DOI: 10.21564/2225-6555.2023.23.281734

Проблемні питання визначення цифрової криміналістики

Ігор Вікторович Лущик
Національний науковий центр
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»
Харків, Україна

Анатолій Серафимович Тяпкін*
Національний науковий центр
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»
Харків, Україна
**e-mail: tyapkin@ukr.net*

Анотація
У статті розглянуто проблему диференціації понять «цифрова криміналістика», «цифрова кримінологія», «цифрова судова експертиза», які широко використовуються сьогодні в науковій літературі й масмедіа, та розкрито їх зміст. Встановлено, що науково-технічний прогрес у сфері протидії злочинності та загальна цифровізація всіх сфер суспільства тісно пов'язані з розвитком нової галузі криміналістичних знань – цифрової криміналістики та використанням цифрових доказів у процесі доказування. Важливу роль у цьому процесі відіграє інтеграція знань, запровадження новітніх інноваційних розробок, спрямованих на вирішення завдань боротьби зі злочинністю. Цифрова криміналістика в Україні досить стрімко розвивається, що зумовлюється в тому числі новими викликами, спричиненими повномасштабним вторгненням рф та необхідністю розробки нових дистанційних електронних засобів пошуку, збору, фіксації та аналізу слідів кримінальних правопорушень. Наголошено, що розвиток цифрової криміналістики відбувається за трьома основними напрямами: 1) формування окремого наукового напрямку в криміналістиці; 2) застосування спеціальних знань при роботі з цифровими доказами; 3) проведення судових експертиз (зокрема комп'ютерно-технічної). З метою класифікації основних напрямів роботи з дотримання законності та протидії злочинам використано загальнонаукові т спеціальні методи дослідження, а саме: аналізу, синтезу, абстрагування, узагальнення, а також системний, функціональний та порівняльний методи. У результаті проведеного дослідження визначено дві великі спільноти, що переважно використовують цифрову криміналістику: правоохоронні органи, які у провадженнях у кримінальних і цивільних справах використовують цифрові докази для винесення обвинувального або виправдувального вироку підозрюваним, та

групи реагування на інциденти на підприємствах, в організаціях і установах, які першими реагують на кібератаки, такі як витік даних або загрози програм-здирників, використовуючи при цьому цифрову криміналістику для дослідження точок проникнення та можливих виправлень. Зроблено висновок, що перспективним напрямком розвитку є інтеграція штучного інтелекту в судову експертизу і криміналістику та використання технологій машинного навчання, що має високий потенціал для автоматизації й прискорення багатьох аспектів розслідування та експертизи, від аналізу та інтерпретації цифрових доказів до ідентифікації підозрюваних.

Ключові слова: *цифрова криміналістика; цифрова кримінологія; цифрова судова експертиза; цифрові сліди; кіберпростір.*

Problematic Issues of Definition of Digital Forensics

Ihor V. Lushchyk
National Scientific Center
"Hon. Prof. M.S. Bokarius Forensic Science Institute"
Kharkiv, Ukraine

Anatolii S. Tiapkin*
National Scientific Center
"Hon. Prof. M.S. Bokarius Forensic Science Institute"
Kharkiv, Ukraine
**e-mail: tyapkin@ukr.net*

Abstract
The article examines the problem of differentiation of the concepts "digital forensics", "digital criminology", "digital forensics", which are widely used today in scientific literature and mass media, and their meaning is revealed. It has been established that scientific and technical progress in the field of combating crime and the general digitization of all spheres of society are closely related to the development of a new field of forensic knowledge – digital forensics and the use of digital evidence in the process of proving. An important role in this process is played by the integration of knowledge, the introduction of the latest innovative developments aimed at solving the problems of combating crime. Digital forensics in Ukraine is developing quite rapidly, which is due, among other things, to new challenges caused by the full-scale invasion of the Russian Federation and the need to develop new remote electronic means of searching, collecting, recording and analyzing traces of criminal offenses. It is emphasized that the development of digital criminology takes place in three main directions: 1) the formation of a separate scientific direction in criminology; 2) application of special knowledge when working with digital evidence; 3) conducting forensic examinations (in particular, computer and technical examinations). In order

to classify the main areas of work on law enforcement and crime prevention, general scientific and special research methods were used, namely: analysis, synthesis, abstraction, generalization, as well as systemic, functional and comparative methods. As a result of the research, two large communities have been identified that mainly use digital forensics: law enforcement agencies, which in criminal and civil proceedings use digital evidence to convict or acquit suspects, and incident response teams in enterprises, organizations and institutions, who are the first to respond to cyber-attacks such as data breaches or ransomware threats, while using digital forensics to investigate penetration points and possible remediations. It was concluded that the integration of artificial intelligence in forensics and criminology and the use of machine learning technologies, which has a high potential for automating and accelerating many aspects of investigation and expertise, from the analysis and interpretation of digital evidence to the identification of suspects, is a promising direction of development.

Keywords: *digital criminalistics; digital criminology; forensic digital examination; digital traces; cyberspace.*

Вступ

Судова експертиза передбачає застосування наукових принципів і методів під час розслідування та судового розгляду кримінальних і цивільних справ, вона є важливим компонентом системи правосуддя, що надає об'єктивні наукові докази на підтримку або спростування доказів і претензій. З розвитком технологій і мінливою природою злочинів удосконалюються й сучасні підходи до судової експертизи, що мають відповідати новим викликам.

Без використання сучасних комп'ютерних технологій було б неможливим проведення аналізу ДНК, спричинив викликав революцію у галузі судової експертизи та криміналістики й дозволив слідчим ідентифікувати з високою точністю підозрюваних на основі біологічного матеріалу, знайденого на місці злочину навіть у незначній кількості. До того ж його можна використовувати для визначення зв'язку підозрюваних із місцем злочину. Іншим напрямом реалізації цифрових підходів у розслідуванні є мікроспектроскопія, що дає змогу ідентифікувати з високою точністю слідові докази (зокрема, дослідження залишків вогнепальної зброї або слідів її застосування, що може допомогти визначити її тип, використаний під час скоєння злочину). Ба більше, сучасні розробки у галузі судової антропології (дослідження людських останків у судових справах), засновані на використанні 3D-друку для створення копій людських кісток, дозволяють ідентифікувати останки. Також досягнуто певного прогресу у використанні аналізу стабільних ізотопів, що може надати інформацію про дієту та спосіб життя людини.

Останнім часом дедалі частіше в науковій літературі та масмедіа використовують поняття «цифрова криміналістика», «цифрова кримінологія», «цифрова судова експертиза», при цьому не виокремлюючи їх, а іноді навіть підміняючи одне іншим. Оскільки вони мають схожу спрямованість і тісно пов'язані між собою, виникає проблема диференціації цих понять і розкриття їхнього змісту.

Цифрові технології впроваджуються у різні сфери життя сучасного суспільства – економічну, соціальну, політичну та ін., викликаючи в них певні зміни, які спочатку можуть бути досягнення корисних цілей. Не залишається осторонь і організована злочинність, виходячи за межі традиційних сфер і способів порушень закону. Тому задля охорони правопорядку та убезпечення інтересів громадян відповідні державні органи мають реагувати на такі виклики часу.

Аналіз сучасних досліджень у галузі криміналістики свідчить, що в останні роки термін «цифрова криміналістика» зустрічається дедалі частіше, захоплюючи нові сфери. Однак сенс, який укладають різні автори в це поняття, і, відповідно, завдання та засоби, що витікають із цього, кожен автор розглядає по-своєму. Відтак в узагальненому вигляді до сфери цифрової криміналістики можна віднести:
– кібербезпеку;
– розслідування за допомогою цифрової техніки;
– розслідування злочинів у цифровому просторі;
– розслідування взагалі у сучасному цифровому суспільстві.

Перша складова спрямована переважно на запобіганні (профілактиці) злочинів, друга – пов'язує сферу злочинів і розслідувань із сучасними комп'ютерними й мобільними пристроями та програмним забезпеченням (засоби), третя – обмежує коло проблем кіберпростором (середовище), а четверта – вбирає всі попередні, узагальнюючи їх до так би мовити цивілізаційного рівня, адже сьогодні важко уявити сучасну людину, яка не користується інтернетом, мобільним телефоном, соціальними мережами, месенджерами тощо.

