March-April 2020
ISSN: 0193-4120 Page No. 6797 - 6806

# Features of the Investigation of Crimes in the Field of It: The Current State and Prospects for Development

Yuliia Chornous [1] Denys Shylin [2]Liubov Omelchuk [3]Anastasiia Antoniuk [4] and Vadym Pozhar [5]
[1] National Academy of Internal Affairs, Ukraine
[2] National University «Odesa Law Academy», Odesa, Ukraine
[3]University of the State Fiscal Service of Ukraine, Ukraine
[4]University of the State Fiscal Service of Ukraine, Ukraine
[5] National University «Odesa Law Academy», Odesa, Ukraine

***Article Info***
***Volume 83***
***Page Number: 6797 - 6806***
***Publication Issue:***
***March - April 2020***

***Abstract:***
The rapid scientific and technological progress and the development of Internet technologies make it possible to open up great opportunities for its social and economic development. At the same time, the results of scientific and technological progress create new prospects for the commission of various crimes. The analysis of legislation, special literature, and practice materials shows that, with considerable attention to the problems of Internet crimes, the features of their investigation remain insufficiently covered in the scientific literature today and are underdeveloped in practice. This determines the relevance of the topic of this article. The purpose of this work is to identify the features of the investigation of crimes in the field of IT, as well as to clarify the current state of investigations of this category of crimes and prospects. The object of the study is the crimes in the field of IT, as well as the public relations associated with their commission. The subject of the study is the mechanism of committing crimes in the field of IT, the patterns of occurrence of traces and features of their investigation activities. The research methodology is a general scientific and special methods of scientific knowledge. As a result of the research, the features of the investigation of crimes in the field of IT were identified; the specifics of the organization and planning of the initial and subsequent stages of investigation of crimes in this category are established; formulated typical investigative situations that may arise during the investigation of the specified category of crimes; the tactics of conducting individual investigative actions of the initial and subsequent stages of the investigation (review of the scene, interrogation, search, seizure) are investigated, as well as the prospects of the development of IT crimes are investigated and recommendations for their investigation are developed and offered.

***Keywords:*** *forensic characteristics, information technology, investigations, IT-crimes*

***Article History***
***Article Received****: 24 July 2019*
***Revised****: 12 September 2019*
***Accepted****: 15 February 2020*
***Publication****: 05 April 2020*

## I. INTRODUCTION

The further development of modern information technologies, the improvement of production and the expansion of the scope of the latest cybernetic technology have enabled the emergence of new types of crimes where computer equipment and electronic information are the objects of unlawful encroachment. In addition, at this stage of technology development, there is a shift from simple single crime in the field of Information Technology to organized (complex). Its transnational character is observed, which, in turn, complicates the possibility of detection and investigation of this category of crimes by law enforcement officials of different states.

For the first time, IT crimes were formed in 1979 at a conference of lawyers in the United States, and two decades later, the United Nations leadership classified cybercrime into industrial espionage, sabotage (criminals terrorize the email owner by interrupting the work of defenseless information ); vandalism (alteration or destruction of data), spoofing (the use of various tricks to steal private information), child pornography (child molestation in any country), gambling (common in countries

where gambling is licensed or prohibited), fraud (seizure of someone else's property or right to it), cracking (removal of protection from software), sending messages of various nature - popularly called "spam"; phishing (access to private data: passwords, bank card details, etc.), computer virus (making copies of one file and distributing it to disrupt work: deleting files, blocking users, etc.), hacking (hacking websites to change information); carding (stealing of requisites for carrying out illegal financial transactions), Dos attacks (actions that cause denial of service (PC "hang-ups"), etc.).

According to Art. 17 of the Constitution of Ukraine (1996), the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the cause of the entire Ukrainian people.

The proliferation in Ukraine of crimes related to IT, unauthorized use of computers, automated systems, and computer networks and telecommunication networks has led to the separation in the Criminal Code of Ukraine (2001) (hereinafter referred to as the CC of Ukraine) of crimes committed in the sphere of use electronic computers (Chapter XVI: Art. 361 – 363-1) as a separate group. Nevertheless, this section does not cover the full range of IT crimes and does not fully reflect their particularities.

