This method is based on analyzing the peculiarities of the formation of the sequence of video frames in a group of images in the video, including the creation feature of individual types of frames.

The peculiarities of three types of video frames, their formation and order of formation into groups in the video stream are described and analyzed. Specific examples of the order of frames used in typical codecs of Moving Picture Experts Group - H.261 and H.264 are presented.

An optimal algorithm for identifying signs of editing has been proposed, which determines these signs based on the general principles of forming the sequence of frames in a videograms, as well as the characteristics of each type of video frame, without using specialized software.

Empirical examples indicate that relying solely on the detected signs of violations in the formation of frames and their sequence is insufficient. Therefore, to establish the truthfulness of the presence of editing in the videograms, the detection of signs of editing is carried out in conjunction with other methods of analysis. The synthesis of all detected signs of editing using as many methods as possible is presented as a result of the research to obtain the most accurate result. The obtained results can be useful for the development of automated systems for detecting fake videos and combating disinformation.

Keywords: Signs of video editing, video frame sequence, video frame, order of frame sequence, codec, MPEG, H.261, H.264.

DOI: 10.33766/2524-0323.102.289-305
УДК: 343.982.9

Степанюк Р. Л., *доктор юридичних наук, професор, професор кафедри криміналістики, судової експертології та домедичної підготовки Харківського національного університету внутрішніх справ (м. Харків, Україна)*
e-mail: stepanuk2@ukr.net
ORCID iD: https://orcid.org/0000-0002-8201-4013
Колесник В. Г., *завідувач відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України (м. Харків, Україна)*
e-mail: vit.kolesnyk@gmail.com
ORCID iD: https://orcid.org/0009-0000-2843-2989

СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА: СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ

У статті проаналізовано сучасний рівень теоретичного розвитку та практичної реалізації судової комп'ютерно-технічної експертизи у кримінальному провадженні. Визначено, що в Україні така експертиза є найбільш вагомим засобом дослідження цифрових доказів з метою вирішення питань, що виникають у кримінальному провадженні. Проте в цій галузі наявні проблеми, пов'язані з недосконалою внутрішньою класифікацією її різновидів, поширенням у правоохоронній практиці завдань, вирі-

шення яких можливе лише в комплексі з іншими видами експертних досліджень, недоліками при підготовці слідчими об'єктів для експертного дослідження та формулюванні питань експертові.

Головним чинником, що визначає результативність комп'ютерно-технічної експертизи, є якість наданих матеріалів, оскільки зараз, крім вилучення безпосередньо електронних носіїв, слідчому варто отримати та зафіксувати процесуальним шляхом паролі від систем логічного захисту. Наголошено, що у сфері комп'ютерно-технічних досліджень з'явились нові виклики, пов'язані з розкриттям і розслідуванням злочинів, пов'язаних з російською збройною агресією проти України.

Ці дослідження суттєво допомагають встановлювати важливі для досудового розслідування факти та виявляти цифрові докази (комп'ютерні дані), які підтверджують протиправні діяння, що виявляються в державній зраді, колабораційній діяльності, порушенні законів та звичаїв війни, пропаганді війни тощо. Забезпечення належного рівня технічного оснащення судової комп'ютерно-технічної експертизи насамперед полягає у використанні спеціалізованих апаратних і програмних засобів, які можна класифікувати на: універсальні експертні програмні та апаратно-програмні засоби, спеціальні пристрої апаратного блокування запису та пристрої для виготовлення побітових копій з оригінальних носіїв, апаратно-програмні мобільні комплекси й експертне програмне забезпечення для дослідження мобільних пристроїв, програмне забезпечення для відновлення даних.

У сфері науково-методичного забезпечення комп'ютерно-технічної експертизи видається актуальною потреба вдосконалення порядку атестації та реєстрації експертних методик у напрямі пришвидшення цих процедур, забезпечення їх відкритості та доступності змісту зацікавленим особам.

Перспективними напрямами подальшого розвитку судової комп'ютерно-технічної експертизи є розроблення процедур і методів вилучення та дослідження віддалених (хмарних) даних, цифрових даних з бортових комп'ютерів автомобілів, пам'яті та програмного забезпечення безпілотних літальних апаратів.

Ключові слова: спеціальні знання, судова експертиза, кримінальне провадження, розслідування кримінальних правопорушень, електронні докази, комп'ютерно-технічна експертиза, цифрова криміналістика.

Постановка проблеми. В останню чверть століття однією з найбільш популярних і результативних галузей судових наук (судової експертизи та криміналістики) є розділ, присвячений дослідженню цифрових (електронних) доказів, який у різних моделях криміналістики відрізняється за назвою і частково за змістом, але динамічно розвивається і стає все більш затребуваним у практичній діяльності правоохоронних органів. Це пов'язано з надзвичайно широкою сферою використання електронних засобів та інформації в повсякденному житті людини. Якщо раніше відповідні знання були потрібними лише під час розслідування комп'ютерних злочинів, то зараз цифрові сліди можуть залишатись і, отже, мають піддаватись криміналістичному дослідженню у кримінальному провадженні фактично за будь-яким кримінальним правопорушенням. Цифрові пристрої все частіше стають предметом вчинення кримінального правопорушення, його інструментом, носіями слідів і слідоутворюючими об'єктами.

Відповідно, цифрові сліди є вагомими джерелами доказів у кримінальних провадженнях про різноманітні кримінальні правопорушення. У сучасних умовах війни в Україні технології дослідження цифрових слідів дозволяють фіксувати обставини воєнних злочинів і викривати осіб, які їх учинили, що додатково підкреслює актуальність зазначеної проблематики.

Однією зі сфер, якій у перманентних умовах політичної й економічної кризи в Україні до недавнього часу не приділялось належної уваги, є галузь цифрової криміналістики, період бурхливого розвитку котрої прийшовся на останні тридцять років. Відповідний розділ криміналістичної техніки поки що не сформовано. Проте розвивається окремий рід судової експертизи – комп'ютерно-технічна, яка потребує постійної уваги науковців і практиків, зважаючи на значення відповідних технологій. Тому існує потреба дослідити теоретичні та прикладні аспекти щодо змісту цієї судової експертизи у вирішенні завдань з розслідування різних видів і груп кримінальних правопорушень задля визначення напрямів подальшого розвитку даної сфери у вітчизняній криміналістиці та судовій експертизі.