Незважаючи на майже півстолітню історію, лише тепер В. Шевчук [1] стверджує про появу нового напряму у вітчизняній криміналістиці – цифрової криміналістики (англ. – Digital Criminalistics), розроблення і впровадження якої він вбачає достатньо перспективним у розвитку криміналістичних знань і судово-експертної діяльності [2]. Ми згодні з ним у тому, що дотепер українська система правосуддя не унормувала ані основні поняття, що належать до цієї специфічної галузі, ані напрацювала необхідний концептуально-методичний апарат, що призводить до очевидної плутанини та підміни понять.

Відтак, метою статті є аналіз поглядів науковців на уявлень про цифрову криміналістику та її предмет, класифікація основних напрямів роботи з дотримання законності та протидії злочинам у цій сфері.

Огляд літератури

Предметом криміналістики В. Шепітько вважає «закономірності злочинної діяльності та її відображення в джерелах інформації» [3, с. 6]. Тобто в самому предметі криміналістики визначено, що вона стикається з інформацією, яка міститься у слідах. Отже, поза всякими сумнівами справедливим є твердження, що криміналістика, хоча й належить до юридичних наук, має тісний зв'язок із природничими й технічними науками, адже її так би мовити інформаційність полягає у дослідженні слідів злочину. Якщо змінюються носії цієї інформації (наприклад, раніше інформація була візуальною й містилася у відбитках ніг на місці злочину, потім – у відбитках пальців і слідах крові на знарядді злочину, то пізніше вона стала більш прихованою, вийшла за межі очевидного, перейшовши до кіберпростору), то криміналістика має пристосуватися до занурювання в цю нову реальність, знаходячи методи і засоби для розслідування злочинів у ній.

Саме за наслідками можна розпізнати й визначити діяльність, адже діяльність, яка не позначається у будь-якій матеріальній або навіть ідеальній сфері, є практично такою, яку неможливо визначити, ідентифікувати й пізнати.

На всіх етапах криміналістичного розслідування – збирання (у вигляді виявлення, фіксації та вилучення), дослідження, оцінювання та використання доказів – закладено можливості для використання традиційних і надсучасних засобів.

Так, К. Латиш у статті «Криміналістичний аналіз кіберінструментів вчинення злочинів» досліджує використання інформаційно-комунікаційних технологій, що використовуються як кіберінструменти для вчинення злочинів. Аналізується емпірична база кіберзлочинів з урахуванням останніх тенденцій, зумовлених пандемією, що триває [4]. Водночас Б. М. Головкін у роботі «Теперішнє і майбутнє кримінології» стверджує, що новітні види об'єктивно небезпечної поведінки найчастіше виникають у кіберпросторі, у сфері обігу електронних грошей, використання штучного інтелекту, надання послуг, використання природних і трудових ресурсів. Злочинність, вмонтована у суспільне життя, є продуктом людської діяльності. Поза системою суспільних відносин вона не існує [5].

А. В. Столітній та І. Г. Каланча у роботі «Формування інституту електронних доказів у кримінальному процесі України» досліджують феномен

«електронних доказів» у кримінальному процесі України. Вони вказали на відсутність єдності в наукових підходах як щодо визначення досліджуваного явища, так і місця електронних доказів у системі процесуальних джерел доказів. Сформульовано висновок, що термін «електронні докази» повинен мати виключно теоретичне оформлення, а сучасний, штучно створений інститут електронних доказів, – не має підміняти електронну форму фіксації доказів. Визначено можливість створення в результаті розвитку інформаційних технологій такого формату електронної інформації, що потребуватиме розширення джерел доказів електронними. Зазначене вимагатиме внесення ґрунтовних змін до кримінального процесуального закону й чіткого розмежування електронного джерела доказів та фіксації доказів у електронному форматі [6].

М. Є. Шумило, Р. Юрка та В. А. Капліна досліджують інформаційну теорія доказів і проблеми використання електронних засобів доказування в кримінальному провадженні. Вони розглянули актуальні для сучасної науки кримінального процесуального права та правозастосовної практики питання використання в кримінальному провадженні цифрових доказів. Науковці наголошують, що розвиток цифрових технологій, електронних форм комунікації, мережі інтернет, транснаціональний та транскордонний характер злочинів, що вчиняються у сфері комп'ютерної інформації, а також специфічний характер утворення цифрових слідів надають можливість констатувати значне розширення можливостей використання у доказуванні цифрових доказів, а також обумовлюють необхідність звернення до вирішення проблем доказування, що виникають в умовах цифровізації, в тому числі спираючись на надбання інформаційної теорії доказування, яка дозволить адаптувати доказову діяльність у кримінальному провадженні до будь-яких майбутніх інноваційних досягнень, науково-технічного прогресу та визначити місце цифрових доказів серед процесуальних джерел доказів. У ході дослідження виявлено чинники, що негативно позначаються на правозастосовній практиці, призводять до визнання отриманих у кримінальному провадженні доказів недопустимими. Пізнавальний потенціал в аспекті розвитку кримінальної процесуальної науки має інформаційна теорія кримінальних процесуальних доказів. Спираючись на те, що цифрові технології засновані на методах кодування та передачі інформації за допомогою подвійного коду шифрування, який дозволяє не лише передавати інформацію, але й розпізнавати її після цього, автори доходять висновку про доцільність використання більш широкого поняття «цифрова інформація» та «цифровий доказ» на відміну від поняття «електронна інформація» або «комп'ютерна інформація» [7].

Ю. Разметаєва та С. Разметаєв у статті «Правосуддя в епоху цифрових технологій: технологічні рішення, приховані загрози та привабливі

можливості» розглядають основні переваги та ризики впровадження та розгортання технологічних інструментів правосуддя, а також їх потенційний вплив на справедливість, заміну та додаткове використання технологічних рішень з урахуванням їх застосування в судовій системі в цифрову епоху. Автори аналізують явні та неявні ризики, що виникають при впровадженні та розгортанні технологічних інструментів. Використовуючи аксіологічний підхід, що передбачає апріорну цінність прав людини, справедливості та верховенства закону, оцінюються основні небезпеки, які спричиняє використання технологічних рішень у системі правосуддя. За допомогою формально-правового та порівняльно-правового методів, а також аналізу наукової літератури й контекстуального аналізу відкритих джерел про можливості штучного інтелекту та необ'єктивності алгоритмів у статті заповнюються прогалини щодо потенціалу технологій удосконалення доступу до правосуддя та використання алгоритмів при прийнятті рішень. Зазначається, що деякі технологічні рішення, і навіть звична поведінка всіх акторів цифрової епохи змінюють характер взаємодій, зокрема в системі правосуддя. Питання можливості алгоритмічної справедливості розглядається з позицій справедливості і недискримінації. У роботі показано, як використання алгоритмів може покращити процедурну справедливість, але й підкреслюється ретельний і збалансований підхід до інших елементів справедливості [14].

Багато цікавих думок щодо визначення різних аспектів цифрової криміналістики міститься у працях Н. М. Ахтирської, А. С. Білоусова, О. І. Котляревського, Д. М. Киценка, І. О. Крицької, В. В. Мурадова, Ю. Ю. Орлова, С. С. Чернявського та ін. [8–13].

Матеріали та методи

При дослідженні проблематики роботи було використано такі загальнонаукові теоретичні методи: аналізу (що дав змогу розділити поняття «цифрова криміналістика», «цифрова кримінологія» тощо та дослідити їх окремо), синтезу (на етапі об'єднання різних криміналістичних понять у єдине ціле), абстрагування (під час переходу від конкретних понять, пов'язаних з окремими видами криміналістичних експертиз, до абстрактних криміналістичних категорій), узагальнення (яке зробило можливим перехід від аналізування окремих напрямів цифрової криміналістики до розуміння цілісного поняття) та пояснення окремих понять, що належать до сфери цифрової криміналістики, а також системний і функціональний.

Окрім того, у роботі використано порівняльний метод для визначення схожості й відмінності між окремими поняттями, що належать до теми дослідження, та виокремлення в них загального й відмінного, а також

системний підхід щодо дослідження поняття «цифрова криміналістика» як цілісної множини елементів в сукупності відношень і зв'язків між ними.

Результати та обговорення

Перші відомості про злочини в цифровій сфері та необхідність їх розслідування з'явилися наприкінці 1970-х – на початку 1980-х років у зв'язку з появою персональних комп'ютерів. Саме в той час виникла комп'ютерна криміналістика, основна увага якої була сфокусована на кібератаках та витоку даних. Пізніше кількість комп'ютерних злочинів поступово зростала, до цієї сфери увійшли питання щодо регулювання питань авторського права, конфіденційності інформації та кіберпереслідування [15].