This confirms the need for research and grouping of this category of crime, to open up and analyze different approaches of scientists to the formation of debatable questions concerning the actual problems of the specified crime, and also to offer the vision of some aspects of research of this type of crime.

In view of the above, it is important to investigate the peculiarities of the investigation of crimes in the sphere of IT, to analyze the current state and prospects of development, to analyze the provisions of legislation governing their application in Ukraine and foreign countries, and to examine theoretical developments in the investigated issue.

## II. METHODOLOGY

To achieve the purpose of this article, to ensure the reliability of the results obtained, a set of general scientific and specific research methods were applied. Thus, such methods as dialectical, analysis, synthesis, deduction, systemic-structural, concrete-sociological, and formal-logical were used.

The methodological basis of this study is the general dialectical method, based on which all phenomena are investigated in their relationship, in the unity of their social content and legal form, as well as special methods:

– analysis, synthesis, deduction – during the research of normative acts, reports of law enforcement agencies of Ukraine, scientific concepts included in the subject of research;

– systemic-structural method – when considering varieties of the studied group of crimes; development of typical investigative situations, tactical tasks, versions, and means of their solution at the initial stage of investigation;

– comparative-legal method – during the investigation of criminal, criminal procedure, information legislation of different states;

– specific-sociological method – was used to obtain additional information about the mechanism of committing crimes using information technologies, as well as about the peculiarities of their investigation.

– formal-logical method – to identify and characterize the notion of unauthorized interference, computer crimes, forensic techniques, methods, and means.

All research methods were used in conjunction, which provided convincing and reliable scientific results.

Besides, it is necessary to highlight the regulations and programs of the Government, which set out provisions for the investigation of crimes in the field of IT. Among them are the following:

1. The Constitution of Ukraine (1996).

2. Council of Europe Convention on Cybercrime: Adopted by the Council of Europe on 23 November 2001.

3. The Criminal Code of Ukraine dated April 05, 2001 No. 2341-III.
4. Criminal Procedure Code of Ukraine of April 13, 2012 No. 4651-VI.
5. Law of Ukraine "On Information Protection in Information and Telecommunication Networks" of July 5, 1994, №80 / 94-BP.
6. Law of Ukraine "On Information" of October 2, 1992 No. 2657-XII.
7. Law of Ukraine "On the Fundamentals of National Security of Ukraine" of June 19, 2003 No. 964-IV.
8. Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" of October 5, 2017 No. 2163-VIII.
9. Law of Ukraine "On Ratification of the Convention on Cybercrime" of September 7, 2005 No. 2824-IV.
10. Onratification of the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature through computer systems: Law of Ukraine of July 21, 2006 No. 23-V.).

## III. ANALYSIS OF RECENT RESEARCH

Questions and problems of investigation of computer crimes and crimes in the field of Internet technologies were investigated by such scientists as Bilenchuk, Gel, Semakov, Volobuev, Golubev, Gavlovsky, Tsymbalyuk, Karchevsky, Motlyakh, Polivanyuk, Romanyuk, Tischenko E., Tischenko V., Bartsitska.

Thus, the object of the study of scientists Bilenchuk, Gel, and Semakova(2007) was forensic tactics and techniques for investigating individual crimes. Moreover, in his articles, Volobuyev (1996) deals with the problems of investigation of "computer" crimes.

Moreover, Golubev, Gavlovsky, and Tsymbalyuk(2002) analyzed the problems of combating crimes in the field of computer technology and explored the issues of information security. Karchevsky (2012) investigated the issue of criminal-law protection of information security of Ukraine.

Furthermore, Motlyakh(2002) analyzed the tactical foundations of information technology crime searches and formulated proposals to investigate the investigated category of crimes. Polivanyuk's(n.d.) article deals with the peculiarities of the use of specialized knowledge in the investigation of criminal offenses related to the use of computer technologies.

In addition, Romanyuk, Gavlovsky, Gutsalyuk, Butuzov (2004) in their research drew attention to the detection and investigation of crimes committed in the field of information technology. Besides, Tyshchenko E. (2010)deals with the peculiarities of the investigation of computer crimes [19]. Also, Tischenko V. (2017, 2012) and Bartsitskaya(2012) in their work analyzed the formation of a technological approach as an innovative direction of the development of forensics.