Аналіз останніх досліджень і публікацій. Питання призначення та проведення комп'ютерно-технічної експертизи під час розслідування кримінальних правопорушень досліджували Д. Гавриленко та М. Войтович, Б. Теплицький, Н.Карпинська та О. Крикунов, І. Завдов'єва та К. Макарук, В. Юсупов та А. Саковський, а також О. Довженко, В. Поліщук, М. Климчук, К. Латиш, В. Білоус й інші науковці, які звертали увагу насамперед на її об'єкти, предмет і можливості. Методичні аспекти цієї експертизи проаналізував П. Харківський. Водночас комплексного наукового аналізу сучасного стану та визначення перспектив розвитку комп'ютерно-технічної експертизи вітчизняними криміналістами не проводилось.

Формулювання цілей. Мета статті – проаналізувати сучасний рівень теоретичного розвитку та практичного застосування судової комп'ютерно-технічної експертизи у кримінальному провадженні, виокремити пріоритети в цій галузі та окреслити перспективні напрями її подальшого розвитку. Для досягнення цієї мети поставлено наступні завдання: визначити сучасні завдання судової комп'ютерно-технічної експертизи, що постають під час розкриття та розслідування кримінальних правопорушень, а також можливості їх вирішення; охарактеризувати стан технічного забезпечення комп'ютерно-технічної експертизи; оцінити рівень науково-методичного забезпечення комп'ютерно-технічної експертизи; визначити перспективи її подальшого розвитку.

Виклад основного матеріалу. Відомо, що цифрова криміналістика почала формуватись ще в 70-х роках минулого століття. Із середини 80-х років перейшла до якісно нового рівня у зв'язку зі значним розширенням сфери використання персональних комп'ютерів. Надалі подолала кілька вагомих віх у своєму розвитку [1] і зараз демонструє значні досягнення у справі протидії злочинності. На нинішньому етапі цифрова криміналістика являє собою самостійну галузь судових наук, систему наукових методів дослідження цифрових доказів з метою сприяння виявленню та розслідуванню кримінальних правопорушень [2, с. 290].

Поки що в Україні немає адекватного аналогу в криміналістиці, проте найбільш вагомі технічні аспекти дослідження цифрових (електронних) слідів кримінальних правопорушень розвиваються в рамках комп'ютерно-технічної експертизи, яка сформована як окремий рід експертизи у вітчизняній системі судових експертиз.

Сьогодні судова комп'ютерно-технічна експертиза є основною процесуальною формою використання спеціальних знань у галузі комп'ютерних технологій, а її результати можуть являти собою найважливішу частину доказової бази в конкретному кримінальному провадженні [3, с. 308]. З-поміж спеціальностей, за якими присвоюється кваліфікація судового експерта, вона визначена окремим індексом 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», тому науковці нерідко вживають терміни «комп'ютерно-технічна експертиза» й «експертиза комп'ютерної техніки і програмних продуктів» як синоніми [4, с. 141], що в нинішніх умовах видається виправданим.

Інструктивними документами Міністерства юстиції України комп'ютерно-технічну експертизу віднесено до класу інженерно-технічних експертиз, визначено її предмет, основні завдання та можливості (Інструкція про призначення та проведення судових експертиз та експертних досліджень, затверджена наказом Міністерства юстиції України від 08.10.1998 №53/5, розділ II, п. 13). Цей вид досліджень прийнято поділяти на кілька підвидів: експертизу комп'ютерної техніки, програмних продуктів, інформаційно-комп'ютерну експертизу [5, с. 32], іноді ще комп'ютерно-мережеву експертизу [6, с. 37-38]. Крім того, варто враховувати, що з комп'ютерно-технічної в самостійний вид експертизи виокремилась експертиза телекомунікаційних систем і засобів [7, с. 76]. Цілком доречно зазначено, що «відсутність чітких уявлень про предмет експертизи, її видовий розподіл, застаріла класифікація об'єктів експертизи тощо перешкоджають системній розробці методів експертного дослідження, налагодженню активної взаємодії між підрозділами, які проводять досудове розслідування злочинів» [8, с. 98]. У зв'язку з цим класифікація може бути і більш розгалуженою, насамперед залежно від об'єктів дослідження.

Об'єкти комп'ютерно-технічної експертизи, як зазначено, «доволі різноманітні і пов'язані із функціонуванням інформаційних систем» [4, с. 141]. У сучасній практиці експертам найчастіше надають на дослідження пристрої, які знаходяться у повсюдному вжитку і можуть вміщувати цифрові сліди кримінальних правопорушень. Через те науковцями, наприклад, запропоновано виокремлювати експертизи мобільних телефонів і комунікаторів, відеореєстраторів [8], що видається доречним, зважаючи на надзвичайну популярність таких пристроїв, затребуваність завдань щодо їх експертного дослідження у практиці правоохоронних органів для розкриття та розслідування кримінальних правопорушень, та водночас специфіку засобів і методів проведення відповідної експертизи. Особливо це має відношення до мобільних телефонів, які зараз є найбільш поширеним об'єктом комп'ютерно-технічної експертизи [9, с. 207], але також й актуальним і щодо інших цифрових пристроїв.

Крім того, варто зауважити, що широке використання цифрової техніки майже в усіх сферах життя людини, у тому числі й у механізмах злочинної діяльності, призвело до потреби застосовувати засоби й методи цифрової криміналістики під час багатьох інших видів судових експертиз. Науковці намагаються визначити коло експертиз, які тісно пов'язані з комп'ютерно-технічною, адже нерідко також досліджують цифрові сліди кримінальних правопорушень. Зокрема, до них відносять технічну експертизу документів, фототехнічну, фоноскопічну, економічну, товарознавчу, автотехнічну, пожежно-технічну, електротехнічну експертизи, судову експертизу з техніки безпеки та ін. [10]. Дослідниками проаналізовано специфіку призначення комплексних комп'ютерно-технічних і мистецтвознавчих [11], економічних[12], техніко-криміналістичних експертиз документів [13] тощо за різними категоріями кримінальних правопорушень. Загалом у судовій експертизі все «більшого значення набувають експертні дослідження комплексного характеру, що цілком зрозуміло, адже надійність висновків щодо об'єкта, вивченого взаємопов'язано з позицій різних наук, якісно зростає» [14, с. 4]. Як свідчить сучасна експертна практика, найчастіше комп'ютерно-технічна експертиза проводиться комплексно з експертизою звуко-, відеозапису, фототехнічною та судово-мистецтвознавчою експертизами.

