DOI: 10.33270/05267202.10
УДК 343.985 (477)

КАРАМАН Костянтин*
доктор філософії в галузі політології, докторант Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України
61177, вул. Золочівська, 8а, м. Харків, Україна
ORCID: https://orcid.org/0000-0003-2965-9661

Призначення комп'ютерно-технічної експертизи під час розслідування злочинів

Анотація. У статті здійснено комплексне дослідження організаційно-тактичних і процесуальних засад призначення комп'ютерно-технічної експертизи під час розслідування кримінальних правопорушень. Обґрунтовано, що в умовах стрімкого поширення цифрових технологій і постійного посилення ролі електронних доказів комп'ютерно-технічна експертиза набуває значення однієї з найзатребуваніших форм використання спеціальних знань у кримінальному провадженні. Встановлено, що її результати використовують не лише під час розслідування кіберзлочинів, а й у кримінальних провадженнях щодо шахрайства, фінансування тероризму, злочинів проти основ національної безпеки, поширення порнографічних матеріалів, передачі відомостей про місця дислокації ЗСУ та інших правопорушень, де доказове значення мають цифрові сліди. У статті визначено предмет, об'єкти й основні різновиди комп'ютерно-технічної експертизи, схарактеризовано її місце в системі інженерно-технічних судових експертиз. Встановлено, що найдоцільнішим є поділ об'єктів дослідження на апаратні, програмні й інформаційні. Окреслено типові завдання, які виконують під час проведення комп'ютерно-технічної експертизи, зокрема встановлення технічного стану пристроїв, дослідження електронного листування, виявлення шкідливого програмного забезпечення, відновлення видаленої інформації, встановлення часу створення чи зміни файлів, IP-адрес, геолокаційних параметрів і фактів використання конкретних програмних продуктів. Визначено особливості підготовки матеріалів для проведення експертизи, специфіку вилучення, пакування, транспортування та зберігання цифрових носіїв інформації. Акцентовано, що неналежне вилучення пристроїв, самостійний перегляд файлів слідчим, відсутність паролів, PIN-кодів, ключів шифрування або інших відомостей про доступ до облікових записів можуть істотно знизити ефективність експертного дослідження або взагалі унеможливити його проведення. На підставі аналізу судової практики узагальнено найпоширеніші обставини, для встановлення яких призначають комп'ютерно-технічну експертизу, а також визначено типові помилки, яких припускаються під час її призначення. Обґрунтовано необхідність подальшого вдосконалення методичних рекомендацій щодо роботи із цифровими доказами, активнішого залучення спеціалістів під час вилучення цифрових носіїв і ширшого використання комплексних експертиз за участю фахівців у галузі телекомунікацій, програмування та цифрової криміналістики.

Ключові слова: цифровізація; кіберпростір; спеціальні знання; судова експертиза; призначення експертизи; комп'ютерна техніка.

Історія статті:
Отримано: 11.03.2026
Прийнято: 16.04.2026
Опубліковано: 29.05.2026

Рекомендоване посилання:
Караман К. Призначення комп'ютерно-технічної експертизи під час розслідування злочинів. *Наука і правоохорона.* 2026. Вип. 2 (72). С. 93–102. DOI: 10.33270/05267202.10

*Відповідальний автор

Вступ

Стрімкий розвиток інформаційних технологій, цифровізація суспільних відносин й активне використання комп'ютерної техніки в усіх сферах життєдіяльності обумовлюють не лише позитивні трансформації, а й появу нових способів учинення кримінальних правопорушень. Комп'ютерні системи, мобільні пристрої, мережеве обладнання, хмарні сервіси, електронна пошта, соціальні мережі й інші цифрові ресурси дедалі частіше стають як знаряддям учинення злочину, так і місцем відображення криміналістично значущої інформації про кримінальне правопорушення. Комп'ютерну техніку використовують не лише під час учинення кримінальних правопорушень у сфері комп'ютерної інформації, а й у справах про шахрайства, легалізацію доходів, незаконний обіг наркотичних засобів, фінансування тероризму, корупційні злочини, воєнні злочини, злочини проти основ національної безпеки, а також злочини, вчинені організованими групами.

Специфіка цифрових слідів полягає в тому, що вони часто мають нематеріальний характер, можуть швидко змінюватися, знищуватися або приховуватися, а їх виявлення та дослідження потребує використання спеціальних знань у галузі комп'ютерної техніки, програмного забезпечення, телекомунікацій, криптографії та цифрової криміналістики. Саме тому в більшості випадків належне документування, вилучення, збереження та дослідження цифрової інформації неможливе без призначення комп'ютерно-технічної експертизи.