From the above literature analysis, we can conclude that scholars pay sufficient attention to the study of computer crimes and crimes in the field of IT. However, currently no comprehensive study would highlight the particularities of Internet technology crime investigations. This fact necessitates the study of the features of the investigation of crimes in the field of Internet technologies, to find out their current state and prospects for development.

## IV. RESULTS

In the age of information technology, it is extremely difficult to feel secure in the information space. With the advancement of technology, the number of crimes in this area is increasing rapidly, and Ukraine, like all countries in the world, faces cybersecurity challenges every day.

In Ukraine, the relevant laws and regulations governing relations in this area are adopted at the legislative level, namely the Constitution of Ukraine (1996), the Criminal Code of Ukraine (2001), the laws of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine" (2017), "On information"

(1992), "On Information Protection in Information and Telecommunication Networks" (1994), "On Basic Principles of Cyber Security of Ukraine" (2003) and the Council of Europe Convention on Cybercrime (2001) and other international treaties, the consent of which was provided by the Verkhovna Rada of Ukraine.

The main articles of the CC of Ukraine (2001), which investigate crimes in the sphere of IT in Ukraine, are Art. 176 of the CC of Ukraine "Copyright and Related Rights Violations"; Art. 190 of the CC of Ukraine "Fraud"; Art. 361 of the CC of Ukraine «Unauthorized interference with the work of electronic computers (computers), automated systems, computer networks or telecommunication networks»; Art. 361-1 of the CC of Ukraine "Creation with the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale"; Art. 361-2 of the CC of Ukraine "Unauthorized sale or distribution of restricted access information stored in electronic computers (computers), automated systems, computer networks or on such media"; 362 of the CC of Ukraine "Theft, misappropriation, solicitation of computer information or taking it by fraud or abuse of office"; Art. 363 of the CC of Ukraine "Violation of the rules of operation of automated electronic-computer systems"; Art. 363-1 of the CC of Ukraine "Obstruction of the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks by mass communication of telecommunication messages".

To increase the detection and proper investigation of the above crimes, there is a need to analyze the particularities of investigating such crimes to date and the prospects for development.

During the investigation of crimes related to the field of IT, there is a need for various investigative actions: inspection (for example, places of events, objects, and documents), search, seizure, seizure of property, questioning, face-to-face, presenting for identification, obtaining samples for expert research, and expertise. The specificity of individual investigative actions, their complexes is determined by the peculiarity of this type of crime, namely the peculiarity of the method of committing this crime, the identity of the offender, purpose, etc.

One of the primary investigations into IT crime investigations is the on-site inspection of an incident that can be conducted on-site to store and process computer-generated criminal information. At the same time, it should be noted that specialists should be involved in the inspection of the venue. They must also have a thorough knowledge of computer hardware and software. The location inspection should be preceded by the coaching of the investigation team, specialist consultations, preparation of computer equipment and equipment for the location inspection. Particular attention should be paid to thorough procedural and forensic methods of fixing the course and results of this investigative action. If the site review of cases of unauthorized interference with the operation of electronic computers (computers), systems and computer networks conducted following scientific recommendations will facilitate a systematic and comprehensive search for traces of criminal activity, their removal, successful preliminary investigation and receipt forensically relevant information at the initial stage of the investigation.

Equally important in the investigation of such a category of crimes is a properly conducted search. Thus, any investigative (search) action is effective only under the condition of its preliminary preparation. Searching for a computer crime trace should begin with identifying the on-site computer hardware connections that trace the crime, and investigating the information associated with those connections computers that are the endpoints of a route.

A special place in the investigation of computer crimes belongs to the interrogation of suspects, witnesses, and victims. The organization of the interrogation of the suspect involves the preparation of technical means of interrogation, objects, physical evidence, which the investigator plans to present to the person. Before conducting the interrogation, it is

necessary to examine the identity of the suspect by familiarizing himself with the materials available in the criminal case: characteristics from the place of work, training, testimony of witnesses, victims; data obtained during the conduct of search operations, the results of its monitoring, etc.; criminal case materials where a person has previously been criminally liable (if possible). The information obtained by the investigators allows establishing psychological contact with the interviewee, to choose the most rational system of tactical methods of interrogation, to determine the nature and condition of the possible and most effective psychological influence and to predict possible ways of counteraction by the interviewee. It should also be noted that IT witnesses might be persons who observed the crime (especially with direct access) or individual moments and also saw the offenders at or after the crime. It is advisable to question a wide range of individuals as witnesses, such as computer operators, programmers, information security officer, or a database administrator, head of a computing center, or a manager of an enterprise, institution, and organization.