За нашими даними, протягом останніх років спостерігається тенденція до збільшення кількості призначених слідчими і прокурорами комп'ютерно-технічних експертиз у кримінальному провадженні. Наприклад, до Харківського НДЕКЦ МВС у 2020 році їх було призначено 206, а у 2021 – 358. З початком активної фази війни у 2022 році Харківська область опинилась у зоні інтенсивних бойових дій, що певним чином відобразилось на показниках роботи експертів і не дозволяє порівнювати статистику 2022 року. Але з'явились нові виклики, пов'язані з розкриттям і розслідуванням злочинів, унаслідок російської збройної агресії проти України. Тут комп'ютерно-технічні дослідження також виявились потрібними і досить дієвими інструментами, на що наголошено науковцями [15, с. 809-812].

З 2022 року разом із молекулярно-генетичними дослідженнями та експертизами зброї, вибухових речовин і виробів у системі експертного забезпечення розслідування злочинів, що пов'язані зі збройною агресією проти України, найбільш актуальними є комп'ютерно-технічні дослідження. За їх допомогою слідчі та прокурори намагаються встановити важливі для досудового розслідування факти та виявити доказову інформацію (комп'ютерні дані), яка зберігається (зберігалася) на електронних носіях та підтверджує інкриміновані підозрюваному діяння, будь то державна зрада, колабораційна діяльність, порушення законів і звичаїв війни, пропаганда війни тощо. Найбільш поширеними видами таких даних є графічні файли (створені підозрюваним цифрові фотографії чи відеозаписи військових об'єктів, графічні файли, на яких відображено карти місцевості з координатами розташування військових формувань Збройних Сил України), файли документів і таблиць (наприклад, документація окупаційної адміністрації держави-агресора або самопроголошених органів, які узурпували

виконання владних функцій на тимчасово окупованих територіях України), листування підозрюваного із представниками збройних формувань та/або окупаційною адміністрацією держави-агресора у програмах обміну повідомленнями (мобільних застосунках), передавання їм інформації про переміщення, рух або розташування Збройних Сил України тощо.

Типовими завданнями, які вирішують експерти, є: 1) установлення технічного стану (працездатності) комп'ютерної техніки; 2) пошук та виявлення інформації, що міститься на електронних носіях; 3) відновлення видаленої інформації; 4) пошук слідів та історії мережевої активності користувача, відвідування інтернет-ресурсів, пошукових запитів, історії листування (обміну повідомленнями); 5) аналіз дій користувача та програмного забезпечення у комп'ютерній системі (пошук слідів віддаленого втручання в систему, впливу шкідливого програмного забезпечення); 6) аналіз пам'яті мобільного телефону, під час якого дослідженню підлягають: історія листування користувача в застосунках обміну повідомленнями (месенджерах, соціальних мережах), історія використання застосунків, історія завантаження та відправлення файлів, історія викликів, текстові SMS-повідомлення;

Аналіз практики призначення комп'ютерно-технічних експертиз, насамперед, але не виключно, при розслідуванні воєнних злочинів дозволяє визначити деякі проблемні аспекти, вирішення яких, на наш погляд, сприятиме поліпшенню цієї сфери практичної діяльності.

Загалом призначення комп'ютерно-технічної експертизи є слідчою дією, спрямованою на отримання віртуальної інформації, з огляду на специфіку об'єкта й предмета її дослідження [16, с. 124]. Призначення судової експертизи слідчим включає кілька послідовних стадій [17, с. 60-64], серед яких найбільш проблемними для окремого роду (виду) експертизи видаються визначення предмета дослідження (формулювання питань експерту) і підготовка об'єктів, які направляються для експертного дослідження.

Під час формулювання питань для комп'ютерно-технічної експертизи слідчому варто дотримуватись вимог, до ряду яких відносять застосування встановленого нормативно понятійного апарату, максимальну чіткість та однозначність поставлених перед експертом питань, які не можуть безпосередньо мати відношення до етапів проведення дослідження ним інформації та методики дослідження; також неприпустимість питань довідкового та правового характеру, відповідність наявній методичній і технічній базі, доступній судовому експерту, спрямованість на встановлення конкретних обставин події, що належать до предмету доказування, мінімізацію матеріальних витрат на проведення експертизи [18, с. 309].

Аналіз сучасної практики в галузі судової комп'ютерно-технічної експертизи свідчить про те, що ці рекомендації ініціатори її проведення враховують не завжди. Зокрема слідчі нерідко ставлять перед експертами неконкретизовані завдання, вирішення яких передбачає дослідження набагато більшого обсягу даних, ніж це необхідно для розслідування. Наслідком цього, як мінімум, є істотне

збільшення строків проведення експертизи, адже експертові доводиться витрачати зайвий час і ресурси. Тому варто наголосити, що поставлені питання мають бути чіткими, а їх перелік збалансованим. Наприклад, ставлячи завдання щодо пошуку, вилучення та збереження листування користувача в програмах обміну повідомленнями (месенджерах), слідчому доцільно вказувати конкретних абонентів або назви чатів, які необхідно дослідити, а не доручати повністю скопіювати всю інформацію з усіх месенджерів. При наданні на дослідження відеореєстратора варто зазначати конкретний часовий інтервал, що стосується події, яку розслідують.

Оскільки однозначного та виключного переліку типових запитань, які можна поставити на вирішення комп'ютерно-технічної експертизи не існує, формувати їх варто, зважаючи на обставини конкретної події. Украй необхідним є постійне навчання та підвищення кваліфікації працівників слідчих підрозділів з метою їх належного інформування щодо особливостей призначення даного виду судової експертизи, поставлення запитань, доведення до них меж компетенції комп'ютерно-технічної експертизи.

Однією з важливих передумов успіху проведення експертизи також є правильне вилучення й упакування об'єктів дослідження. Постійний розвиток систем апаратного та програмного захисту інформації та збільшення розміру даних є одними із основних технічних проблем при підготовці об'єктів для проведення судової комп'ютерно-технічної експертизи. Наявність засобів повнодискового шифрування носіїв, таких як Bitlocker, TrueCrypt, VeraCrypt на системах OS Windows, LUKS на системах OS Linux, FileVault2 на системах Mac OS, за відсутності відомого паролю, який ініціатор має надати судовому експерту, унеможливлює дослідження таких носіїв та пошук інформації на них.