Водночас із появою інтернету та його поширенням як всесвітньої платформи для обміну знаннями, ресурсами та послугами виникли нові види злочинів (зокрема, кібербулінг, розповсюдження заборонених відеоматеріалів, розсилка спаму та ін.). У 1990-ті роки основними завданнями правоохоронців із цифрової криміналістики було вилучення, збереження та аналізування доказів, що зберігаються на комп'ютері [16].

Саме тоді вперше в науковій літературі P. Sommer і M. Goodman у статті "Computers and Law: the Use of Computers in British Criminal Investigations" використали термін «комп'ютерна криміналістика» (англ. Computer Forensics) [17], що став передвісником і синонімом цифрової криміналістики.

Наступним проривом стало розповсюдження мобільних пристроїв і їхня глобалізація, пов'язана з використанням месенджерів, ютубу, штучного інтелекту та ін., що дало змогу злочинцям і їхнім організованим угрупуванням вийти за межі національних кордонів.

Уперше комп'ютерні злочини як такі було визначено Законом про комп'ютерні злочини, прийнятим у штаті Флорида (США) 1978 р. (він передбачав протидію несанкціонованому внесенню змін або видаленню даних у комп'ютерній системі) [18]. Розслідуванням комп'ютерних злочинів спочатку займалися поліцейські – аматори комп'ютерів, які попервах використовували розроблені ними самими інструменти та методи, спеціально підготовлених експертів у цій галузі на той момент ще не існувало. Відтак виникла проблема підготовки кадрів і стандартизації протоколів, методів і засобів.

Цифрова криміналістика

На думку M. Rouse [19], цифрова криміналістика – це процес виявлення, збереження, аналізування та документування цифрових дока-

зів з метою представлення їх у суді. Схоже визначення наводить R. Mohanakrishnan [20] – галузь криміналістичної науки, що займається відновленням, дослідженням і збереженням цифрових доказів із дотриманням усіх правових стандартів. Вона вважає, що можна використовувати терміни «цифрова криміналістика» (англ. – Digital Forensics), «комп'ютерна криміналістика» (англ. Computer Forensics) та «кіберкриміналістика» (англ. Cyber Forensics) як синоніми.

Українські фахівці А. С. Колодіна та Т. С. Федорова визначають цифрову криміналістику як прикладну науку «про розкриття злочинів, пов'язаних із комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів» [21]. Водночас С. Прокопенко визначає цифрову криміналістику як прикладну науку «про відновлення та дослідження даних на цифрових пристроях, які можуть бути доказами у злочинах (інцидентах), пов'язаних із інформацією в електронному вигляді» [22].

Робота фахівця при розслідуванні цифрових злочинів передбачає пошук доказів після доступу до вилученого в процесі оперативно-розшукових дій обладнання, застосовуючи для цього спеціалізовані інструменти.

Наприклад, у США визначено п'ять галузей цифрової криміналістики [23], класифікованих за ознаками, в який спосіб дані передають та де вони зберігаються:
– комп'ютерна криміналістика (англ. Computer Forensics) фокусується на відновленні та збереженні доказів у комп'ютерах і пристроях зберігання (жорсткі диски та флеш-накопичувачі);
– криміналістика мобільних пристроїв (англ. Mobile Device Forensics) зосереджена на відновленні та збереженні цифрових доказів у мобільних і переносних пристроях (смартфони, флеш-накопичувачі та фітнес-трекери);
– мережева криміналістика (англ. Network Forensics) досліджує журнали мережевого трафіку для встановлення зв'язку між доступом до мережі та кримінальною дією;
– криміналістика баз даних (англ. Database Forensics) ідентифікує, збирає, зберігає, реконструює, аналізує звітність про інциденти, які потенційно можуть негативно вплинути на цілісність даних (вилучати дані та метадані можна з баз даних навіть таких, які зберігаються сторонніми службами в договорі з підозрюваним);
– криміналістичний аналіз даних (англ. Forensics Data Analysis) виявляє закономірностей у даних, які можуть свідчити про шахрайську діяльність (у першу чергу, економічну).

У кожній із цих галузей (типів) цифрової криміналістики сьогодні активно проводяться дослідження з актуальних питань. Як відомо,

кібератаки на комп'ютери залишають на них певні артефакти, які після збирання, обробки та аналізування можуть допомогти виявити особу та поведінку кіберзлочинців. Так, A. R. Javed із співавторами зосередили увагу на визначенні сучасних концепцій цифрової криміналістики, висвітленні прогалин та плануванні напрямів майбутніх досліджень, зокрема, надали опис різних галузей комп'ютерної криміналістики та наборів інструментів для фахівців [24].

O. Angelopoulou, A. Jones, G. Horsman і S. Pourmoafi визначали наявність персональної інформації, що залишилася на мобільних телефонах і планшетах, придбаних на ринку вживаних товарів у Великій Британії. Дослідження засвідчило, що конфіденційні та особисті дані залишалися на мобільному пристрої, здебільшого навіть не було спроб видалити їх [25].

У своїй статті A. Kapur досліджує питання цифрової криміналістики в моделі хмарних обчислень, які забезпечують мережевий доступ до набору фізичних і віртуальних об'єктів для виконання спільних обчислень із будь-якої точки світу за допомогою мереж, серверів, сховищ, програм і служб, а також надає необхідні рекомендації для убезпечення такої діяльності [26].

Основою будь-якої комп'ютерної програми є бази даних, дедалі збільшується їх використання для зберігання важливої та конфіденційної інформації, що може призводити до злочинів у цій сфері. R. Chopade і V. K. Pachghare наголошують, що криміналістика баз даних – це підгалузь цифрової криміналістики, яка зосереджена на детальному аналізуванні баз даних (зокрема, їх вмісту, файлів журналів, метаданих та ін.) [27]. Вони дослідили реляційні бази даних і бази даних NoSQL, а також вивчали артефакти, які слід ураховувати під час криміналістичних досліджень баз даних.

Міжнародний майданчик покупців і торгівців високотехнологічних продуктів Spiceworks додатково зазначає такі типи цифрової криміналістики (деякі з них наразі є розгалуженням наведених вище) [28]:
– електронне відкриття (англ. E-discovery) аналізує, оброблює та зберігає цифрові дані в нормативному або правовому контексті;
– реагування на інцидент (англ. Incident Response) забезпечує безперервність ведення бізнесу та зменшення впливу негативних несанкціонованих подій (наприклад, витіку даних, промислове шпигунство) в окремих організаціях;
– дискова експертиза (англ. Disk Forensics) спеціалізується на пошуку та відновленні даних із енергонезалежних пристроїв;
– криміналістика пам'яті (англ. Memory Forensics) зосереджена на даних із оперативної пам'яті комп'ютерів і мобільних пристроїв;

– хмарна криміналістика (англ. Cloud Forensics) аналізує конфігурацію, безпеку та геолокацію хмарних ресурсів;
– криміналістика електронної пошти (англ. Email Forensics) досліджує отримання та сканування електронної пошти, відшукуючи метадані з електронних листів і визначаючи їх шкідливий вміст (наприклад, фішингові електронні листи);
– криміналістика шкідливих програм (англ. Malware Forensics) відстежує джерела зловмисного програмного забезпечення.

Подібного поділення цифрової криміналістики дотримують у Китаї, де 2013 р. було акредитовано такі напрями цифрової криміналістики [29]:
а) за напрямом 2401 «Вилучення, збереження та відновлення даних» (Data Extraction, Preservation and Recovery):
– комп'ютерні носії інформації (Computer Storage media);
– вбудовані системи (Embedded Systems);
– мобільні пристрої (зокрема, мобільні телефони) (Mobile Devices (including mobile phones));
– смарт- та магнітні картки (Smart Cards and Magnetic Cards);
– цифрові пристрої (Digital Devices);
– мережеві дані (зокрема, з інтернету) (Network Data (including Internet data));
– дані комп'ютерної системи в режимі реального часу (зокрема, запущене вилучення системних даних) (Computer System Live Data (specifically running system data extraction));
б) за напрямом 2402 «Автентифікація електронних даних» (Authentication of Electronic Data):
– електронні підписи (Electronic Signatures);
– електронна пошта (E-mail);
– миттєві повідомлення (Instant Messaging);
– електронні документи (Electronic Documents);
– база даних (Database);
в) за напрямом 2403 «Узгодженість і подібність електронних даних» (Consistency and Similarity of Electronic Data):
– програмне забезпечення (Software);
– цифрові документи (Digital Documents);
– інтегральні схеми (зокрема, мікросхеми) (Integrated Circuit (including chips)).