Комп'ютерно-технічна експертиза є однією з найпоширеніших форм використання спеціальних знань у кримінальному провадженні. Її результати дають змогу встановити робочий стан комп'ютерних засобів, виявити ознаки несанкціонованого втручання в роботу комп'ютерних систем, відновити видалені файли, дослідити програмне забезпечення, встановити способи використання технічних пристроїв, визначити зміст цифрової інформації та отримати інші відомості, що мають доказове значення. Особливої актуальності така експертиза набуває в умовах збільшення кількості кібератак, використання шкідливого програмного забезпечення, незаконного втручання в інформаційні системи та реалізації інших форм протиправної поведінки.

У правозастосовній практиці постає низка проблем, пов'язаних із призначенням комп'ютерно-технічної експертизи. Серед них – складність визначення виду та підвиду експертного дослідження, недостатній рівень обізнаності слідчих щодо можливостей окремих видів експертиз, помилки під час формулювання питань експерту, неналежне пакування та зберігання цифрових носіїв інформації, а також складнощі у виборі об'єктів, які підлягають направленню на дослідження. Усе це негативно впливає на ефективність доказування та може призводити до втрати важливої доказової інформації.

З огляду на викладене, актуальності набуває наукове дослідження організаційно-тактичних і процесуальних аспектів призначення комп'ютерно-технічної експертизи під час розслідування злочинів, а також визначення її ролі у встановленні обставин кримінального правопорушення та формуванні належної доказової бази.

Матеріали та методи

Методологічну основу дослідження становлять загальнонаукові та спеціально-юридичні методи пізнання, використані для визначення сутності, предмета, об'єктів і процесуального значення комп'ютерно-технічної експертизи в кримінальному провадженні. Теоретико-нормативну основу дослідження становлять положення КПК України, Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5[1], а також наукові праці, присвячені проблемам використання цифрових доказів, комп'ютерно-технічної експертизи, цифрової криміналістики та розслідування злочинів з використанням комп'ютерної техніки.

У дослідженні застосовано діалектичний метод, який дав змогу розглянути комп'ютерно-технічну експертизу як динамічне явище, що трансформується під впливом розвитку цифрових технологій, ускладнення способів вчинення кримінальних правопорушень і розширення кола цифрових слідів. Формально-юридичний метод використано для аналізу нормативних приписів, що визначають порядок призначення, проведення та використання висновків комп'ютерно-технічної експертизи в кримінальному провадженні. За допомогою системно-структурного методу визначено місце комп'ютерно-технічної експертизи в системі судових експертиз, схарактеризовано її основні різновиди, предмет, об'єкти й типові завдання.

Структурно-функціональний метод надав можливість дослідити роль комп'ютерно-технічної експертизи в механізмі доказування, з'ясувати її значення для встановлення технічного стану пристроїв, виявлення шкідливого програмного забезпечення, відновлення видаленої інформації, дослідження електронного листування, мережевої активності й інших цифрових слідів.

Емпіричну основу дослідження становлять матеріали судової практики, зокрема вироки в кримінальних провадженнях, пов'язаних із використанням комп'ютерної техніки, програмного забезпечення, месенджерів, цифрових носіїв

[1] Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text

інформації та інших електронних ресурсів. Це дало змогу встановити типові об'єкти експертного дослідження, найпоширеніші питання, які ставлять перед експертом, а також виявити проблеми, що виникають під час вилучення, пакування, зберігання та дослідження цифрових носіїв інформації.

Огляд літератури

Проблематика призначення та проведення комп'ютерно-технічної експертизи під час розслідування злочинів неодноразово ставала предметом наукового аналізу. Вагомий внесок у розроблення цієї тематики зробили Б. Б. Теплицький (2018), О. Ю. Довженко (2019), В. П. Любавіна та Г. В. Скляренко (2023), Ж. В. Удовенко та В. В. Удовенко (2024), Р. Л. Степанюк і В. Г. Колесник (2023), П. П. Харківський (2014), а також інші науковці, які досліджували питання класифікації різновидів комп'ютерно-технічної експертизи, визначення її об'єктів, формулювання питань експерту й використання цифрових доказів у кримінальному провадженні.

П. П. Харківський (2014) увагу спрямував на методичний аспект комп'ютерно-технічної експертизи, зокрема проблеми формування запитань експерту, дослідження програмного забезпечення та встановлення ознак несанкціонованого втручання в роботу комп'ютерних систем. Новаторською для того часу була його позиція щодо необхідності виокремлення спеціального напряму експертних досліджень, пов'язаного із шкідливими програмами, вірусами й засобами несанкціонованого доступу.

Одним із найрозробленіших напрямів є визначення змісту й структури комп'ютерно-технічної експертизи. Б. Б. Теплицький (2018) обґрунтовує, що основними її завданнями є діагностування апаратних засобів комп'ютерної системи, визначення функціонального призначення програмного забезпечення та пошук, виявлення, аналіз й оцінка комп'ютерної інформації, створеної користувачем або програмами. Науковець одним із перших запропонував концентрувати увагу не лише на технічному стані пристроїв, а й на функціональних характеристиках програмного забезпечення та цифрових даних як самостійних об'єктах експертного дослідження.

