УДК 341.1 DOI https://doi.org/10.26661/2616-9444-2021-1-14

Застосування криміналістичної техніки під час досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Проценко М. В.
кандидат юридичних наук, доцент,
доцент кафедри галузевого права
Херсонський державний університет
вул. Університетська, 27, Херсон, Україна
orcid.org/0000-0003-0834-5655
protsenkonv1980@gmail.com

Гавловська А. А.
кандидат юридичних наук, доцент,
доцент кафедри галузевого права
Херсонський державний університет
вул. Університетська, 27, Херсон, Україна
orcid.org/0000-0002-7973-7560
lyolikalina@gmail.com

Ключові слова: *криміналістична техніка, кримінальні правопорушення, розслідування, електронно-обчислювальні машини, комп'ютери, системи, комп'ютерні мережі, мережі електрозв'язку.*

Досліджено застосування криміналістичної техніки під час досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Проаналізовані наявні у сучасній криміналістичній літературі визначення криміналістичної техніки. Зазначені перелік функцій, для виконання яких використовується криміналістична техніка під час розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, відеофіксація результатів проведення слідчих дій у рамках відповідних кримінальних проваджень (оглядів, допитів, обшуків, виїмки, слідчих експериментів тощо), експертне дослідження комп'ютерної техніки, засобів зв'язку, проведення «пошукових заходів на предмет виявлення можливих витоків інформації з обстежуваного приміщення чи конкретної операційної системи, виявлення слідів, розташованих на зовнішніх поверхнях комп'ютерної техніки, окремих її складових частинах, огляду комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. Також досліджено засоби криміналістичної техніки, які використовуються під час розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. А також пристрої для «клонування» носіїв інформації, програмні засоби для криміналістичних досліджень вмісту носіїв інформації та їх образів, ноутбуки з комплексом програмних та апаратних засобів, призначених для дослідження комп'ютерної інформації за межами експертних установ, Хеш набори для фільтрації вмісту файлової системи, що досліджується, з метою відшукання файлів, які створив користувач, пристрої для під'єднання носіїв інформації з апаратним блокуванням здійснення запису на них, програмні засоби для дослідження локальних мереж, апаратні та програмні засоби для дослідження мобільних телефонів, SIM-карт та банківських карт. Зроблено висновки щодо необхідності вдосконалення традиційного підходу до застосування криміналістичної техніки під час розкриття та розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, кримінального процесуального законодавства у частині вимог до доказів вчинення вказаних кримінальних правопорушень.

Application forensic techniques during the pretrial investigation of criminal offenses in the use of computers (computer) systems and computer networks and telecommunication networks

Protsenko M. V.
Candidate of Law, Associate Professor,
Associate Professor at the Department of Branch Law
Kherson State University
Universitetska str., 27, Kherson, Ukraine
orcid.org/0000-0003-0834-5655
protsenkonv1980@gmail.com

Havlovska A. A.
Candidate of Law, Associate Professor,
Associate Professor at the Department of Branch Law
Kherson State University
Universitetska str., 27, Kherson, Ukraine
orcid.org/0000-0002-7973-7560
lyolikalina@gmail.com

Key words: *forensic technology, criminal offenses, investigations, computers, computer systems, computer networks, telecommunication networks.*

The application of forensic techniques during the pre-trial investigation of criminal offenses in the field of use of computers, systems and computer networks and telecommunications networks has been studied. The definitions of forensic technique available in the modern forensic literature are analyzed. The list of functions for which forensic equipment is used in the investigation of criminal offenses in the use of electronic computers (computers), systems and computer networks and telecommunications networks. In particular: video recording of the results of investigative actions in the relevant criminal proceedings (inspections, interrogations, searches, seizures, investigative experiments, etc.), expert study of computer equipment, communications, conducting search activities to identify possible leaks of information from the subject premises or a specific operating system, detection of traces located on the external surfaces of computer equipment, its individual components, inspection of computers, systems and computer networks and telecommunications networks. The means of forensic equipment used in the investigation of criminal offenses in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks are also studied. In particular: devices for "cloning" media, software for forensic research of the content of media and their images, laptops with a set of software and hardware designed to study computer information outside the expert institutions, hash kits for filtering the contents of the file system, under investigation in order to find user-created files, devices for connecting media with hardware blocking of recording on them, software for research of local networks, hardware and software for research of mobile phones, SIM-cards and bank cards. Conclusions are made on the need to improve the traditional approach to the use of forensic techniques in the detection and investigation of criminal offenses in the use of computers, systems and computer networks and telecommunications networks, criminal procedural law in terms of evidence requirements commission of the specified criminal offenses.