Протягом останніх років значно зросла якість шифрування та засобів забезпечення безпеки сучасних мобільних пристроїв. Пам'ять сучасного мобільного телефону та інформація в ній шифрується виробником одразу з моменту його випуску. З кожним роком можливості комп'ютерно-технічної експертизи в подоланні систем логічного захисту зменшуються (навіть з використанням сучасних програмних та апаратних засобів), звужується вікно можливостей для повного та якісного вилучення інформації. Таким чином, усе частіше проведення експертизи стає неможливим у зв'язку з технічною неможливістю отримати доступ до інформації, що розташована на електронному носії (у пам'яті) об'єкта дослідження за відсутності пароля. Тому при підготовці об'єкта для його направлення на комп'ютерно-технічну експертизу, ініціатору необхідно вжити всіх можливих процесуальних заходів для виявлення пароля від системи логічного захисту цього об'єкту та надати його експертові.

Крім того, постійний розвиток засобів захисту в сучасних телефонах та недостатня обізнаність слідчих та оперативних співробітників в особливостях їх функціонування, нерідко призводить до негативних наслідків, що виражаються у втраті можливості доступу до інформації в телефоні або самої такої інформації через помилки під час вилучення пристроїв. Серед таких помилок найбільш ти-

повими є невмикання автономного режиму («режиму польоту») і відповідно незабезпечення його захисту від зовнішнього впливу через мережу мобільного оператора та мережі бездротового зв'язку, вимикання телефону без його попереднього огляду, витягання SIM-карти з увімкненого телефону і втрата можливості дослідження телефону після його розблокування відбитком пальця або системою розпізнавання обличчя.

Як зазначається в міжнародних інструкціях для правоохоронних органів, на місці події доцільно використовувати лише два основних алгоритми дій правоохоронця по збереженню інформації в телефоні. Перший – ввімкнення «режиму польоту» без витягання SIM-карти з одночасним постійним підтримуванням стану зарядженості батареї (під'єднання power bank) та упакуванням телефону в пакет, що блокує радіохвилі (т.з. «пакет Фарадея») [19, с. 153]. Другий алгоритм витікає з першого та виконується в разі можливості розблокування особою телефону відбитком пальця або системою розпізнавання обличчя – розблокований телефон переводиться в «режим польоту», після чого в його налаштуваннях дисплею та меню налаштувань безпеки встановлюються параметри: «Вимикання екрану» – «ніколи», «Блокування екрану/режим очікування» – «ніколи», яскравість екрану виставляється в мінімум з метою збільшення строку збереження заряду батареї, телефон під'єднується до зовнішнього носія живлення (power bank) та упаковується в пакет, що блокує радіохвилі. Таким чином, екран телефону не буде гаснути, телефон знаходитиметься постійно в розблокованому стані та може вільно оглядатись до розряджання всіх джерел живлення. Вимкнути біометричний захист у сучасних телефонах неможливо, оскільки при спробі його вимкнення телефон запитає числовий пароль розблокування. Указаний другий спосіб наразі є найбільш ефективним, його застосовують навіть для розблокування телефону потерпілого при вбивстві, використовуючи палець чи обличчя вбитого прямо на місці події, звичайно, із дотриманням усіх процесуальних процедур. Діючи невідкладно, доки телефон не заблокований, існує можливість синхронізувати переписку з месенджерів та деякі інші відомості з телефону на комп'ютер.

Як можемо спостерігати на практиці, спираючись на стан мобільних телефонів, що надходять на експертизу, переважній більшості слідчих та оперативних співробітників, окрім працівників спеціальних технічних управлінь, вищевказані алгоритми відомі не завжди, що призводить до непоодиноких випадків втрати важливої доказової інформації. Отже, головним чинником, що визначає результативність комп'ютерно-технічної експертизи, наразі є якість наданих матеріалів, оскільки зараз, крім вилучення безпосередньо електронних носіїв, слідчому варто отримати та зафіксувати фіксації процесуальним шляхом паролі від систем логічного захисту.

Щодо технічного забезпечення комп'ютерно-технічної експертизи, зауважимо, що під час її проведення експерти застосовують спеціалізовані апаратні засоби та програмне забезпечення, асортимент яких на ринку є солідним. Науковцями відзначено критичну залежність судової експертизи від відповідних інструментів, без яких неможливий аналіз цифрових пристроїв [20]. Тому кожна

експертна лабораторія повинна мати відповідне обладнання, програмне забезпечення, підтримувати його в дієвому стані та періодично оновлювати.

Пропонуємо наступну криміналістичну класифікацію спеціалізованих засобів для виявлення й аналізу цифрових слідів, які використовують у вітчизняній експертній практиці:

1. Універсальні експертні програмні та апаратно-програмні засоби, призначені для криміналістичного дослідження комп'ютерних носіїв інформації та мобільних пристроїв: X-Ways Forensics та EnCase® Forensic (універсальні програмні комплекси, що дозволяють вирішувати практично весь спектр експертних завдань від знімання даних (створення образів) до їх відновлення та складання звітів); AccessData Forensic Toolkit (універсальний програмний комплекс, що здатний впоратися зі значними обсягами даних); Magnet AXIOM (багатофункціональний програмний засіб, спрямований, насамперед, на дослідження мережевої активності користувача (дослідження веббраузерів, месенджерів, програм для файлообміну) та журналів дій користувача в операційній системі); Magnet DVR Examiner (спеціальний програмний засіб для дослідження носіїв цифрових відеореєстраторів, пошуку та відновлення інформації на них); UFED 4PC (універсальний апаратно-програмний комплекс для аналізу цифрових даних із мобільних пристроїв) [21, с. 152].

2. Спеціальні пристрої апаратного блокування запису для запобігання умисного втручання або випадкового редагування інформації на вилучених оригінальних носіях інформації: Tableau Forensic Bridge, Digital Intelligence UltraBlock, WiebeTech Forensic UltraDock, EPOS WriteProtector, а також пристрої для виготовлення побітових копій з оригінальних носіїв, наприклад, Tableau Forensic Duplicator TD3, IM Solo-4 Forensic, ICS Image MASSter 4000 Pro, EPOS DiskMaster Portable [22, с. 47-48].

3. Апаратно-програмні мобільні комплекси, які дають можливість одержувати, декодувати й аналізувати цифрову інформацію з мобільних пристроїв: «Cellebrite UFED Touch 2»; «MSAB XRY Field».

4. Експертне програмне забезпечення для криміналістичного дослідження мобільних пристроїв: Oxygen Forensic Detective, MD-NEXT, MOBILedit Forensic.

5. Програмне забезпечення для відновлення даних: «UFS Explorer Professional Recovery», «R-Studio» тощо [23, с. 322].