О. Ю. Довженко (2019) зосереджує увагу на складності визначення різновиду комп'ютерно-технічної експертизи на початковому етапі розслідування. Учений стверджує, що неправильне зазначення слідчим конкретного підвиду експертизи може ускладнити її проведення або призвести до неповного вирішення поставлених питань. Саме тому він пропонує орієнтуватися не на вузький різновид експертного дослідження, а на його загальний інженерно-технічний характер із подальшим уточненням експертною установою.

В. П. Любавіна та Г. В. Скляренко (2023) акцентують на особливостях кіберзлочинів як кримінальних правопорушень, що не залишають традиційної слідової картини. Науковці запропонували поділ об'єктів комп'ютерно-технічної експертизи на апаратні, програмні й інформаційні. Такий підхід дає змогу чітко визначати предмет дослідження, правильно формулювати питання експерту й обирати необхідні технічні засоби для дослідження. Крім того, автори обґрунтовують необхідність активної комунікації між слідчим й експертною установою, оскільки саме належне забезпечення експерта матеріалами, носіями інформації та доказами визначає результативність експертного дослідження.

Вагомий внесок у розвиток сучасного бачення судової комп'ютерно-технічної експертизи зробили Р. Л. Степанюк і В. Г. Колесник (2023). Науковці розглядають її як основний процесуальний інструмент дослідження цифрових доказів у кримінальному провадженні й зауважують, що цифрові сліди можуть залишатися майже в будь-якому кримінальному правопорушенні. Новаторською є їхня позиція щодо необхідності розвитку цифрової криміналістики як самостійної галузі судових наук і вдосконалення класифікації комп'ютерно-технічних досліджень. Вони також засвідчують перспективність дослідження віддалених хмарних даних, інформації з бортових комп'ютерів автомобілів, безпілотних літальних апаратів та інших новітніх цифрових систем. Виокремлюють значення отримання паролів доступу й інших засобів логічного захисту як необхідної умови повноцінного проведення експертизи.

Ж. В. Удовенко та В. В. Удовенко (2024) запропонували деталізовану класифікацію підвидів комп'ютерно-технічної експертизи. Науковці визначають експертизу комп'ютерної техніки, експертизу програмних продуктів та інформаційно-комп'ютерну експертизу. Вони обґрунтовують доцільність виокремлення експертизи шкідливих програмних засобів як комплексного дослідження, спрямованого на встановлення можливості використання певних кодів, файлів чи програм для несанкціонованого втручання в роботу інформаційних систем. Важливим є й запропонований авторами підхід до розмежування експертизи комп'ютерної техніки та експертизи телекомунікаційних систем залежно від характеру об'єкта дослідження і способу вчинення кримінального правопорушення.

Водночас аналіз наукової літератури дає підстави стверджувати, що більшість досліджень зосереджені або на окремих видах комп'ютерно-технічної експертизи, або на методичних аспектах формулювання питань експерту й дослідженні цифрових носіїв. Водночас недостатньо уваги спрямовано на комплексний аналіз організаційно-тактичних засад призначення таких експертиз, взаємодії слідчого з експертом, проблеми вилучення та збереження цифрових слідів, а також використання комп'ютерно-технічної експертизи під час розслідування воєнних злочинів, злочинів

проти основ національної безпеки, фінансування тероризму та інших кримінальних правопорушень, де цифрові докази відіграють дедалі важливішу роль.

Результати й обговорення

Комп'ютерно-технічна експертиза є одним із різновидів інженерно-технічних судових експертиз, предметом якої є встановлення фактичних даних щодо властивостей, стану, режиму функціонування, умов використання комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем і цифрової інформації. Необхідність її призначення зумовлена стрімким поширенням цифрових технологій, використанням комп'ютерних пристроїв майже в усіх сферах суспільного життя та збільшенням кількості кримінальних правопорушень, у механізмі яких застосовують комп'ютерну техніку, мобільні пристрої, мережеві ресурси чи цифрові сервіси.

Відповідно до Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5[1], комп'ютерно-технічна експертиза спрямована на дослідження апаратних і програмних засобів, інформації, що міститься на цифрових носіях, а також процесів оброблення, передавання та збереження інформації.

До ключових напрямів експертизи комп'ютерної техніки та програмного забезпечення належать встановлення технічного стану комп'ютерних засобів, з'ясування особливостей їх використання, виявлення інформації та програм, що зберігаються на цифрових носіях, а також перевірка відповідності програмних продуктів визначеним технічним параметрам, версіям чи вимогам, закладеним у технічному завданні на їх розроблення.

