us to formulate the following tactical recommendations with aim to optimize the tactics of its performance in the selected crime category.

Firstly, the tactical purpose of crime commission monitoring in the form of a special investigative experiment is to establish the ultimate motive for criminal activity performed in cyberspace; in the form of criminal environment imitation – to establish the requestor of a committed cybercrime; in the form of controlled supply / controlled and operative procurement - overcoming the means of conspiracy used by members of a criminal network.

During the investigation of a specific cybercrime, the initiator, guided by the investigative situation, with certain practical considerations establishes the predominant organizational and tactical purpose of this covert investigative (search) action and chooses a specific form of control over crime commission.

Secondly, direct control over crime commission is entrusted to the operative unit. Regarding the organizational and tactical aspects, investigative or operative unit, acting on behalf of the investigator, draws up a plan or several plans during the active stage, determining the purpose of a particular (tactical or organizational) measure to control the crime, participants, procedure, selected simulation tools. Investigator may on a daily or step-by-step basis monitor the results of actions performed by the operative unit and adjust the tactics of subsequent investigative (search) actions in accordance with the information obtained.

Thirdly, controlled supply, controlled and operative procurement are chosen as a tactical tool to investigate serious and especially serious cybercrimes, including the acquisition or sale of weapons, ammunition or explosives, the illegal acquisition, sale of narcotic drugs, psychotropic substances or their analogues and precursors. Tactical recommendations, methods and techniques of controlled supply, controlled and operative procurement are determined by the characteristics of its implementation subject.

Control over crime commission, depending on its form, is accompanied by other covert investigative actions, in particular - the removal of information from transmitting telecommunications networks. In particular, controlled delivery, controlled and operative procurement are often followed by the withdrawal of information from communication channels; special investigative experiment - audio, video control of a person and / or location. This allows to expand the time limits of the crime commission documentary support.

Finally, the issue of provoking (inciting) a person to commit crimes raises the question; how qualified and active are the operational units employees as members of thematic Internet communities (in order to identify individuals and facts). Law enforcement officers can only be passive users in thematic online communities in order to detect individuals and facts of potential investigative/operative interest.

REFERENCES

1. Edwards B., Hofmeyr S., Forrest S. Hype and heavy tails: A closer look at data breaches. Journal of Cybersecurity. Volume 2, Issue 1, December 2016, Pages 3-14.
2. Yuliia Chornous. Forensic support of crime investigation: monograph. Vinnytsia: Nilan-LTD, 2017. 492 p.
3. Convention on Cybercrime: adopted on November 23, 2001. Additional Protocol to Convention dd. January 28, 2003; ratified with cautionary statements by the Law of Ukraine № 2824-IV dd. September 7, 2005 Verkhovna Rada of Ukraine: [website]. URL: https://zakon.rada.gov.ua/laws/show/994_575
4. Criminal Code of Ukraine: Law of Ukraine № 2341-III dd. April 5, 2001. Verkhovna Rada of Ukraine: [website]. URL: http://zakon4.rada.gov.ua/laws/show/2341-14.
5. Criminal Procedure Code of Ukraine: Law of Ukraine №