Вступ. Розвиток вітчизняного суспільства, запровадження в Україні новітніх технологій вимагає забезпечення надійного захисту від злочинних посягань та інших правопорушень, вчинених у сфері їх застосування.

Вирішальну роль у протидії злочинам, скоєним у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, відіграє вдосконалення методики їх розслідування.

Питанням розслідування злочинів, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, присвячено праці таких учених, як О.І. Мотлях, Л.П. Паламарчук, В.М. Стратонов та ін. Однак, незважаючи на значний внесок указаних учених у розвиток вітчизняної юридичної науки, низка питань потребує подальшого дослідження, низка питань залишається дискусійною. До них належать проблемні питання застосування криміналістичної техніки під час досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Виклад основного матеріалу дослідження. Слушним вважаємо почати розгляд указаних проблемних питань з визначення термінів.

Питанню визначення терміна «криміналістична техніка» присвячено багато досліджень. У т. 3 юридичної енциклопедії, підготовленої авторським колективом на чолі із Ю.С. Шемшученком, дається таке визначення терміна «юридична техніка»: «система технічних прийомів, засобів та методів збирання, дослідження і використання джерел криміналістичної інформації». Автори зазначають, що «до засобів криміналістичної техніки за суб'єктом діяльності належать технічні комплекти: оперативного працівника (валіза інспектора ДАІ, дільничного інспектора), слідчого (валіза, портфель, сумка), прокурора-криміналіста (валіза, пересувна лабораторія), експерта (спеціалізовані лабораторії, фізичні, хімічні, біологічні, пожежно-технічні, вибухотехнічні, автотехнічні, комп'ютерно-технічні, товарознавчі тощо)» [12].

У підручнику «Криміналістика», підготовленому авторським колективом під редакцією В.Ю. Шепітька, надається таке визначення криміналістичної техніки: «це важливий розділ криміналістики, що виник у результаті впровадження досягнень природничо-технічних наук у практику боротьби зі злочинністю. Методи фізики, хімії, біології, медицини та інших галузей знань пристосовувалися для виявлення слідів злочину та отримання інформації з метою кримінального судочинства. Кримінальна, або поліцейська, техніка в XIX ст. заклала підґрунтя сучасної криміналістики». Авторами також надається визначення поняття «науково-технічні засоби криміналістики» – «це прилади, пристосування і матеріали, які використовуються для збирання і дослідження доказів або створення умов, що ускладнюють учинення злочинів». Як зазначають автори підручника, «такі засоби можуть бути розподілені на кілька груп: 1) взяті без змін з різних технічних і природничо-технічних наук; 2) спеціально пристосовані для криміналістичних цілей; 3) спеціально розроблені для цілей криміналістики» [11].

Авторський колектив у складі А.В. Кофанова, О.Л. Кобилянського, Я.В. Кузьмічова та ін. пропонує розглядати поняття криміналістичної техніки у двох значеннях: 1) криміналістична техніка як розділ науки криміналістики (це розділ науки криміналістики, що являє систему теоретичних положень і розроблених на їх основі технічних засобів, методів виявлення, фіксації, вилучення, збереження і переробки інформації про подію, що розслідується, а також технічних засобів і методів запобігання злочинам); 2) криміналістична техніка як технічні засоби, а також їх сукупність, прийоми їх використання у розслідуванні злочинів [10, с. 57].

Виходячи зі спрямованості цієї статті на отримання та надання у розпорядження юристів практичних рекомендацій щодо застосування криміналістичної техніки під час досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, видається за необхідне розглядати криміналістичну техніку у такому разі як технічні засоби та порядок їх використання під час збирання доказів у кримінальних провадженнях за фактами вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Використання зазначених технічних засобів аналізу комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку не варто обмежувати лише розкриттям та розслідуванням злочинів. Зазначені засоби можуть стати у нагоді у цивільному та господарському процесі (йдеться передусім про призначення та проведення судових експертиз), а також під час службових розслідувань та перевірок, які проводяться у компаніях, діяльність яких пов'язана із використанням комп'ютерних технологій.

Під час розслідування злочинів, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та

комп'ютерних мереж і мереж електрозв'язку, криміналістична техніка використовується для вирішення таких завдань, як:

1. Відеофіксація результатів проведення слідчих дій у рамках відповідних кримінальних проваджень (оглядів, допитів, обшуків, виїмки, слідчих експериментів тощо). Вказані технічні засоби обов'язково повинні мати функцію запису на окремий носій інформації, який після проведення слідчої дії може бути від'єднаний та упакований у присутності понятих у спеціальний сейф-пакет (адже копія відеозапису не може бути процесуальним джерелом доказів, виходячи зі змісту ч. 2 ст. 84 КПК України, згідно з якою процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів) [13].