Also, the peculiarities of the investigation of this category of crimes are manifested in the conduct of unspoken investigative (investigative) actions. When preparing or agreeing on a request for the conduct of an unlawful investigative action of a prosecutor (procedural supervisor), it should be borne in mind that the basis for conducting a specific unlawful investigative action is the availability of information that needs to be verified about the crime and the person who committed it, to confirm or refute them, unless otherwise possible, other than carrying out an implicit investigative (search) action, to obtain information. However, in the criminal proceedings of the specified category, there are problems with the practical application of the requirements for disclosure to the party of the protection of materials related to the sanctioning of conducted unspoken investigative (search) actions, in the presence of restricted information in them and the possibility of their declassification at the stage of judicial review. Moreover, it should be noted that the law does not regulate the issue of declassifying the decisions of investigative judges of appellate courts for granting permissions to conduct unspoken investigative (investigative) actions, in connection with which the courts reject the respective written appeals of prosecutors, which in the future negatively influences the disclosure of crimes in IT sphere.

Each investigative action has several peculiarities of conducting it following the Criminal Procedure Code of Ukraine (2012), as well as developed recommendations for conducting investigative actions to avoid procedural irregularities and to obtain evidence that will facilitate a proper investigation of the case and its further consideration in court.

The use of specialized knowledge plays an important role in investigating crimes involving unauthorized interference with computers, automated systems, and computer networks and the telecommunication network. The most common form of application of specialized knowledge in criminal proceedings is forensic examination. The peculiarity of the examination in this category of crimes is that to investigate the information contained on computer media, the expert is provided with a computer medium himself, and if necessary, a computer block (a complex of computer tools, which includes test carrier). To ensure that the information provided to the research media is kept in working order, they are individually packaged (the PCs must be packed in such a way as to prevent access to the media directly or to connect the system unit to the power supply).

Other investigations may be used in the investigation of IT crimes. For example, tracology for the analysis of fracture traces, and dactyloscopic for the analysis of traces of hands-on both the external and internal surfaces of computers and components. Forensic examinations are intended if, for example, crimes in the use of electronic computers, systems and computer networks and telecommunication networks are related to offenses in the financial and financial sphere. The forensic examination of documents is quite widespread when the computer is used as a

means of making counterfeit documents, counterfeit paper money and more. Phonoscopic examination is assigned when negotiating listening equipment is used. The use of specialized knowledge in the investigation of crimes in the field of IT is necessary to: determine the status of the object as a machine carrier of information, its status, purpose, and features; research of computer information, including its search and seizure; identification of signs and traces of influence on the media, as well as on the information itself; the use of ancillary measures to identify, record and remove physical evidence.

Thus, the aforementioned investigative actions, their proper organization, and implementation play an important role in the work of IT-crime investigators. However, investigative tactics in investigating crimes involving unauthorized interference with computers, automated systems, computer networks, and telecommunication networks require further active research and practical refinement.

It is important to analyze the international experience of securing, preventing, detecting and combating investigated crimes to find out the specifics of investigating IT crimes.

Consider the foreign experience of the UK, Germany, France, and Poland.

Thus, when considering the countries of Europe, one should pay attention to the experience of the UK, in which cybersecurity is provided at a high level. The main document aimed at ensuring cybersecurity in the UK is the national cybersecurity strategy for 2016-2021 (2016). It should also be noted that the aforementioned Strategy addresses cybercrime in the context of two interrelated forms of criminal activity: cyber dependence of crimes, that is, crimes that can only be committed the use of information and communication technology devices, where these devices are tools for crime and the purpose of crime and crimes related to the use of cyberattacks – traditionally crimes that can be increased in scale or covered by computers, networks or other information and communication technologies.