4651-VI dd. April 13, 2012. Verkhovna Rada of Ukraine: [website]. URL: https:// zakon.rada.gov.ua/laws/show/4651–17.
6. M. Bahrii. Imitation of the criminal environment: concept, content, place in the system of covert investigative (search) actions. Comparative-analytical law. 2015. № 4. p. 371–374.
7. V. Dintu. Special investigative experiment as a form control over crime commission. Comparative-analytical law. 2014. № 4. p. 184–186.
8. M. Hribov. Division of special investigative experiment and simulation of criminal environment. Scientific Journal of National Academy of Internal Affairs. 2016. № 4 (101). p. 64–73.
9. V. Zhuravel. Tactical tasks of investigation and performance mechanism. Theory and practice of forensic examination and criminalistics. 2017. Vol. 17. p. 11–18.
10. Order of Prosecutor General's Office of Ukraine, MoI of Ukraine, Security Service of Ukraine, Administration of State Border Service of Ukraine, Ministry of Finance of Ukraine, Ministry of Justice of Ukraine dd. November 16, 2012, № 114/1042/516/1199/936/1687/5. Verkhovna Rada of Ukraine: [website]. URL: https://zakon2.rada.gov.ua/laws/show /v0114900-12.
11. Akhgar B., Staniforth A., Bosco F. Cyber Crime and Cyber Terrorism Investigator's Handbook. 2014, 306 p. Pages 1-10. https://doi.org/10.1016/B978-0-12-800743-3.00001-3.
12. Law of Ukraine "On State Secret" № 3855-XII dd. January 21, 1994. Verkhovna Rada of Ukraine: [website]. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
13. Rosén, G. (2018). Contestation and co-optation: why secrecy in EU external relations varies. West European Politics, 41:4, 933–957. DOI: 10.1080/01402382.2017.1413217 (in Eng.)
14. V. Korzh. Theoretical background of investigative methodology: crimes committed by organized criminal groups in economic sector: monograph. Kharkiv, 2002. 412 p.
15. Transnational organized crime: definitions and reality: monograph / edited by V. Nomokonov. Vladivostok: Far East University, 2001. 375 p. (81).
16. A. Osypenko. Organized crime in Internet. Journal of Voronezh Institute of MoI of Russian Federation. 2012. № 3. p. 10–15.
17. Yuliia Chornous. Forensic support of pre-trial investigation: crimes of international significance: thesis … LLD: 12.00.09. Kyiv, 2013. 556 p.
18. Law of Ukraine "On measures to counteract the illegal turnover and abuse of narcotics, psychtropic substances and precursors" № 62/95-BP dd. February 15, 1995. Verkhovna Rada of Ukraine: [website]. URL: https://zakon.rada.gov.ua/laws/ show/62/95-%D0%B2%D1%80.
19. Y. Govorukhina. Concept and legal consequences of provocation in criminal law: thesis abstract …Doctor of Philosophy in Law: 12.00.08. Rostov-on-Don, 2002.
20. Legal opinions of the Superior Specialized Civil and Criminal Court of Ukraine: Resolution of Superior Specialized Civil and Criminal Court of Ukraine Plenum dd. June 3, 2016 N 6. Verkhovna Rada of Ukraine: [website]. URL: http://search.ligazakon.ua/l_doc2.nsf/link1 /VRR00201. html
21. Decision of Judge Panel (Criminal Case Chamber of the Superior Specialized Civil and Criminal Court of Ukraine dd. March 31, 2015, case № 5-872км15. Unified State Register of Court Decisions: [website]. URL: http://reyestr.court.gov.ua/Review/43409601.
22. Caines A., Pastrana S., Hutchings A. et al. Automatically identifying the function and intent of posts in underground forums. Crime Sci. 2018. URL: https://link.springer.com/article/10.1186/s40163-018-0094-4#citeas; https://doi.org/10.1186/s40163-018-0094-4
23. Seminar Policing Crime on the Darkweb 24 November 2017. Cyber Science Center. URL:https://cybersciencecenter.nl/policing-the-darkweb/ seminars/
24. Yuliia Chornous, Svitlana Pylypenko, Olga Vakulyk, Hanna Bidniak, Anatoliy Ostapchuk. Current challenges of international cooperation in the area of human trafficking countering. International Journal of Advanced Science and Technology. Vol. 29, No. 8s, (2020), pp. 2344-2353.
25. Nadiia R.P., Oleksandr G.V. Strategic planning of the socio-economic development of Ukraine: Conceptual aspects. International Journal of Scientific and Technology Research. 2020. http://www.scopus.com/inward/record.url?eid=2-s2.0-85082866364&partnerID=MN8TOARS.