2. Експертне дослідження комп'ютерної техніки, засобів зв'язку.

3. Проведення пошукових заходів на предмет виявлення можливих витоків інформації з обстежуваного приміщення чи конкретної операційної системи (застосування фахівцями спеціального оснащення та перевірки ймовірних місць зняття інформаційних даних: електроустановча арматура, дверні та віконні отвори, пожежна і вентиляційна системи, сигналізація, телекомунікаційне устаткування, а також усе комп'ютерне обладнання тощо) [14].

4. Виявлення слідів, розташованих на зовнішніх поверхнях комп'ютерної техніки, окремих її складових частинах (усередині системних блоків та іншого устаткування), робочих місцях співробітників, на яких зловмисниками могли бути залишені сліди відшарування, можливо, нашарування чи інші (невидимі безбарвні, одорологічні, трасологічні тощо) [14].

5. Огляд комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. При цьому, як справедливо зазначає А.С. Білоусов, «відмінною особливістю огляду таких комп'ютерних об'єктів, як системні блоки електронно-обчислювальних машин, комп'ютерні програми, інформація, що міститься на магнітних носіях тощо, є те, що їх не можна оглянути і сприйняти безпосередньо всіма учасниками огляду, як це передбачено завданнями проведення слідчого огляду. Для сприйняття властивостей окремих комп'ютерних об'єктів потрібно здійснити доступ до них шляхом використання спеціальних технічних пристроїв з відповідним програмним забезпеченням. При цьому слідчий у присутності понятих не просто спостерігає за комп'ютерним об'єктом, а повинен сам або за допомогою спеціаліста ввести в автоматизовану систему певні команди, і лише після цього буде отримана інформація, яка й розкриє та зробить доступною для сприйняття властивість комп'ютерних об'єктів» [6].

Виходячи зі змісту складів злочинів, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, та методики їх розслідування слід виділити такі види криміналістичної техніки, що застосовується під час їх розслідування:

1. Пристрої для «клонування» носіїв інформації:

− AOMEI Backupper забезпечує створення резервних копій та відновлення системи, жорсткого диска, розділів, файлів і папок; підтримку повного, часткового, диференціального та автоматичного резервного копіювання; клонування дисків, розділів для поновлення HDD або перенесення даних; створення резервних копій диска допоможе автоматично видалити старі резервні копії; копіювання з використанням «скриптів» командного рядка; злиття резервної копії та пов'язаних з нею додаткових копій в одну; створення завантажувального середовища для WinPE або Linux у разі поломки системи; стиснення, коментування, поділ, шифрування і перевірку резервних копій зображень; підтримку динамічних дисків, дисків MBR, GPT та режиму завантаження EFI /UEFI;
− Macrium Reflect;
− Handy Backup;
− HDClone;
− Acronis True Image;
− EASEUS Disk Copy;
− Norton Ghost [8].

2. Програмні засоби для криміналістичних досліджень вмісту носіїв інформації та їх образів:

− EnCase (Guidance Software) надає списки файлів та каталогів, поновлює видалені файли, здійснює пошук за ключовими словами, «проглядає» графіку, складає часові діаграми файлових операцій та ідентифікує файли за базовими даними хеш-кодів;

− Forensic Toolkit (Access Data) дозволяє проглядати файли та каталоги файлової системи, відновлювати видалені файли та каталоги файлової системи, здійснювати пошук за ключовими словами та різноманітними характеристиками файлів, проглядати всі графічні файли та ідентифікувати відомі файли за базами даних хеш-кодів;

− ProDiscover (Technology Pathways). У цій програмі реалізовані основні функції складання списків файлів та каталогів, відновлення видалених файлів, пошуку за ключовими словами та ідентифікації файлів за базами даних хеш-кодів;

− SMART (ASR Data) – програма зняття та аналізу даних на платформі Linux. Під час пошуку доказів програма дає можливість фільтрувати файли та каталоги в образі диска, поновлювати

видалені файли, проводити пошук за ключовими словами, проглядати графічні файли та ідентифікувати файли за базами даних хеш-кодів;

− The Sleuth Kit/Autopsy аналізує файлові системи FAT, NTFS, Ext2/3, UFS, виводить списки файлів та каталогів, відновлює видалені файли, будує часові діаграми файлових операцій, здійснює пошук за ключовими словами та працює з базами даних хеш-кодів [1].