Знання у галузі цифрової криміналістики, крім співробітників правоохоронних органів, у кримінальних, адміністративних і цивільних провадженнях використовують спеціальні групи реагування на інциденти в бізнес-структурах, які першими стикаються з кібератаками, витоком даних, крадіжками об'єктів інтелектуальної власності або загрозами небезпечного програмового забезпечення.

A. Leppänen і T. Kankaanranta, проаналізувавши організацію розслідування кіберзлочинів у Фінляндії, доходять висновку, що вони не є однорідною категорією певного виду злочинів, оскільки в кожному злочині використовують різні цифрові технології, тому кіберзлочинність є нестійким рішенням [30]. З огляду на це, на їхню думку, більш плідним може виявитися підхід, що базується на технічній експертизі, у якій існує потреба під час кримінального розслідування. З іншого боку, важко забезпечити якісну підготовку слідчих у справах комп'ютерних злочинів, проте такі знання мають експерти у цій галузі.

Технічні чинники, що впливають на криміналістику даних, мають певні труднощі з шифруванням і використанням місця для зберігання інформації на пристрої та методи протидії незаконним спробам обійти інструменти криміналістики даних за допомогою процесуальних засобів або програмного забезпечення [31]. Розроблення нових інструментів і методів для аналізування цифрових доказів призвело до значного підвищення точності та надійності цифрової криміналістики.

Фахівці визначають дві великі спільноти, що переважно використовують цифрову криміналістику [54]:
– правоохоронні органи – у провадженнях по кримінальних та цивільних справах: ці установи використовують цифрові докази для винесення обвинувального або виправдувального вироку підозрюваним;
– групи реагування на інциденти на підприємствах, в організаціях і установах: ці групи першими реагують на кібератаки, такі як витік даних або загрози програм-здирників. Вони використовують цифрову криміналістику для дослідження точок проникнення та можливих виправлень.

До цього можна додати, що зовсім у недалекому майбутньому ми додамо до цього переліку штучний інтелект як соціальне та юридичне явище.

Цифрова криміналістика має реагувати на виклики часу досить швидко, адже постійно виникають нові загрози, пов'язані з кібератаками, новими видами злочинів у віртуальному просторі, що спровоковані доступністю хакерських інструментів і розповсюдженням даркнету (це прихована мережа, що дає змогу передавати дані в зашифрованому та вільному від контролю вигляді. Його можна використовувати як для забезпечення недоторканності приватного життя і захисту від політичних переслідувань, так і для скоєння злочинів у сфері інформаційних технологій, передавання інформації з порушенням авторських прав, тероризму та кібершпигунства). З іншого боку, хмарні технології передбачають зберігання даних у різних географічних точках, що призводить до проблем визначення юрисдикції під час розслідування злочинів у цій сфері.

Цифрова кримінологія

Відмінності у розумінні понять «цифрова криміналістика» та «цифрова кримінологія» знаходяться, на нашу думку, в тій же площині, що й відмінності в їхніх родових поняттях, тому має сенс звернутися до визначень. Криміналістика – це застосування наукових принципів для надання доказів у кримінальних справах, тому фахівці у цій галузі повинні вміти збирати докази на місці злочину, доводити причини нещасних випадків і перевіряти докази, здобуті на місці злочину або в спеціально обладнаних лабораторіях. Натомість кримінологія – це дослідження злочинності, засобів її попередження, а також особи злочинців та поводження з ними, тому фахівці цього напряму вивчають систему кримінального правосуддя та розробляють нові підходи до боротьби зі злочинністю та її причинами [32].

Однією з перших фундаментальних праць у галузі цифрової кримінології стала книга A. Powell, G. Stratton і R. Cameron «Digital criminology: crime and justice in digital society» (1982) [33]. У ній, зокрема, зазначено, що цифрова кримінологія досліджує концептуальні, правові, політичні та культурні межі злочинності, формальні заходи правосуддя і неформальні рухи окремих громадян щодо дотримання законності в суспільстві, що дедалі більше стає глобалізованим і цифровим.

Цифрова кримінологія використовує кримінологічні теорії та уявлення про поведінку людини, поєднуючи їх із філософією права та правовими принципами, а також із науками про кібербезпеку як інструменти розслідування цифрових злочинів [34].

Поширення цифрових технологій глобально позначається на суспільстві та окремій людині, на структурі злочинності та на діяльності правоохоронних органів. Тому кримінологію можна використовувати для аналізування наявних даних, виявлення їх зловмисного використання, а також для ідентифікації людей, які отримують вигоду від зібраних даних, щоб допомогти розкрити такі злочини. Ба більше, такі (за виразом A. Vasileiadis) [35] цифрові «медичні експерти» (англ. Digital «medical examiners») можуть працювати з правоохоронними органами та приватними компаніями, щоб допомогти їм зрозуміти, як реагувати на кібератаку та що робити, щоб усунути прогалину в безпеці. Наскільки б розумними кримінологи не вважали злочинців, останні завжди залишають інформацію, яку може знайти досвідчений кримінолог, починаючи від злому паролів і завершуючи відновленням видаленої або зашифрованої інформації. Етапи кримінологічного розслідування цифрових злочинів співпадають із тими, що використовують криміналісти, до яких належать: розпізнавання місця, де шукати; зберігання інформації

для подальших досліджень, документуючи, як саме були зібрані докази; збирання інформації; аналізування з метою перевірки наявних даних і визначення, що насправді сталося; звітування з представленням результатів дослідження в офіційній формі, яке не може бути оскаржене іншими учасниками для створення доказової бази в судовому розгляді.

На нашу думку, оскільки кримінологія вивчає особу злочинця з метою попередження або доказування злочину, а особистість людини мало змінилася за останні кількасот років (а може й кілька тисячоліть від початку нашої цивілізації), істотно змінилися технології, які вона може використовувати у виробничій і повсякденній діяльності, то говорити про виникнення цифрової кримінології наразі не доречно. Адже це не виникнення нової віртуальної людини, яка може скоювати злочини у кіберпросторі, це поява нових технологічних можливостей у звичайної людини для скоєння злочинів. Це може бути пов'язано зі зміною мотивації злочинця, виникнення у нього оманливого відчуття безкарності через вихід у віртуальний простір, де (на його думку) можна зберегти анонімність. Але будь-яка діяльність (навіть віртуальна) залишає по собі сліди, тому кримінологи мають здійснювати превентивні заходи щодо запобігання злочинності, зменшенні її негативного впливу, а завдання криміналістів і судових експертів полягає в тому, щоб знайти, ідентифікувати та представити ці сліди з метою створення доказової бази у судовому розгляді.

Саме з цього боку слід розглядати й назву книги творців поняття «цифрова кримінологія» як злочин і розслідування в суспільстві на етапі цифрових технологій. Хоча можна вважати (як це зробили в Університеті Сюррея, Велика Британія [36]) про виникнення нового напряму – кримінології кіберзлочинів і кібербезпеки.

Цифрова криміналістична експертиза

На думку А. С. Колодіної та Т. С. Федорової (2022) [37], (яку поділяють К. Є. Борисова та В. А. Світличний [38]), існує також цифрова криміналістична експертиза – це «одна із галузей криміналістичної експертизи, яка зосереджується на кримінально-процесуальному праві та доказах щодо комп'ютерів та пов'язаних із ними пристроїв», таких як мобільні телефони, смартфони, планшети, навігатори, ігрові консолі, фітнес-браслети та ін. Вона передбачає ідентифікацію, отримання, зберігання, аналізування та представлення цифрових доказів.

Криміналістичні експертизи поєднують значну кількість її різновидів: почеркознавчу, лінгвістичну експертизу мовлення; технічну експертизу документів; експертизу зброї та слідів і обставин її використання; трасологічну; фототехнічну, портретну; експертизу голограм; відео-, звукозапису; вибухотехнічну; техногенних вибухів; матеріалів, речовин

та виробів і біологічну [39]. До того ж згідно зі ст. 7 Закону України «Про судову експертизу» «виключно державними спеціалізованими установами здійснюється судово-експертна діяльність, пов'язана з проведенням криміналістичних, судово-медичних і судово-психіатричних експертиз» [40], що обмежує коло фахівців, які можуть брати участь у таких дослідженнях тільки співробітниками державних установ, залишаючи поза увагою судових експертів, які не працюють у таких установах. З іншого боку, знання в галузі цифрових технологій стають у пригоді фахівцям не тільки в криміналістичній експертизі відео- та звукозапису за їх прямим призначенням, а й в інших (наприклад, ст. 2 Інструкції про призначення та проведення судових експертиз та експертних досліджень визначає, що «об'єктом дослідження лінгвістичної експертизи мовлення є продукт мовленнєвої діяльності людини, відображений у писемній або в усній формі (зафіксований у відео-, фонограмі)») [39].