В аспекті методичного забезпечення комп'ютерно-технічної експертизи з одного боку спостерігається суттєва кількість офіційно затверджених експертних методик, але з іншого існують і деякі проблемні питання. Зважаючи на постійний розвиток комп'ютерної індустрії, слушно зауважено, що рівень науково-методичного забезпечення комп'ютерно-технічної експертизи потребує постійного вдосконалення [24, с. 9], а отже, експертні методики мають динамічно розвиватись.

Нині в Україні зареєстровано понад 20 експертних методик за спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», більшість яких розроблена фахівцями судово-експертних установ Міністерства юс-

тиції України. Проте надзвичайно швидке оновлення засобів і програмного забезпечення у сфері інформаційних технологій призводить до швидкої застарілості методів їх криміналістичного аналізу. Крім того, існує досить дивна ситуація, коли навіть наявні методики є недоступними для судових експертів, що працюють в інших установах. Як приклад, можемо навести методику експертного дослідження грального автоматів, відеоатракціонів, лотерейних терміналів та конструктивно схожих з ними пристроїв (10.9.16), яка в установах Експертної служби МВС України не використовується. Немає й критеріїв обов'язковості обрання експертами офіційно зареєстрованих методик, їх пріоритетності, порівняно з іншими методами судової експертизи. Відповідно, у практичній діяльності виникають складнощі, пов'язані з використанням експертами різних методик, конкуренцією офіційно визнаних та інших експертних методів, відсутності методик дослідження новітніх цифрових приладів, комп'ютерних програм і додатків тощо.

З цього приводу зазначимо, що, на нашу думку, у нинішніх умовах бурхливого науково-технічного прогресу в галузі інформаційних технологій існуюча в Україні система атестації та державної реєстрації методик проведення судових експертиз виглядає дещо архаїчною й потребує перегляду з метою адаптації до сучасних підходів. Вважаємо доцільним вжити заходів принаймні щодо забезпечення швидкості оновлення зареєстрованих методик та доступності їх змісту зацікавленим особам. Варто вдосконалити нинішній порядок атестації методик, який являє собою недостатньо прозору внутрішньовідомчу процедуру оцінки наукових звітів на користь відкритих дискусій у провідних наукових виданнях. Можливо, взагалі варто відмовитись від практики державної реєстрації методик. Крім того, недоступність текстів експертних методик заважає не тільки їх засвоєнню судовими експертами, а і в цілому об'єктивній оцінці з боку наукової спільноти, а також оцінки наукової обґрунтованості висновків судових експертиз в конкретних кримінальних провадженнях.

Насамкінець звернемо увагу на найбільш, на нашу думку, перспективні напрями подальшого розвитку судової комп'ютерно-технічної експертизи.

Завдяки технології хмарних середовищ та засобів резервного копіювання, значна частина даних користувача перебуває на віддалених ресурсах, які не можуть бути об'єктом дослідження комп'ютерно-технічної експертизи, оскільки виходять за межі класичного підходу до об'єкта дослідження, згідно з яким об'єкт має бути фізично наданий експерту на матеріальному носії. Таким чином, значна частина даних (файли з електронної поштової скриньки, дані збережені на Google Drive, Google Docs, Amazon AWS, One Drive, Dropbox, MEGA і т.ін.), котрими користувався власник пристрою, але які не були фізично збережені на його електронному носії та перебувають у віддалених сховищах, лишаються недоступними для експерта. Аналізуючи функціональні властивості та оновлення у спеціальному програмному забезпечені для комп'ютерно-технічної експертизи, можемо спостерігати появу майже в кожному з них інструментів для вилучення таких даних. Для цього використовуються авторизаційні дані, токени та ключі користувача, вилучені з пристрою.

Законодавство багатьох держав, інструкції та процедури вже адаптовані та дозволяють здійснення таких експертних досліджень [25, с. 641]. На жаль, сучасна українська експертна практика та науковці у своїх працях визначають об'єктами дослідження виключно матеріальні та матеріалізовані носії інформації, що досліджуються експертом засобами спеціальних наукових знань у межах предмета експертного дослідження. Тобто, вилучення та дослідження віддалених (хмарних) даних наразі можливе лише шляхом слідчого огляду, оскільки в судовій експертизі неможлива практика проведення дослідження інформації, яка фізично не перебуває на матеріальному об'єкті, що ініціатор надає експерту. На нашу думку, комп'ютерно-технічна експертиза в Україні має стати більш гнучкою в питаннях допустимості та належності об'єктів дослідження, необхідно оновлення вже існуючих і створення нових методик, що розширюють поточний перелік об'єктів дослідження в галузі експертизи хмарних даних. Також серед перспективних напрямів розвитку комп'ютерно-технічної експертизи слід виділити дослідження програмного забезпечення бортових комп'ютерів автомобілів, а також і пам'яті та програмного забезпечення безпілотних літальних апаратів (дронів), насамперед в умовах воєнного стану.

Висновки. Комп'ютерно-технічна експертиза в Україні є найбільш вагомим засобом дослідження цифрових доказів з метою вирішення питань, що виникають у кримінальному проваджені. Проте в цій галузі експертизи існують і чисельні проблеми, пов'язані з недосконалою внутрішньою класифікацією її різновидів, поширенням у правоохоронній практиці завдань, вирішення яких можливе в комплексі з іншими видами експертних досліджень, недоліками при підготовці слідчими об'єктів для експертного дослідження та формулюванні питань експертові. Головним чинником, що визначає результативність комп'ютерно-технічної експертизи, є якість наданих матеріалів, оскільки зараз, крім вилучення безпосередньо електронних носіїв, слідчому варто отримати та зафіксувати процесуальним шляхом паролі від систем логічного захисту.

У сфері комп'ютерно-технічних досліджень з'явились нові виклики, пов'язані з розкриттям і розслідуванням злочинів унаслідок російської збройної агресії проти України. Зазначена експертиза є найбільш актуальною в експертному забезпеченні розслідування таких кримінальних правопорушень. Вона надає слідчим і прокурорам можливість встановити важливі для досудового розслідування факти та виявити цифрові докази (комп'ютерні дані), які підтверджують протиправні діяння, що виявляються в державній зраді, колабораційній діяльності, порушенні законів та звичаїв війни, пропаганді війни тощо.