3. Ноутбуки з комплексом програмних та апаратних засобів, призначених для дослідження комп'ютерної інформації за межами експертних установ (у так званих «польових» умовах).

4. Хеш-набори для фільтрації вмісту файлової системи, що досліджується, з метою відшукання файлів, які створив користувач.

5. Пристрої для під'єднання носіїв інформації з апаратним блокуванням здійснення запису на них.

6. Програмні засоби для дослідження локальних мереж.

7. Апаратні та програмні засоби для дослідження мобільних телефонів, SIM-карт та банківських карт [1]:

− комплекс UFED TOUCH LOGICAL здійснює повне логічне вилучення відомостей з пристроїв BlackBerry, iOS, Android, Symbian, Windows Phone, Palm та телефонів китайського виробництва; клонування ідентифікатора SIM-карти, що дозволяє виконати блокування будь-якої мережевої активності телефону на час аналізу та обхід блокування SIM-карт і відсутніх SIM-карт; аналіз, створення звітів і їх індивідуальне налаштування за допомогою UFED Logical Analyzer; забезпечує можливість роботи в польових умовах, для отримання даних не потрібно ПК [9];

− комплекс CellXtract дає можливість отримувати інформацію про пропущені дзвінки, набрані або вхідні номери, телефонну книгу, SMS-повідомлення з SIM-карти, MMS-повідомлення, календар, записи, фото, відео, аудіо та інші файли [2];

− комплекс Mobile Field Kit дозволяє експерту провести комплексний аналіз даних, вилучених з мобільного пристрою, а саме: сортувати файли, відновлювати вилучену інформацію, використання функції Data Carving для мультимедіа файлів, створювати закладки, читати «бекап файли», здійснювати пошук протиправних зображень і аналіз «логів» чатів [5].

− програма MOBILedit! Forensic – аналіз телефонів через Bluetooth, ІК-порт або кабель, аналіз записної книжки, набраних номерів, пропущених дзвінків, вхідних дзвінків, SMS і мультимедійних повідомлень, фотографій, файлів, інформації про телефон, календаря, нотаток, щоденника, читання видалених повідомлень з SIM-карти, створення звітів на основі шаблонів, друк звітів, адаптованих для надання у судовому засіданні, наявність ручного режиму дослідження [3].

8. Інструменти для демонтажу обладнання:
− викрутки (плоскі та фігурні);
− кусачки;
− плоскогубці;
− пінцет тощо.

9. Інструменти для документування процесу:
− фото- та відеокамера;
− бирки для нумерації доказів.

10. Матеріали для упаковки та транспортування вилучених об'єктів:
− антистатичні пакети;
− кабельна стяжка;
− коробки для DVD-дисків;
− коробки різноманітних розмірів для інших вилучених об'єктів.

11. Інші засоби та матеріали [7].

Висновки з дослідження. Розгляд питань щодо застосування криміналістичної техніки під час досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, дає змогу зробити такі висновки.

Традиційний підхід до застосування криміналістичної техніки у розкритті та розслідуванні кримінальних правопорушень, який сформульовано та вдосконалено протягом багатьох років науковцями та співробітниками «практичних підрозділів» щодо «традиційних» злочинів під час розкриття та розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку потребує вдосконалення.

Оскільки кінцевою метою зазначеної вище діяльності є отримання доказів, а чинне кримінальне процесуальне законодавство містить вимогу щодо надання до суду саме оригіналів доказів [13] (що у низці випадків розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку взагалі не є можливим з технічних міркувань), кримінальне процесуальне законодавство у частині вимоги щодо оригінальності доказів вчинення вказаних кримінальних правопорушень потребує уточнення.

Питання, пов'язані з криміналістичним дослідженням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, потребують подальшого дослідження.