Тому вважаємо, що переліком, який містить ця Інструкція, можна обмежитися й не додавати новий вид або підвид криміналістичних експертиз. Водночас (докладніше ми розглянемо це далі) з-поміж судових експертиз існує достатня кількість інших, некриміналістичних, об'єктами дослідження в яких можуть стати цифрові носії інформації.

Цифрова судова експертиза

Деяка плутанина виникає, на нашу думку, через те, що англійські поняття «Criminalistics», «Forensic science», «Forensics» у значенні використання наукових методів під час розслідування відповідно до вимог кримінального та цивільного законодавства, в англомовному світі вживають як синоніми (див., наприклад, сторінки на освітньому порталі Study.com [41] та в енциклопедії Британніка [42]).

У чинному Законі України визначається, що «судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду» [40].

Згідно із законодавством України [43] як окремі види існують експертиза відео, звукозапису, в якій виокремлено спеціальність 7.1 «Технічне дослідження матеріалів та засобів відео-, звукозапису», комп'ютерно-технічна (спеціальність 10.9 «Дослідження комп'ютерної техніки та програмних продуктів») та телекомунікаційна експертизи (спеціальність 10.17 «Дослідження телекомунікаційних систем (обладнання) та засобів»).

До того ж існує окремий напрям – експертизи у сфері інтелектуальної власності, пов'язаний (між іншими) із дослідженнями, пов'язаними

з комп'ютерними програмами і компіляціями даних (базами даних) за спеціальністю 13.1.2; дослідження фонограм, відеограм, програм (передач) організацій мовлення (спеціальність 13.2); дослідження, пов'язані з топографіями інтегральних мікросхем (13.7); дослідження, пов'язані з комерційною таємницею (ноу-хау) і раціоналізаторськими пропозиціями (13.8) та ін.

Ще одним доказом щодо взаємного проникнення криміналістики та судової експертизи є змішування цих понять у галузі послуг. Наприклад, українська компанія «Експерти з цифрової криміналістики» надає послуги з проведення експертиз із цифрової криміналістики або комп'ютерно-технічні експертизи, зауважуючи, що судові справи вимагають переконливих фактів, які можуть міститися на цифрових приладах [44].

О. В. Александренко та В. І. Женунтій вважають, що використання сучасних цифрових та інноваційних технологій стосується насамперед галузі судово-експертної діяльності, де вони є додатковим інструментарієм, що дає можливість розширити можливості дослідження речових доказів із метою отримання доказової інформації в інтересах розслідування. Водночас перспективними такі технології можна вважати і для криміналістичної техніки, тактики і методики [45].

Інші похідні словотворення (форензіка, форензік тощо)

Слово форензіка з'явилося як запозичення відповідного англійського (forensics) спочатку в російській мові [46], де його використовували для означення прикладної науки про розкриття злочинів, пов'язаних із комп'ютерною інформацією, про дослідження доказів у вигляді комп'ютерної інформації, методах пошуку, отримання та закріплення таких доказів.

У програмі підготовки фахівців на юридичному факультеті Львівського національного університету імені Івана Франка існує курс цифрової (комп'ютерної) криміналістики (форензики) як судової науки практичного спрямування, що вивчає відновлення та дослідження даних, пов'язаних із кіберзлочинністю, у цифрових пристроях [47]. У програмі цього курсу зазначено, що «цифрова криміналістика традиційно охоплює не лише рекомендації, прийоми і засоби викриття та розслідування уже вчинених кіберзлочинів та інших цифрових зловживань, а й рекомендації щодо їх запобігання й випередження – тобто кібербезпеку».

Пізніше подібне трапилося зі словом форензік, яке (на відміну від попереднього російського) використовують у діловому світі для позначення комплексу заходів із виявлення шахрайських схем, організованих співробітниками або топ-менеджерами стосовно звітності, фінансових операцій, промислового шпигунства, хабарництва та ін. [48] В. О. Маль-

ський визначає форензік як «юридичний і фінансовий аудит, спрямований на виявлення незаконної або шахрайської діяльності посадових осіб або акціонерів компанії, що завдала або може завдати збитки компанії або акціонерам» [49]. На відміну від аудиту, на думку А. Ковбеля [49], форензік, на основі всебічного аналізу фінансових, юридичних і нематеріальних аспектів, спрямований на запобігання (виділено нами. – *Автори*) випадків шахрайства з метою мінімізації шкоди компанії. Нашу думку, це свідчить про психологічну природу такої діяльності, а використання методів психологічного та юридичного тиску на потенційних шахраїв і наближує його до кримінології.

Так само М. В. Дубініна, С. В. Сирцева та Т. Ю. Янковська вважають форензік ефективним видом контролю, метою якого є виявлення фактів шахрайства та фінансових зловживань, а також розслідування інших злочинних дій (пошук активів, виявлення ознак навмисного банкрутства, моніторинг підозрілих операцій, захист інтелектуальної власності, запровадження системи корпоративного комплаєнсу [50]). До речі, до сфери комплаєнсу як відповідності законам, правилам і стандартам [51] належать, поміж інших:
протидія легалізації доходів, отриманих злочинним шляхом, і фінансуванню тероризму;
захист інформаційних потоків, протидія шахрайству і корупції, встановлення етичних норм поведінки співробітників тощо.

Отже, українське форензік не тотожне криміналістиці або судовій експертизі (як спочатку може скластися враження), воно перебуває в точці дотику криміналістичної протидії зловживанням у сфері бізнесу, кримінології, кібербезпеки, корпоративної етики та судової економічної експертизи.

На останок хотілося б зауважити, що існують певні складнощі, пов'язані з долученням цифрових даних судом до справ, адже іноді це зробити дещо складно й суд не завжди готовий їх прийняти, також можуть різнитися думки фахівців та інших учасників судочинства з приводу вже долучених даних. Як і будь-яка інформація, яка може бути використана в суді, вона має бути надійною; способи, як відновити видалений файл або як прочитати шифрування, можуть мати значний вплив на те, чи зможе суд використати цю інформацію. Якими міжнародними нормами і стандартами слід керуватися співробітникам правоохоронних, експертних і судочинних органів у разі збирання, оцінювання та залучення до матеріалів справи цифрових даних?

Існує спеціальний міжнародний стандарт у цій галузі – ISO/IEC 27037:2012 [52], який надає рекомендації щодо ситуацій, які вини-

кають у процесі оброблення цифрових доказів, та полегшує обмін такими доказами між різними юрисдикціями. Його дія поширюється на цифрові носії даних комп'ютерів, мобільних телефонів і навігаційних систем, цифрових фото- та відеокамер і комп'ютерні мережі. З іншого боку, Центр із прав людини університету Берклі (США) та Офіс Верховного комісара ООН із прав людини розробили так званий Протокол Берклі, який містить усі вимоги до збирання, зберігання та використання інформації з відкритих джерел [53].

Проблему допущення цифрових доказів власне як доказів під час розгляду їх в українських судах окреслив екс-заступник Генерального прокурора Г. Мамедов, зазначивши, що вже існує світова практика (зокрема, у Міжнародному кримінальному суді) залучення цифрових доказів до справ на основі норм місцевого законодавства, Протоколу Берклі та принципів SWGDE (англ. The Scientific Working Group on Digital Evidence – група, яка об'єднує правоохоронні, академічні та комерційні організації, що співпрацюють у сфері цифрової криміналістики, із метою розроблення міждисциплінарних вказівок і стандартів для відновлення, збереження та експертизи цифрових даних). Автор зазначає, що дотепер процедура їх збирання, верифікації, зберігання та застосування не унормована у вітчизняних законодавчих актах [53].

Висновки

Предмет криміналістики, незважаючи на стрімкі зміни сучасних технологій, залишається незмінним, змінюються тільки форми збирання, дослідження, оцінювання та використання доказів відповідно до сучасних умов, що впливають на громадян і суспільство загалом. У своїй повсякденні діяльності фахівці можуть використовувати найсучасніші техніку й технологію, але вони стають складовою всіх сфер життєдіяльності людини – економічної, соціальної, політичної та ін. Тому цифрова криміналістика – це не окрема галузь криміналістики, на нашу думку, коректніше говорити про криміналістику злочинів у цифровому просторі. Цифрова криміналістика займається відновленням та дослідженням матеріалів, виявлених у цифрових пристроях, пов›язаних з кіберзлочинністю. Цифрова криміналістика – це процес виявлення, збереження, аналізу та документування цифрових доказів.