Germany is the next European country that is worth the experience. In 2011, the German National Cyber Security Strategy was adopted, according to which the federal government applies measures based on structures already in place to the appropriate levels of threats, and enhances the capacity of law enforcement agencies. In July 2015, the German IT Security Act was adopted in Germany to prevent attacks on important information systems. The law sets minimum cybersecurity standards for more than 2,000 carrier companies. These standards should be ensured through the improvement, accessibility, authenticity, confidentiality, and integrity of IT security throughout Germany; improving the level of security of citizens; the best value of important infrastructure.

Moreover, Poland also pays attention to ensuring IT security. In recent years, Poland has demonstrated a consistent state policy against cyber threats. For example, Poland has taken several measures that have taken it to a new level in ensuring the security of information, namely the adoption of amendments to the legislation, which allow introducing a state of emergency in the case of an attack in virtual space. In 2011, the Ministry of Administration and Digitization was set up to ensure cybersecurity in the military sphere, protect the privacy of citizens, build a national educational platform, and engage the elderly and remote areas of the country. Within the Ministry of Digitization, in 2016, they established a National Cyber Security Center, whose key objective was to prevent, respond to, and coordinate threats. Poland has also developed a new cybersecurity strategy. It stipulates that by 2020 the authorities will guarantee the security of citizens, economic operators, and government agencies in the field of cybersecurity. The systematic approach and the introduction of effective counter-tools do not indicate that Poland has coped with the threats, which means that this country has made significant steps to ensure cybersecurity.

Considering the experience of France, it is worth noting that the normative act defining the strategic directions of France's national security policy is the

FrenchWhite Paperon Defenseand NationalSecurityof 2008 and the National Digital Security Strategy of 2015. Thus, in the FrenchWhite Paperon Defenseand NationalSecurity (2008) among the most likely threats to the territories of France and the European community are the large-scale attacks on information systems; espionage and strategic influence. As for the National Digital Security Strategy (2015), it aims to follow the digital transition of French society and respond to the new challenges of information technology. It is also worth noting that France, in particular, participated in five groups of United Nations government experts on cybersecurity, whose assistance facilitated the deployment of cyberspace in the international system created by the Charter of the United Nations, and directed states to prevention, Collaboration, and Proliferation in Cyberspace Crime.

As regards the perpetuation of IT crimes, criminal liability for such crimes is provided for in the Criminal Codes of foreign countries such as Austria, Belgium, Republic of Belarus, Republic of Bulgaria, Republic of Armenia, Georgia, Denmark, Republic of Kazakhstan, Latvia, Republic of Moldova, The Netherlands, the Federal Republic of Germany, the Republic of Poland, the Russian Federation, the Republic of San Marino, Turkey, the Republic of Uzbekistan, France, Switzerland, Sweden as they are within those geopolitics institutions that developed and adopted international standards for criminal liability for crimes in the field of computer information.

It should also be noted that to ensure international security and counteract cybercrime, the Council of Europe has adopted the Convention on Cybercrime (2001), which was ratified by the Law of Ukraine "On Ratification of the Convention on Cybercrime" of September 7, 2005. Also, the Law of Ukraine of 21 July 2006 ratified the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature through computer systems. The above documents set out international standards for the criminalization of socially dangerous acts in the field of computer information and set out specific provisions for establishing responsibility for crimes in the said area, which are subject to mandatory implementation in the national legislation of Ukraine. These provisions should include Articles 2 to 6 of Title 1, "Offenses against the confidentiality, integrity, and availability of computer data and systems" of the Convention on Cybercrime of 23 November 2001, and Art. 3 CIS cooperation agreements on combating computer information crimes of June 1, 2001, which are specifically aimed at protecting public relations in the field of computer information. However, an analysis of November 23, 2001, Convention on Cybercrime shows that the criminal liability law of Ukraine does not fully reflect the requirements of international legal acts to establish responsibility for crimes in the field of computer information. This requires determining the appropriate proposals to bring the Criminal Code of Ukraine in line with these acts. The provisions of the heading "Offenses against the confidentiality, integrity, and availability of computer data and systems" in Part 1, Substantive Criminal Law, of the Convention on Cybercrime of 23 November 2001, and Section 12, Crimes against Information Security, of the Model CIS for the CIS Member States grouped by a generic object - public relations in the field of computer information. This testifies to the expediency of the existence of Section XVI of the Special Part of the Criminal Code of Ukraine, and also confirms the already stated position on changing the name of the said section to "Crimes in the field of computer information", which will serve to bring it in compliance with international standards.