Забезпечення належного рівня технічного оснащення судової комп'ютерно-технічної експертизи насамперед полягає у використанні спеціалізованих апаратних і програмних засобів, які можна класифікувати на: універсальні експертні програмні та апаратно-програмні засоби, спеціальні пристрої апаратного блокування запису та пристрої для виготовлення побітових копій з оригінальних носіїв, апаратно-програмні мобільні комплекси й експертне програмне забезпечення для дослідження мобільних пристроїв, програмне забезпечення

для відновлення даних. У сфері науково-методичного забезпечення комп'ютерно-технічної експертизи видається актуальною потреба вдосконалення порядку атестації та реєстрації експертних методик у напрямі пришвидшення цих процедур, забезпечення їх відкритості та доступності змісту зацікавленим особам.

Перспективними напрямами подальшого розвитку судової комп'ютерно-технічної експертизи вбачаються розроблення процедур і методів вилучення та дослідження віддалених (хмарних) даних, цифрових даних з бортових комп'ютерів автомобілів, пам'яті та програмного забезпечення безпілотних літальних апаратів.

Використані джерела:

1. Pollitt M. A History of Digital Forensics. In: Chow KP., Shenoi S. (eds) Advances in Digital Forensics VI. Digital Forensics 2010. IFIP *Advances in Information and Communication Technology*. Vol 337. Springer, Berlin, Heidelberg. URL : https://doi.org/10.1007/978-3-642-15506-2_1.

2. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2022. Вип. 3(99). С. 283-284.

3. Стецик Б. В. Завдання експерта при проведенні судової комп'ютерної-технічної експертизи. *Актуальні проблеми правового регулювання в Україні та країнах ближнього зарубіжжя: Матеріали XI міжнародної науково-практичної Інтернет конференції (Львів, 28 грудня 2021 року): тези доповідей/Відп. ред. П.О. Куцик*. Львів : Растр-7, 2021. С. 308-311.

4. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис: журнал/упоряд. О. Крикунов*. Луцьк : Східноєвроп. нац. ун-т ім. Лесі Українки, 2017. № 1 (9). С. 140-144

5. Теплицький Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 3 (120). С. 28-34.

6. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навчальний посібник / Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с.

7. Лапта С. П. Щодо предмета експертизи телекомунікаційних систем і засобів. *Вісник Харківського національного університету внутрішніх справ*. 2011. № 3 (54). С. 75-79.

8. Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. № 2 (22). С. 97-100

9. Латин К. В. Судова комп'ютерно-технічна експертиза мобільних телефонів: аспекти призначення. *Інновації в криміналістиці та судовій експертизі:* матеріали міжвідом. наук.-практ. конф. (Київ, 25 листоп. 2021 р.) / [редкол.: В. В. Чернєй, С. С. Чернявський, А. А. Саковський та ін.]. Київ : Нац. акад. внутр. справ, 2021. С. 206-209

10. Гавриленко Д. Є., Войтович М. М. Комплексний характер судової комп'ютерно-технічної експертизи та її зв'язок з іншими родами та видами судових експертиз. *Судово-експертна діяльність:* сучасний стан та перспективи розвитку: збірник матеріалів круглого столу. / редкол.: Кобилянський О. Л., Антонюк П. Є., Свобода Є. Ю. Київ: ННІПФЕКП НАВС, 2015. С. 94-97.

11. Кравчук О. В. Особливості призначення і проведення комплексних комп'ютерно-технічних та мистецтвознавчих судових експертиз. *Порівняльно-аналітичне право*. 2015. № 1. С. 302-304.

12. Завдов'єва І. Г., Макарук К. Є. Особливості призначення і проведення комплексних комп'ютерно-технічних та економічних судових експертиз. *Криміналістичний вісник*. 2014. № 2. С. 107-111.

13. Юсупов В. В., Саковський А. А. Особливості призначення технічної експертизи документів у кримінальних провадженнях про корупційні правопорушення. Реалізація державної антикорупційної політики в міжнародному вимірі: матеріали VI Міжнар. наук.- практ. конф. (Київ, 9–10 груд. 2021 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2021. С. 174-175.

14. Гончаренко В. Г. Організаційні та правові проблеми судової експертизи в Україні. *Часопис Академії адвокатури України*. 2011. № 1(10). С. 1-5.

15. Shevchuk V. M. Criminalistics support for the investigation of military criminal offenses and war crimes: digitalization, innovations, prospects. *Military offences and war crimes: background, theory and practice : collective monograph. Ed. by V. M. Stratonov*. Riga, Latvia : «Baltija Publishing», 2023. URL : dhttps://doi.org/10.30525/978-9934-26-302-6-35.

16. Довженко О. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2019. Вип. 55. Т. 2. С. 124-127.

17. Пирог І. В. Щодо питання відносення судової експертизи до слідчих (розшукових) дій. *Криміналістика і судова експертиза*. 2019. Вип. 64. С. 58-68. URL : https://doi.org/10.33994/kndise.2019.64.03.

18. Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. Науковий вісник Національної академії внутрішніх справ. 2018. № 3. С. 303-315.

19. Sammons J. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier, 2012. 208 p. URL : https://doi.org/10.1016/C2010-0-68337-4.

20. Horsman G. «I couldn't find it your honour, it mustn't be there!» –Tool errors, tool limitations and user error in digital forensics. *Science & Justice*. 2018. 58(6). P. 433-440. URL : https://doi.org/10.1016/j.scijus.2018.04.001.

21. Полішук В. А. Роль комп'ютерно-технічної експертизи в розкритті та розслідувані кримінальних правопорушень. *Матеріали VI Міжнародної науково-технічної конференції молодих учених та студентів. «Актуальні задачі сучасних технологій» (Тернопіль, 16-17 листопада 2017)*. Тернопіль : ТНТУ ім. Івана Пулюя, 2017. 151-152.

22. Неня О. В., Корнійко С. М., Гуляєв А. В., Березненко Н. М. Окремі питання використання інформаційних технологій в комп'ютерно-технічній експертизі. *Актуальні проблеми криміналістичного та експертного забезпечення діяльності правоохоронних органів та суду в Україні : тези доп. учасників наук.-практ. конф. (Харків, 28 трав. 2021 р.)*. Харків : НДІ ППСН, 2021. С. 46-49.

23. Омельян О. С. Актуальні питання впровадження цифрових технологій у діяльність судового експерта. *Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 15 травня 2020 р.)*. Київ : НА СБУ, 2020. С. 321-323.