Визначено дві великі спільноти, що переважно використовують цифрову криміналістику:
– правоохоронні органи – у провадженнях у кримінальних і цивільних справах: ці установи використовують цифрові докази для винесення обвинувального або виправдувального вироку підозрюваним;
– групи реагування на інциденти на підприємствах, в організаціях і установах: ці групи першими реагують на кібератаки, такі як витік

даних або загрози програм-здирників. Вони використовують цифрову криміналістику для дослідження точок проникнення та можливих виправлень.

До цього можна додати, що в недалекому майбутньому цей перелік доповниться таким соціальним і юридичним явищем, як штучний інтелект.

Серед перспективних напрямів розвитку – інтеграція штучного інтелекту в судову експертизу і криміналістику та використання технологій машинного навчання, що має високий потенціал для автоматизації та прискорення багатьох аспектів розслідування й експертизи, від аналізу та інтерпретації цифрових доказів до ідентифікації підозрюваних.

На окрему увагу заслуговує використання в судовій експертизі міждисциплінарних підходів, що передбачає об'єднання судових, судово-медичних та експертів інших дисциплін і криміналістів для аналізування та тлумачення доказів.

Список використаних джерел

[1] Шевчук В. Сучасні проблеми криміналістики в умовах війни та глобальних загроз. *Теорія та практика судової експертизи і криміналістики*. 2022. Вип. 28. С. 11–27. https://doi.org/10.32353/khrife.03.2022.02.

[2] Shevchuk V. Modern problems of formation and prospects for researching the concept of criminalistic innovation. *Tendances scientifiques de la recherche fondamentale et appliquée: collection de papiers scientifiques «ΛΌГОΣ»*. 2020. Vol. 2. P. 67–72. https://doi.org/10.36074/30.10.2020.v2.20.

[3] Криміналістика : підручник : у 2 т. Т. 1 / В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін. ; за ред. В. Ю. Шепітька. Харків : Право, 2019. 456 с.

[4] Латиш К. В. Криміналістичний аналіз кіберінструментів вчинення злочинів. *Проблеми законності*. 2021. Вип. 153. С. 165–172. https://doi.org/10.21564/2414-990X.153.230429.

[5] Головкін Б. М.Теперішнє і майбутнє кримінології. *Проблеми законності*. 2020. Вип 149. С. 168–184. https://doi.org/10.21564/2414-990x.149.200724.

[6] Столітній А. В., Каланча І. Г. Формування інституту «електронних доказів» у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179–191. https://doi.org/10.21564/2414-990x.146.171218.

[7] Kaplina V. A., Raimundas J., Shumylo M. Ye. Informational theory of evidence and the problems of using the electronic means of proving in criminal procedure. *Journal of the National Academy of Legal Sciences of Ukraine*. 2019. Vol. 26, issue 2. P. 118–130.

[8] Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. 2016. Вип. 36 (2). С. 123–125.

[9] Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. … канд. юрид. наук / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2008. 18 с.

[10] Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації*. 1998. № 2. С. 70–79.

[11] Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301–305.

[12] Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3-2. С. 313–315.
[13] Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12–22
[14] Razmetaeva Yu., Razmetaev S. Justice in the era of digital technologies: technological solutions, hidden threats and tempting opportunities. *Access to Justice in Eastern Europe*. 2021. Vol. 2, issue 10. P. 104–117. https://doi.org/10.33327/AJEE-18-4.2-a000061.
[15] Digital forensics. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Digital_forensics (last accessed: 24.03.2023).
[16] Rosenblatt K. S. High-Technology Crime: Investigating Cases Involving Computers. San Jose : KSK Publications, 1995. 603 p.
[17] Meah J. Digital Forensics: The Ultimate Guide. *Techopedia*. 19 August, 2022. URL: https://www.techopedia.com/digital-forensics-the-ultimate-guide/2/34721 (last accessed: 24.03.2023).
[18] Kabay M. E. A Brief History of Computer Crime: An Introduction for Students. Norwich : School of Graduate Studies of Norwich University, 2008. P. 51. URL: http://www.mekabay.com/overviews/history.pdf (last accessed: 24.03.2023).
[19] Rouse M. Digital Forensics. *Techopedia*. 24 August, 2022. URL: https://www.techopedia.com/definition/27805/digital-forensics (last accessed: 24.03.2023).
[20] Mohanakrishnan R. What is Digital Forensics? Meaning, Importance, and Types. *Spiceworks*. July 18, 2022. URL: https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/ (last accessed: 24.03.2023).
[21] Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. № 1. С. 176–180. https://doi.org/10.32782/klj/2022.1.27.
[22] Прокопенко С. Практика та особливості проведення комп'ютерно-технічних експертиз. *Матеріали IV Всеукраїнської конференції з кримінального права та процесу*. Київ, 2017. URL: https://www.slideshare.net/cyberlab_ua/ss81935770 (дата звернення: 24.03.2023).
[23] Rouse M. Op. cit.
[24] Javed A. R., Ahmed W., Alazab M., Jalil, Z. A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*. 2022. Vol. 10. P. 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508.
[25] Angelopoulou O., Jones A., Horsman G., Pourmoafi S. A Study of the Data Remaining on Second-Hand Mobile Devices in Study of the Data Remaining on Second-Hand Mobile Devices in the UK. *Journal of Digital Forensics, Security and Law Security and Law*. 2022. Vol. 17. Art. 5. URL: https://commons.erau.edu/jdfsl/vol17/iss2/5 (last accessed: 24.03.2023).
[26] Kapur A. Digital Forensics in Cloud Computing. International Journal of Computer Applications. 2021, Vol. 183, issue 18. P. 10–13. https://doi.org/10.5120/ijca2021921524.
[27] Chopade R., Pachghare V. K. Ten years of critical review on database forensics research. *Digital Investigation*. 2019. Vol. 29. P. 180–197. https://doi.org/10.1016/j.diin.2019.04.001.
[28] Mohanakrishnan R. Op. cit. URL: https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/ (last accessed: 24.03.2023).
[29] Guo H., Hou J. Review of the accreditation of digital forensics in China. *Forensic Sciences Research*. 2018. Vol. 3, issue 3. P. 194–201. https://doi.org/10.1080/20961790.2018.1503526.

[30] Leppänen A., Kankaanranta T. Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime Prevention. 2017. Vol. 18, issue 2. P. 157–175. https://doi.org/10.1080/14043858.2017.1385231.
[31] What is Data Forensics? *Digital Guardian*. URL: https://www.digitalguardian.com/dskb/data-forensics (last accessed: 24.03.2023).
[32] Criminology Vs. Criminalistics: What's the Difference? *BestAccreditedColleges*. URL: https://bestaccreditedcolleges.org/articles/criminology-vs-criminalistics-whats-the-difference.html (last accessed: 24.03.2023).
[33] Powell A., Stratton G., Cameron R. Digital criminology: Crime and Justice in Digital Society. London : Taylor & Francis, 1982. 220 p. https://doi.org/10.4324/9781315205786.
[34] Digital Criminology. *Purdue University.* URL: https://www.admissions.purdue.edu/majors/a-to-z/digital-criminology.php (last accessed: 24.03.2023).
[35] Vasileiadis A. Digital criminology in solving cybercrime. *hakin9*. URL: https://hakin9.org/digital-criminology-in-solving-cybercrime-by-anastasis-vasileiadis/ (last accessed: 24.03.2023).
[36] Criminology (Cybercrime and Cybersecurity) MSc–2023 entry. *University of Surrey*. URL: https://www.surrey.ac.uk/postgraduate/criminology-cybercrime-and-cybersecurity-msc (last accessed: 24.03.2023).
[37] Колодіна А. С., Федорова Т. С. Зазнач. твір.
[38] Борисова К. Є., Світличний В. А. Застосування цифрової криміналістики. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану* : тези доп. міжнар. наук.-практ. конф. (м. Харків, 25 листоп. 2022 р.). Харків : ХНУВС, 2022. С. 83–84. URL: https://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/14869/Zastosuvannia% 20tsyfrovoi%20kryminalistyky_Borysova_Svitlychnyi_2022.pdf?sequence=1&isAllowed=y (дата звернення: 24.03.2023).
[39] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та доп.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 24.03.2023).
[40] Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змін. та доп.). URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 24.03.2023).
[41] Forensic Science: Types & Etymology. *Study.Com.* URL: https://study.com/learn/lesson/what-is-forensic-science-forensic-science-types-etymology.html (дата звернення: 24.03.2023).
[42] Forensic Science. *Britannica.Com*. URL: https://www.britannica.com/science/forensic-science (дата звернення: 24.03.2023).
[43] Про затвердження Положення про Центральну експертно-кваліфікаційну комісію при Міністерстві юстиції України та атестацію судових експертів : наказ Мін'юсту України від 03.03.2015 р. № 301/5 (зі змін. та доп.). URL: https://zakon.rada.gov.ua/laws/show/z0249-15#Text (дата звернення: 24.03.2023).
[44] Експерти з цифрової криміналістики. *Ukrforensic.Com.* URL: https://www.ukrforensic.com/ (дата звернення: 24.03.2023).
[45] Александренко О. В., Женунтій В. І. Інновації та цифрові технології в криміналістиці та судовій експертизі: сучасні можливості та проблеми застосування. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці* : матеріали міжнар. «круглого столу» (м. Харків, 12 груд. 2019 р.). Харків, 2019. С. 10–14.