Thus, by analyzing the international experience of securing, preventing and investigating IT crimes, we can conclude that these crimes are often transnational in nature and in the context of globalization, it is necessary to tackle these crimes jointly using the means of international cooperation. Nevertheless, to effectively investigate crimes and ensure information security, states, including Ukraine, must first and foremost establish proper internal mechanisms for investigating crimes and

introduce progressive provisions of international normative legal acts for the sake of uniformity of interpretation of the investigated crimes.

## V. DISCUSSION

Thus, the investigation of crimes in the field of IT has several features. Such features are evident in typical investigative situations and tactical tasks. Unfortunately, to date, the forensic science has not made recommendations on the peculiarities of the use of tactical techniques in the investigation of crimes in the field of IT, and therefore this issue needs further elaboration. In addition, in the investigation of crimes in the field of IT have the features of some investigative (search) actions, such as inspection of the area, premises, things and documents, search, seizure, etc. actions, and the use of specialized knowledge. Proper organization and conduct of investigative (investigative) actions play an important role in the work of employees involved in the investigation of crimes in the field of IT. However, at present, the tactics of investigative action in the investigation of this category of crimes require further active research and practical refinement.

Summarizing the experience of investigating the article investigating crimes in foreign countries,it is safe to say that global trends in the development of information society encourage all countries in the world to take measures to prevent crime and ensure the security of information retention. Ukraine is no exception. An analysis of the experience of the United Kingdom, Poland, Germany and other countries makes it possible to identify the following measures to ensure effective investigation of IT crimes:

1. Increase funding for crime investigators and provide them with advanced technical (software) tools.
2. Improve the quality of education of law enforcement officials.
3. Update the Cybersecurity Strategy by expanding on the issues it should cover.
4. Expand international cooperation in the field of order execution and investigate crimes involving unauthorized interference with computers, automated systems and computer networks and telecommunication networks.
5. To carry out educational activities that will promote the need to protect information among the population (companies).

Therefore, the implementation of the above measures will help to effectively investigate crimes in the field of IT, as well as ensure the security of information for the public. However, as noted above, given the transnational nature of the investigated category of crimes, their effective investigation is possible with proper international cooperation, and therefore Ukraine needs to cooperate with other countries to detect, investigate and investigate IT crimes quickly, in a timely and effective manner.Thus, by analyzing the international experience of securing, preventing and investigating IT crimes, we can conclude that these crimes are often transnational in nature and in the context of globalization, it is necessary to tackle these crimes jointly using the means of international cooperation. Nevertheless, to effectively investigate crimes and ensure information security, states, including Ukraine, must primarily establish proper internal mechanisms for investigating crimes and introduce progressive provisions of international normative legal acts for the sake of uniformity of interpretation of the investigated crimes.

## VI. CONCLUSIONS

1. Therefore, the investigation of crimes in the field of IT has several features. Thus, in the investigation of crimes in the field of IT, practitioners, involved in the investigation of such crimes, have some difficulties, whichis caused by the specific tactics of conducting individual investigative actions and the peculiarity of detecting such crimes.
2. It should also be noted that the development of tactical features of individual investigative actions in the investigation of the studied category of crimes requires further active scientific and practical

research. The further research should take into account the international experience of investigating such crimes and the constant new challenges of technological progress in the case of posting on the Internet information that violates the honor, dignity, and goodwill of the person. He or she can directly appeal to the person who committed the violation, with a request to delete such information, or to court.