Література

1. Carrier B. File System Forensic Analysis. New Jersey : Addison-Wesley, 2005. 600 p.
2. CellXtract. The Cellxtract Has Been Discontinued. URL: https://docplayer.net/55104024-Cellxtract-user-s-manual-version-date-12-19-2011.html (дата звернення 3.03.2021).
3. Complete data extraction from phones and SIM. URL: https://www.mobiledit.com/mobiledit-forensic (дата звернення: 3.03.3021).
4. Middleton B. Cyber Crime Investigator's Field Guide. Second Edition. Boca Raton : Auerbach Publications, 2004. 296 p.
5. WWT's Threat Detection Platform. URL: https://www.wwt.com/mobile-field-kit-threat-detection-platform (дата звернення: 3.03.3021).
6. Білоусов А.С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук : 12.00.09. Запоріжжя, 2008. 245 с.
7. Використання електронних (цифрових) доказів у кримінальних провадженнях : методичні рекомендації / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.
8. Вісім кращих програм для клонування жорсткого диска. URL: https://naukovistudii.org.ua (дата звернення: 2.03.2021).
9. Ефективний комплекс для високопродуктивних пристроїв. URL: https://bakotech.ua/uploads/product/278/files/554/file.pdf (дата звернення: 3.03.2021).
10. Кофанов А.В., Кобилянський О.Л., Кузьмічов Я.В. та ін. Криміналістика: питання і відповіді : навчальний посібник. Київ : Центр учбової літератури, 2011. 280 с.
11. Криміналістика : підручник для студентів юридичних спеціальностей вищих закладів освіти / За ред. В.Ю. Шепітька. 2-ге вид., переробл. і допов. Київ : Концерн «Видавничий Дім «Ін Юре», 2004. 728 с.
12. Криміналістична техніка. Юридична енциклопедія у 6 т. / ред. кол. Ю.С. Шемшученко (відп. ред.) та ін. Київ : Українська енциклопедія ім. М.П. Бажана, 2001. Т. 3 : К–М. 792 с.
13. Кримінальний процесуальний кодекс України від 19.11.2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n2186 (дата звернення: 1.03.2021).
14. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 221 с.

References

1. Carrier B. File System Forensic Analysis. New Jersey: Addison-Wesley, 2005. 600 p.
2. CellXtract. The Cellxtract Has Been Discontinued. Retrieved from: https://docplayer.net/55104024-Cellxtract-user-s-manual-version-date-12-19-2011.html.
3. Complete data extraction from phones and SIM. Retrieved from: https://www.mobiledit.com/mobiledit-forensic.
4. Middleton B. Cyber Crime Investigator's Field Guide. Second Edition. Boca Raton: Auerbach Publications, 2004. 296 p.
5. WWT's Threat Detection Platform. Retrieved from: https://www.wwt.com/mobile-field-kit-threat-detection-platform.
6. Bilousov, A.S. (2008) Kryminalistychnyj analiz ob'jektiv komp'juternykh zlochyniv [Forensic analysis of objects of computer crimes] (PhD Thesis), Zaporizhzhja: Classical Private University [in Ukrainian].
7. Kornejko, O.V. (ed.), Ghucaljuk, M.V., Ghavlovsjkyj, V.D., Khakhanovsjkyj, V.Gh. et al. (2010). Vykorystannja elektronnykh (cyfrovykh) dokaziv u kryminaljnykh provadzhennjakh: metod. rekom [The use of electronic (digital) evidence in criminal proceedings: guidelines]. Kyiv: Vyd-vo Nac. akad. vnutr. sprav. [in Ukrainian].
8. Visim krashhykh proghram dlja klonuvannja zhorstkogho dyska [Eight best programs for cloning a hard drive]. Retrieved from: https://naukovistudii.org.ua [in Ukrainian].
9. Efektyvnyj kompleks dlja vysokoproduktyvnykh prystrojiv [An efficient complex for high-performance devices]. Retrieved from: https://bakotech.ua/uploads/product/278/files/554/file.pdf [in Ukrainian].
10. Kofanov, A.V., Kobyljansjkyj, O.L., Kuzjmichov, Ja.V. et al. (2011). Kryminalistyka: pytannja i vidpovidi. Navchalniy posibnyk [Forensics: questions and answers. Tutorial], Kyiv: Centr uchbovoji literatury [in Ukrainian].
11. Shepitjko, V.Ju. (ed.) (2004). Kryminalistyka: pidruchnyk dlja studentiv juryduchnyih specialnosteiy vyshhchyh zakladiv osvity [Forensics: A textbook for law students in higher education], Kyiv: Koncern "Vydavnychyj Dim "In Jure" [in Ukrainian].

12. Shemshuchenko, Ju.S. (ed.) (2001). Kryminalistychna tekhnika [Forensic technique]. *Jurydychna encyklopedija* [Legal encyclopedia]. Kyiv: Ukrajinsjka encyklopedija im. M.P. Bazhana [in Ukrainian].
13. Kryminaljnyj procesualjnyj kodeks Ukrajiny vid 19.11.2012 [Criminal Procedure Code of Ukraine of 19.11.2012]. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n2186 [in Ukrainian].
14. Motljakh, O.I. (2005). Pytannja metodyky rozsliduvannja zlochyniv u sferi informacijnykh komp'juternykh tekhnologhij [Questions of methods of investigation of crimes in the field of information computer technologies] (PhD Thesis), Kyiv: Academy of Labor and Social Relations of the Federation Trade Unions of Ukraine [in Ukrainian].