[46] Федотов Н. Н. Форензика – компьютерная криминалистика. Москва, 2007. 432 с.
[47] Комп'ютерна криміналістика. Львів : Юридичний факультет факультеті Львів. нац. ун-ту ім. І. Франка. URL: https://law.lnu.edu.ua/course/digitalforensics (дата звернення: 24.03.2023).
[48] Андрианова Т. Форензик – must have украинского бизнеса. *Nota Group. На захісті українського бізнесу*. 20.07.2018. URL: https://notagroup.com.ua/ru/news/forenzik-must-have-ukrainskogo-biznesa/ (дата звернення: 24.03.2023).
[49] Стулина А. Прикладное искусство. *Юридическая практика.* 2019. № 41. URL: https://pravo.ua/articles/prikladnoe-iskusstvo/ (дата звернення: 24.03.2023).
[50] Дубініна М. В., Сирцева С. В., Янковська Т. Ю. Форензік як метод розслідування внутрішньокорпоративних випадків шахрайства. *Інфраструктура ринку*. 2019. Вип. 38. С. 377–383. https://doi.org/ 10.32843/infrastruct38-59.
[51] Чубенко А. Г., Лошицький М. В., Павлов Д. М., Бичкова С. С., Юнін О. С. Дотримання вимог законодавства та внутрішніх процедур (комплаєнс); Комплаєнс. *Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції.* Київ : Ваіте, 2018. 826 с.
[52] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (last accessed: 24.03.2023).
[52] Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Нью-Йорк : ООН, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (last accessed: 24.03.2023).
[53] Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? *New Voice.* 08.06.2022. URL: https://nv.ua/opinion/voyna-v-ukraine-kak-cifrovaya-kriminalistika-razoblachaet-prestupleniya-rf-v-ukraine-novosti-ukrainy-50248411.html (дата звернення: 24.03.2023).
[54] Mohanakrishnan R. What Is Digital Forensics? Meaning, Importance, and Types. *Spiceworks*. July 18, 2022. Retrieved from www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/ (last accessed: 24.03.2023).

References

[1] Shevchuk, V. (2022). Modern Problems of Forensics in Conditions of War and Global Threats. *Theory and Practice of Forensic Examination and Criminology*, 28, 11-27. https://doi.org/10.32353/khrife.03.2022.02.
[2] Shevchuk, V. (2020). Modern Problems of Formation and Prospects for Researching the Concept of Criminalistic Innovation. *Tendances Scientifiques de la Recherche Fondamentale et Appliquée: Collection de Papiers Scientifiques «ΛΟΓΟΣ»*, 2, 67-72. https://doi.org/10.36074/30.10.2020.v2.20.
[3] Shepitko, V.Yu., Zhuravel, V.A., Konovalova, V.O. & al. (2019). *Criminalistics*. (Vols. 1-2). Vol. 1. V.Yu. Shepitko (Ed.). Kharkiv: Pravo.
[4] Latysh, K.V. (2021). Forensic Analysis of Cyber Tools for Committing Crimes. *Problems of Legality*, 153, 165-172. https://doi.org/ 10.21564/2414-990X.153.230429.
[5] Golovkin, B.M. (2020). The present and future of criminology. *Problems of Legality*, 149, 168-184. https://doi.org/10.21564/2414-990x.149.200724.
[6] Stolitniy, A.V., & Kalancha, I.G. (2019). Formation of the Institute of «Electronic Evidence» in the Criminal Process of Ukraine. *Problems of Legality*, 146, 179-191. https://doi.org/10.21564/2414-990x.146.171218.
[7] Kaplina, V.A., Raimundas, J., & Shumylo, M.Ye. (2019). Informational Theory of Evidence and the Problems of Using the Electronic Means of Proving in Criminal Procedure. *Journal of the National Academy of Legal Sciences of Ukraine*, 26(2), 118-130.

[8] Akhtyrska, N.M. (2016). To the Issue of Evidentiary Power of Cyber Information in the Aspect of International Cooperation During Criminal Proceedings. *Scientific Bulletin of the Uzhhorod National University*, 36(2), 123-125.
[9] Bilousov, A.S. (2008). Forensic analysis of objects of computer crimes. PhD Thesis. Kyiv: Taras Shevchenko National University of Kyiv.
[10] Kotlyarevsky, O.I., & Kytsenko, D.M. (1998). Computer Information as Physical Evidence in Criminal Case. *Information Technologies and Information Protection*, 2, 70-79.
[11] Krytska, I.O. (2016). Physical Evidence and Digital Information: Concepts and Relationships. *Journal of the Kyiv University of Law*, 1, 301-305.
[12] Muradov, V.V. (2013). Electronic Evidence: Forensic Aspect of Use. *Comparative-analytical Law*, 3-2, 313-315.
[13] Orlov, Yu.Yu., & Chernyavskyi, S.S. (2017). Electronic Display as a Source of Evidence in Criminal Proceedings. *Legal Journal of the National Academy of Internal Affairs*, 1(13), 12-22.
[14] Razmetaeva, Yu., & Razmetaev, S. (2021). Justice in the Era of Digital Technologies: Technological Solutions, Hidden Threats and Tempting Opportunities. *Access to Justice in Eastern Europe*, 2(10), 104-117. https://doi.org/10.33327/AJEE-18-4.2-a000061.
[15] Digital forensics. *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Digital_forensics.
[16] Rosenblatt, K.S. (1995). *High-Technology Crime: Investigating Cases Involving Computers*. San Jose: KSK Publications.
[17] Meah, J. (August 19, 2022). Digital Forensics: The Ultimate Guide. *Techopedia*. Retrieved from https://www.techopedia.com/digital-forensics-the-ultimate-guide/2/34721.
[18] Kabay, M.E. (2008). *A Brief History of Computer Crime: An Introduction for Students*. Norwich: School of Graduate Studies of Norwich University. Retrieved from http://www.mekabay.com/overviews/history.pdf.
[19] Rouse, M. (August 24, 2022). Digital Forensics. *Techopedia.* Retrieved from https://www.techopedia.com/definition/27805/digital-forensics.
[20] Mohanakrishnan, R. (July 18, 2022). What Is Digital Forensics? Meaning, Importance, and Types. *Spiceworks*.. Retrieved from https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/.
[21] Kolodina, A.S., & Fedorova, T.S. (2022). Digital forensics: problems of theory and practice. *Kyiv Journal of Law*, 1, 176-180. https://doi.org/10.32782/klj/2022.1.27.
[22] Prokopenko, S. (2017). Practice and Features of Conducting Computer and Technical Examinations. Materials of the IV All-Ukrainian Conference on Criminal Law and Procedure. Kyiv. Retrieved from https://uba.ua/documents/events/2017/20171109/Prokopenko.pdf.
[23] Rouse, M. Op. cit.
[24] Javed, A.R., Ahmed, W., Alazab, M., & Jalil, Z. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*, 10, 11065-11089. https://doi.org/10.1109/ACCESS.2022.3142508.
[25] Angelopoulou, O., Jones, A., Horsman, G., & Pourmoafi, S. (2022). A Study of the Data Remaining on Second-Hand Mobile Devices in Study of the Data Remaining on Second-Hand Mobile Devices in the UK. *Journal of Digital Forensics, Security and Law Security and Law*, 17(5). Retrieved from https://commons.erau.edu/jdfsl/vol17/iss2/5.
[26] Kapur, A. (2021). Digital Forensics in Cloud Computing. *International Journal of Computer Applications*, 183(18), 10-13. https://doi.org/10.5120/ijca2021921524.