## VII. REFERENCES


1. Bilenchuk,P.D., Gel, A.P.,Semakov, G.S. (2007). Forensic tactics and methods of investigation of individual crimes. Retrieved from http://maup.com.ua/assets/files/lib/book/p09_25.pdf.
2. Constitution of Ukraine: Law of June 28, 1996, No. 254k / 96-VR. Revision of September 30, 2016, grounds - 1401-19. (2016). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
3. Council of Europe Convention on Cybercrime: adopted by the Council of Europe on 23 November 2001. (2001). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575.
4. Criminal Code of Ukraine: Law of Ukraine. (2001). Bulletin of the Verkhovna Rada of Ukraine. Retrieved fromhttps://zakon.rada.gov.ua/laws/show/2341-14
5. Criminal Procedure Code of Ukraine of April 13, 2012 No. 4651-VI. (2012). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.
6. “Data Mining Analysis for National Security”, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 7, Issue 3, pp. 19-32
7. FrenchWhite Paperon Defenseand NationalSecurity. (2008).Retrieved fromhttp://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf
8. German IT Security Act. (2015). Retrieved fromhttps://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2
9. German National Cyber Security Strategy. (2011). The European Union Agency for Cybersecurity (ENISA). Retrieved fromhttps://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany.
10. Golubev, V.O.,Gavlovsky, V.O.,Tsymbalyuk, V.S. (2002).Information security: the problems of combating crime in the use of computer technology.Zaporizhzhia: Prosvita.
11. Golubev, V.O.,Gavlovsky, V.O.,Tsymbalyuk, V.S. (2002).Problems of combating crime in the field of computer technology. Zaporizhzhia: State University "ZDMU".
12. “Deformed Identity Crime Detection”, International Journal of Applied Engineering Research and Development (IJAERD), Vol. 4, Issue 2, pp. 81-88
13. Information Protection in Information and Telecommunication Networks: Law of Ukraine of July 05, 1994, №80 / 94-VR. (1994).Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
14. Karchevsky, M.V. (2012). Criminal law protection of information security of Ukraine. Lugansk: RVV LSUVS.
15. Motlyakh, O.I. (2002). Tactical foundations for information technology crime search.Bulletin of the FPU Academy of Labor and Social Relations, 2, 157 - 160.
16. National Cyber Security Strategy 2016 to 2021. (2016). GOV.UK.Retrieved fromhttps://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
17. National Digital Security Strategy. (2015).Retrieved fromhttps://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf
18. On Basic Principles of Cyber Security of Ukraine: Law of Ukraine of June 19, 2003, No.

964-IV. (2003). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/964-15.
19. "Criminal Justice Delivery System in India: An Exploratory Analytical Overview", International Journal of Humanities and Social Sciences (IJHSS), Vol. 7, Issue 5, pp. 65-82
20. On information: Law of Ukraine of October 2, 1992 No. 2657-XII. (1992).Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12.
21. On the basic principles of ensuring the cybersecurity of Ukraine: Law of Ukraine dated 05.10.2017 № 2163-VIII. (2017). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.
22. On the ratification of the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature through computer systems: Law of Ukraine of July 21, 2006 No. 23-V. (2006). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/23-16.
23. "Assessment of Faithbased Crime Preventive Measures in a Third World City: Case of Ifo, Ogun State, Nigeria", International Journal of Humanities and Social Sciences (IJHSS), Vol. 5, Issue 5, pp. 189-200
24. Polivanyuk. V. (n.d.). Use of Special Knowledge in Investigating Criminal Cases in the Use of Computer Technologies.Retrieved from http://www.crime-research.ru/library/Polivan2.htm.
25. Ratification of the Convention on Cybercrime: Law of Ukraine of September 7, 2005 No. 2824-IV. (2005). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2824-15.
26. Romanyuk, B.V.,Gavlovsky, V.D.,Gutsalyuk, M.V.,Butuzov.V.M. (2004).Detection and investigation of crimes committed in the field of information technology. Kyiv: PALIVODA.
27. Tischenko, V.V. (2017). The concept, tasks, and content of the forensic investigation methodology. Odessa: Helvetica Publishing House.
28. "When Virtual World Meets the Real World: Cyber Crime Induced Drug Trafficking", IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL), Vol. 2, Issue 2, pp. 115-126
29. Tischenko, V.V.,Bartsitskaya, A.A. (2012). Formation of technological approach – an innovative direction of development of criminalistics.Actual problems of the state and law, 68, 560-566.
30. Tishchenko, E.F. (2010).Investigation of computer crimes. Scientific-methodical manual.Kyiv: SBU National Academy.
31. "Mapping from Mental State of Brain to the Musical World", BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE), Vol. 4, Issue 1, pp. 7-18
32. Volobuev, V.A. (1996). Problems of investigation of "computer" crimes.Bulletin of National University of Ukraine, 1, 63–70.