24. Білоус В., Латиш К. Судові експертизи радіоелектронних засобів як форма використання спеціальних знань під час розслідування корупційних кримінальних

правопорушень. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2022. № 1 (61). С. 5-11. URL : https://doi.org/10.32689/2522-4603.2022.1.1

25. Mamta Khanchandani, Dr. Nirali Dave. Analysis of Cloud Forensics : Review and Impact on Digital Forensics Aspects. *International Journal of Scientific Research in Science and Technology (IJSRST)*. March-April 2021. Vol. 8 Iss. 2. P. 639-646. URL : https://doi.org/10.32628/IJSRST 2182118

References:

1. Pollitt, M. A. (2010) History of Digital Forensics. *In: Chow KP., Shenoi S. (eds) Advances in Digital Forensics VI. Digital Forensics. IFIP Advances in Information and Communication Technology, vol. 337.* Springer, Berlin, Heidelberg. URL : https://doi.org/10.1007/978-3-642-15506-2 1.

2. Stepaniuk, R. L., Perlin, S. I. (2022) Tsyfrova kryminalistyka y udoskonalennia systemy kryminalistychnoi tekhniky v Ukraini. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E.O. Didorenka – Bulletin of the Luhansk State University of Internal Affairs named after E.O. Didorenko, 3(99), 283-284.* [in Ukrainian].

3. Stetsyk, B. V. (2021) Zavdannia eksperta pry provedenni sudovoi kompiuterno-tekhnichnoi ekspertyzy. *Aktualni problemy pravovoho rehuliuvannia v Ukraini ta krainakh blyzhnoho zarubizhzhia: Materialy XI mizhnarodnoi naukovo-praktychnoi Internet konferentsii (Lviv, 28 hrud.): tezy dopovidei - Actual problems of legal regulation in Ukraine and the countries of the near abroad: Materials of the 11th international scientific and practical Internet conference (Lviv, December 28): abstracts of reports, 308-311* / Vidp. red. P.O. Kutsyk. Lviv : Rastr-7,. [in Ukrainian].

4. Karpinska, N., Krykunov, O. (2017) Okremi pytannia provedennia sudovoi kompiuterno-tekhnichnoi ekspertyzy u kryminalnomu sudochynstvi. *Istoryko-pravovyi chasopys: zhurnal. Lutsk : Skhidnoievrop. nats. un-t im. Lesi Ukrainky – History and Law Journal: scientific journal. Lutsk: Lesya Ukrainka Volyn National University, 1 (9), 140-144.* [in Ukrainian].

5. Teplytskyi, B. (2021) Aktualni pytannia pryznachennia ekspertyzy kompiuternoi tekhniky i prohramnykh produktiv pid chas rozsliduvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system, kompiuternykh merezh i merezh elektrozviazku. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav – Scientific journal of the National academy of internal affairs, 3 (120), 28-34.* [in Ukrainian].

6. Klymchuk, M. P., Komissarchuk, Yu. A., Marko, S. I., Stetsyk, B. V. (2022) Sudova kompiuterno-tekhnichna ekspertyza u kryminalnomu provadzhenni : navchalnyi posibnyk . Lviv : Lvivskyi derzhavnyi universytet vnutrishnikh sprav. [in Ukrainian].

7. Lapta, S. P. (2011) Shchodo predmeta ekspertyzy telekomunikatsiinykh system i zasobiv. *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav – Bulletin of Kharkiv National University of Internal Affairs, 3 (54), 75-79.* [in Ukrainian].

8. Kharkivskyi, P. P. (2014) Kompiuterno-tekhnichna ekspertyza: problemni pytannia. *Kryminalistychnyi visnyk – Forensic Herald, 2 (22), 97-100.* [in Ukrainian].

9. Latysh, K. V. (2021) Sudova kompiuterno-tekhnichna ekspertyza mobilnykh telefoniv: aspekty pryznachennia. *Innovatsii v kryminalistytsi ta sudovii ekspertyzi : materialy mizhvidom. nauk.-prakt. konf. (Kyiv, 25 lystop.) - Innovations in criminology and forensic examination: interdisciplinary materials. science and practice conf. (Kyiv, November 25), 206-209. / [redkol.: V. V. Cherniei, S. S. Cherniavskyi, A. A. Sakovskyi (Eds.) et al.]. Kyiv : Nats. akad. vnutr. Sprav.* [in Ukrainian].

10. Havrylenko, D. Ye., Voitovych, M. M. (2015) Kompleksnyi kharakter sudovoi kompiuterno-tekhnichnoi ekspertyzy ta yii zviazok z inshymy rodamy ta vydamy

sudovvkh ekspertvz. *Sudovo-ekspertna diialnist: suchasnui stan ta perspektyvy rozvutku: zbirnuk materialiv kruhloho stolu - Forensic expert activity: current state and development prospects: collection of materials of the round table, 94-97./ redkol..: Kobylianskyi O. L., Antoniuk P. Ie., Svoboda Ye. Iu. (Eds.) Kyiv: NNIPFEKP NAVS, 94-97.* [in Ukrainian].

11. Kravchuk, O. V. (2015) Osoblyvosti pryznachennia i provedennia kompleksnykh kompiuterno-tekhnichnykh ta mystetstvoznavchykh sudovykh ekspertyz. *Porivnialno-analitychne pravo – Comparative and analytical law, 1, 302-304.* [in Ukrainian].

12. Zavdovieva, I. H., Makaruk, K. Ye. (2014) Osoblyvosti pryznachennia i provedennia kompleksnykh kompiuterno-tekhnichnykh ta ekonomichnykh sudovykh ekspertyz. *Krymina listychnyi visnyk – Forensic Herald, 2, 107-111.* [in Ukrainian].

13. Yusupov, V. V., Sakovskyi, A. A. (2021) Osoblyvosti pryznachennia tekhnichnoi ekspe rtyzy dokumentiv u kryminalnykh provadzhenniakh pro koruptsiini pravopo rushennia. *Realizatsiia derzhavnoi antykoruptsiinoi polityky v mizhnarodnomu vymiri: materialy VI Mizhnar. nauk.-prakt. konf. (Kyiv, 9–10 hrud.) - Implementation of the state anti-corruption policy in the international dimension: materials of VI International. science - practice conf. (Kyiv, December 10), 174-175 / [redkol.: V. V. Cherniei, S. D. Husariev, S. S. Cherniavskyi et al.]. Kyiv : Nats. akad. vnutr. sprav.* [in Ukrainian].