[27] Chopade, R., & Pachghare, V.K. (2019). Ten Years of Critical Review on Database Forensics Research. *Digital Investigation*, 29, 180-197. https://doi.org/10.1016/j.diin.2019.04.001.
[28] Mohanakrishnan, R. Op. cit.
[29] Guo, H., & Hou, J. (2018). Review of the Accreditation of Digital Forensics in China. *Forensic Sciences Research*, 3(3), 194-201. https://doi.org/10.1080/20961790.2018.1503526.
[30] Leppänen, A., & Kankaanranta, T. (2017). Cybercrime Investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 18(2), 157-175. https://doi.org/10.1080/14043858.2017.1385231.
[31] What is Data Forensics? *Digital Guardian*. Retrieved from https://www.digitalguardian.com/dskb/data-forensics.
[32] Criminology Vs. Criminalistics: What's the Difference? *BestAccreditedColleges*. Retrieved from https://bestaccreditedcolleges.org/articles/criminology-vs-criminalistics-whats-the-difference.html.
[33] Powell, A., Stratton, G., & Cameron, R. (1982). *Digital Criminology: Crime and Justice in Digital Society*. London: Taylor & Francis. https://doi.org/10.4324/9781315205786.
[34] Digital Criminology. *Purdue University*. Retrieved from https://www.admissions.purdue.edu/majors/a-to-z/digital-criminology.php.
[35] Vasileiadis, A. Digital criminology in solving cybercrime. *hakin9*. Retrieved from https://hakin9.org/digital-criminology-in-solving-cybercrime-by-anastasis-vasileiadis/.
[36] Criminology (Cybercrime and Cybersecurity) MSc–2023 entry. *University of Surrey*. Retrieved from https://www.surrey.ac.uk/postgraduate/criminology-cybercrime-and-cybersecurity-msc.
[37] Kolodina, A.S., & Fedorova, T.S. Op. cit.
[38] Borysova, K.E., & Svitlichnyi, V.A. (November 25, 2022). Application of Digital Forensics. In *Modern trends in the Development of Criminology and the Criminal Process under Martial Law: Materials of the Int. Scient. and Pract. Conf.* (pp. 83-84). Kharkiv: KhNUVS. Retrieved from https://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/14869/Zastosuvannia%20tsyfrovoi%20kryminalistyky_Borysova_Svitlychnyi_2022.pdf?sequence=1&isAllowed=y.
[39] Order of the Ministry of Justice of Ukraine No. 53/5 "On the Approval of the Instructions on the Appointment and Conduct of Forensic Examinations and Expert Studies and Scientific and Methodological Recommendations on the Preparation and Appointment of Forensic Examinations and Expert Studies". (October 8, 1998). Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text.
[40] Law of Ukraine No. 4038-XII "On forensic examination". (February 25, 1994). Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12#Text.
[41] Forensic Science: Types & Etymology. *Study.Com.* Retrieved from https://study.com/learn/lesson/what-is-forensic-science-forensic-science-types-etymology.html.
[42] Forensic Science. *Britannica.Com.* Retrieved from https://www.britannica.com/science/forensic-science.
[43] Order of the Ministry of Justice of Ukraine No. 301/5 "On the Approval of the Regulation on the Central Expert Qualification Commission under the Ministry of Justice of Ukraine and the Certification of Judicial Experts". (March 3, 2015). Retrieved from https://zakon.rada.gov.ua/laws/show/z0249-15#Text.
[44] Experts in Digital Forensics. *Ukrforensic.Com.* Retrieved from https://www.ukrforensic.com/.
[45] Aleksandrenko, O.V., & Zhenuntiy, V.I. (December 12, 2019). Innovations and Digital Technologies in Forensics and Forensics: Modern Opportunities and Problems of Application. *Innovative Methods and Digital Technologies in Criminology, Forensic*

Examination and Legal Practice: International "Round Table" Materials. Kharkiv, 10-14.
[46] Fedotov, N.N. (2007). *Forensics – Computer Forensics*. Moscow.
[47] *Computer forensics*. Lviv: Faculty of Law of Ivan Franko National University of Lviv. Retrieved from https://law.lnu.edu.ua/course/digitalforensics.
[48] Andrianova, T. (July 20, 2018). Forenzik – Must have Ukrainian Business. *Nota Group. In Defense of Ukrainian Business*. Retrieved from https://notagroup.com.ua/ru/news/forenzik-must-have-ukrainskogo-biznesa/.
[49] Stulina, A. (2019). Applied Art. *Legal Practice*, 41. Retrieved from https://pravo.ua/articles/prikladnoe-iskusstvo/.
[50] Dubinina, M.V., Syrtseva, S.V., & Yankovska, T.Yu. (2019). Forensics as a Method of Investigating Intra-Corporate Cases of Fraud. *Market infrastructure*, 38, 377-383. https://doi.org/10.32843/infrastruct38-59.
[51] Chubenko, A.G., Loshytskyi, M.V., Pavlov, D.M., Bychkova, S.S., & Yunin, O.S. (2018). Compliance with Legislation and Internal Procedures (Compliance); Compliance. *Terminological dictionary on issues of prevention and countermeasures against legalization (laundering) of proceeds obtained through crime, financing of terrorism, financing of proliferation of weapons of mass destruction and corruption*. Kyiv: Vaite.
[52] ISO/IEC 27037:2012. Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Retrieved from https://www.iso.org/standard/44381.html.
[52] The Berkeley Protocol for Conducting Investigations Using Open Digital Data. New York: United Nations. Retrieved from https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf .
[53] Mamedov, G. (June 8, 2022). Digital Forensics. How Did it Help Gather Evidence of the Buch Crimes? *New Voice*. Retrieved from https://nv.ua/opinion/voyna-v-ukraine-kak-cifrovaya-kriminalistika-razoblachaet-prestupleniya-rf-v-ukraine-novosti-ukrainy-50248411.html.
[54] Mohanakrishnan, R. (July 18, 2022). What Is Digital Forensics? Meaning, Importance, and Types. *Spiceworks*. Retrieved from www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/.

Ігор Вікторович Лущик
науковий співробітник лабораторії теоретичних досліджень,
міжнародної, редакційно-видавничої та науково-методичної діяльності
Національний науковий центр
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»
61177, вул. Золочівська, 8-а, Харків, Україна
e-mail: fizedu@ukr.net
ORCID 0000-0001-9766-4628

Анатолій Серафимович Тяпкін
завідувач сектору лабораторії теоретичних досліджень,
міжнародної, редакційно-видавничої та науково-методичної діяльності
Національний науковий центр
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»
61177, вул. Золочівська, 8-а, Харків, Україна
e-mail: tyapkin@ukr.net
ORCID 0000-0003-0773-8959

Ihor V. Lushchyk
Researcher Laboratory of Theoretical Research,
International, Editorial and Publishing, Scientific and Methodological Activities
National Scientific Center "Hon. Prof. M.S. Bokarius Forensic Science Institute"
61177, Zolochivska Str., 8-a, Kharkiv, Ukraine
e-mail: fizedu@ukr.net
ORCID 0000-0001-9766-4628

Anatolii S. Tiapkin
Head of Sector of Laboratory of Theoretical Research,
International, Editorial and Publishing, Scientific and Methodological Activities
National Scientific Center "Hon. Prof. M.S. Bokarius Forensic Science Institute"
61177, Zolochivska Str., 8-a, Kharkiv, Ukraine
e-mail: tyapkin@ukr.net
ORCID 0000-0003-0773-8959

Рекомендоване цитування: Лущик І. В., Тяпкін А. С. Проблемні питання визначення цифрової криміналістики. *Теорія і практика правознавства.* 2023. Вип. 1(23). С. 135–160. https://doi.org/10.21564/2225-6555.2023.23.281734.

Suggested Citation: Lushchyk, I.V., & Tiapkin, A.S. (2023). Problematic Issues of Definition of Digital Forensics. *Theory and Practice of Jurisprudence,* 1(23), 135-160. https://doi.org/10.21564/2225-6555.2023.23.281734.

Стаття надійшла / Submitted: 12.06.2023
Прорецензовано / Revised: 22.06.2023
Затверджено / Approved: 26.06.2023
Опубліковано / Published online: 30.06.2023