14. Honcharenko, V. H. (2011) Orhanizatsiini ta pravovi problemy sudovoi ekspertyzy v Ukraini. *Chasopys Akademii advokatury Ukrainy – Journal of the Academy of Advocacy of Ukraine, 1(10), 1-5.* [in Ukrainian].

15. Shevchuk, V. M. (2023) Criminalistics support for the investigation of military criminal offenses and war crimes: digitalization, innovations, prospects. *Military offences and war crimes: background, theory and practice : collective monograph. Ed. by V.M. Stratonov*. Riga, Latvia : «Baltija Publishing». URL : https://doi.org/10.30525/978-9934-26-302-6-35.

16. Dovzhenko, O. (2019) Deiaki pytannia pryznachennia kompiuterno-tekhnichnoi ekspertyzy pid chas rozsliduvannia kiberzlochyniv. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Uzhhorod National University Herald. Series: Law, 55 (2), 124-127.* [in Ukrainian].

17. Pyrih, I. V. (2019) Shchodo pytannia vidnesennia sudovoi ekspertyzy do slidchykh (rozshukovykh) dii. *Kryminalistyka i sudova ekspertyza – Criminalistics and Forensics, 64, 58-68*. URL : https://doi.org/10.33994/kndise.2019.64.03. [in Ukrainian].

18. Teplytskyi, B. B. (2018) Zavdannia, obiekty y pytannia kompiuterno-tekhnichnoi sudovoi ekspertyzy. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav – Scientific journal of the National academy of internal affairs, 3, 303-315.* [in Ukrainian].

19. Sammons, J. (2012) The basics of digital forensics: the primer for getting started in digital forensics. Elsevier. URL : https://doi.org/10.1016/C2010-0-68337-4.

20. Horsman, G. (2018) «I couldn't find it your honour, it mustn't be there!» –Tool errors, tool limitations and user error in digital forensics. *Science & Justice, 58(6), 433-440.* URL : https://doi.org/10.1016/j.scijus.2018.04.001.

21. Polishchuk, V. A. (2017) Rol kompiuterno-tekhnichnoi ekspertyzy v rozkrytti ta rozsliduvani kryminalnykh pravoporushen. *Materialy VI Mizhnarodnoi naukovo-tekhnichnoi konferentsii molodykh uchenykh ta studentiv. «Aktualni zadachi suchasnykh tekhnolohii» (Ternopil, 16-17 lystop.).* Ternopil : TNTU im. Ivana Puliuia, *151-152.* [in Ukrainian].

22. Nenia, O. V., Korniiko, S. M., Huliaiev, A. V., Bereznenko, N. M. (2021) Okremi pytannia vykorystannia informatsiinykh tekhnolohii v kompiuterno-tekhnichnii ekspertyzi. *Aktualni problemy kryminalistychnoho ta ekspertnoho zabezpechennia diialnosti pravookhoronnykh*

orhaniv ta sudu v Ukraini : tezy dop. uchasnykiv nauk.-prakt. konf. (Kharkiv, 28 trav.) - "Actual tasks of modern technology" (Ternopil, November 16-17), 46-49. Kharkiv: NDI PPSN. [in Ukrainian].

23. Omelian, O.S. (2020) Aktualni pytannia vprovadzhennia tsyfrovykh tekhnolohii u diialnist sudovoho eksperta. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 15 trav.), 321-323.* Kyiv : NA SBU. [in Ukrainian].

24. Bilous, V., Latysh, K. (2022) Sudovi ekspertyzy radioelektronnykh zasobiv yak forma vykorystannia spetsialnykh znan pid chas rozsliduvannia koruptsiinykh kry minalnykh pravoporushen. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Yurydychni nauky – Scientific Works of Interregional Academy of Personnel Management. Legal Sciences, 1 (61), 5-11.* URL : https://doi.org/10.32689/2522-4603.2022.1.1. [in Ukrainian].

25. Mamta Khanchandani, Dr. Nirali, Dave (2021) Analysis of Cloud Forensics : Review and Impact on Digital Forensics Aspects. *International Journal of Scientific Research in Science and Technology (IJSRST).* March-April, *Vol. 8, Iss. 2, 639-646.* URL : https://doi.org/10.32628/IJSRST2182118.

Стаття надійшла до редколегії 26.04.2023

Stepaniuk R., *Doctor of Law, Professor, Professor of the Department of Criminalistics, Forensic Expertise and Pre-Medical Training Kharkiv National University of Internal Affairs (Kharkiv, Ukraine)*
Kolesnyk V., *Head of the Department of Computer and Telecommunication Forensics, Kharkiv Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine (Kharkiv, Ukraine)*

FORENSIC COMPUTER AND TECHNICAL EXPERTISE: STATE AND PROSPECTS OF DEVELOPMENT

The article analyzes the current level of theoretical development and practical implementation of forensic computer-technical expertise in criminal proceedings. This expertise is defined to be the most significant means of examining digital evidence in order to resolve issues arising in criminal proceedings in Ukraine.

However, there are problems in this area related to the imperfect internal classification of its types, the spread in law enforcement practice of tasks that can only be solved in conjunction with other types of expert research, and shortcomings in the preparation of objects for expert research by investigators and the formulation of questions to the expert. The main factor that determines the effectiveness of a computer-technical expertise is the quality of the materials provided, since now, in addition to seizing electronic media directly, the investigator should obtain and record passwords to logical security systems. It is emphasized that new challenges have emerged in the field of computer science research related to the detection and investigation of crimes related to Russian armed aggression against Ukraine.

These studies significantly help to establish facts important for the pre-trial investigation and identify digital evidence (computer data) confirming illegal acts manifested in treason, collaboration, violation of the laws and customs of war, war propaganda, etc. Ensuring an appropriate level of technical equipment for forensic computer and technical expertise primarily involves the use of specialized hardware and software, which can be classified into: universal expert software and hardware and software tools, special hardware record

blocking devices and devices for making bit copies from original media, hardware and software mobile complexes and expert software for the study of mobile devices, data recovery software.

In the field of scientific and methodological support of computer and technical expertise, it seems urgent to improve the procedure for certification and registration of expert methods in order to speed up these procedures, ensure their openness and accessibility of content to interested persons. Promising areas for the further development of forensic computer-technical expertise are the development of procedures and methods for extracting and examining remote (cloud) data, digital data from on-board computers of cars, memory and software of unmanned aerial vehicles.

Keywords: specialized knowledge, forensic expertise, criminal proceedings, investigation of criminal offenses, electronic evidence, computer-technical expertise, digital forensics.