У межах такого виду експертизи можуть вирішувати питання щодо наявності на певному носії конкретної інформації, її змісту, форми збереження та способу відображення. Також встановлюють, чи містяться на досліджуваному пристрої відомості про певні дії користувача, зокрема відкриття, редагування, копіювання, видалення або передавання файлів. Важливе значення має встановлення того, чи здійснювали спроби знищення інформації шляхом форматування, видалення, перезапису чи застосування спеціальних програмних засобів.

Окремим напрямом є дослідження походження інформації. Експерт може визначити, чи було певну інформацію створено безпосередньо на конкретному комп'ютері, чи її було перенесено з іншого носія, а також установити спосіб такого перенесення. У необхідних випадках досліджують технологію та послідовність створення електронного документа, встановлюють дату й час його створення, редагування, друку, копіювання, переміщення чи видалення.

Під час дослідження програмного забезпечення може бути встановлено, чи містить накопичувач певні програми, які саме функції вони виконують, чи здатні вони забезпечувати реалізацію конкретних завдань, а також чи відповідає програмний продукт технічним вимогам, закладеним на етапі його розроблення. Крім того, експерт може визначити, чи реалізовані в програмному коді окремі функціональні можливості, передбачені технічним завданням.

Якщо предметом дослідження є технічний стан обладнання, експерт установлює наявність несправностей у роботі комп'ютерної техніки, окремих пристроїв або їх складових, а також визначає, як ці дефекти впливають на функціонування системи загалом.

Для проведення експертизи цифрової інформації здебільшого надають носій інформації, а за потреби – також системний блок або інший комплекс технічних засобів, до складу якого належить відповідний накопичувач. Носії інформації мають бути запаковані окремо, щоб уникнути їх пошкодження або несанкціонованого доступу до інформації. Системні блоки слід передавати в упаковці, яка виключає можливість підключення до електромережі чи безпосереднього доступу до носіїв без порушення цілісності пакування.

У випадках, коли досліджують відповідність програмного продукту певним параметрам, експерту необхідно надати носій з копією програми або її програмного коду. Якщо ж перевіряють технічний стан обладнання, разом із комп'ютерними засобами обов'язково надають технічну документацію до них.

З огляду на різноманітність цифрових пристроїв, програмних продуктів і способів збереження інформації, у кожному конкретному випадку доцільно попередньо консультуватися зі спеціалістом або експертом у галузі комп'ютерної техніки щодо визначення оптимального переліку об'єктів, які необхідно вилучити й направити на дослідження.

Експертиза комп'ютерної техніки спрямована на встановлення технічного стану пристроїв, їх справності, функціонального призначення, комплектності, наявності ознак втручання чи модифікації. Дослідженню можуть підлягати цифрові сліди й електронні докази (Kalancha, & Harkusha, 2021; Demydova, 2024; Pohoretskyi, 2025; Shepitko, 2025; Pohoretskyi, 2026). Експертиза програмних продуктів дає змогу дослідити характеристики програмного забезпечення, встановити його функціональне призначення, наявність ліцензійності, ознаки модифікації чи

[1] Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text

шкідливого впливу. Інформаційно-комп'ютерна експертиза пов'язана з пошуком, відновленням, дослідженням й аналізом цифрової інформації. Комп'ютерно-мережеві й телекомунікаційні експертизи застосовують для дослідження функціонування мереж, каналів зв'язку, маршрутизації трафіку, роботи серверів, базових станцій, мережевих пристроїв і телекомунікаційного обладнання.

Предметом комп'ютерно-технічної експертизи є фактичні дані про технічний стан комп'ютерної техніки, зміст і характеристики програмного забезпечення, властивості цифрової інформації, способи її створення, модифікації, передавання, видалення чи відновлення, а також причиново-наслідкові зв'язки між функціонуванням комп'ютерної системи та певними подіями.

Об'єктами дослідження під час проведення комп'ютерно-технічної експертизи можуть бути: 1) персональні комп'ютери, ноутбуки, сервери, планшети, смартфони; 2) периферійні пристрої; 3) мережеве обладнання; 4) носії інформації (жорсткі диски, SSD-накопичувачі, USB-носії, карти пам'яті, оптичні диски); 5) програмне забезпечення; 6) бази даних; 7) електронні документи; 8) електронна пошта; 9) журнали подій; 10) історія браузерів; 11) облікові записи; 12) хмарні сервіси; 13) резервні копії; 14) мультимедійні файли; 15) файли журналів, метадані й інші цифрові сліди.

Типовими завданнями, які виконує судовий експерт під час проведення комп'ютерно-технічної експертизи, є:

1) встановлення технічного стану комп'ютерного обладнання;

2) визначення працездатності пристроїв;

3) встановлення факту втручання у функціонування комп'ютерної системи;

4) виявлення ознак несанкціонованого доступу;

5) встановлення часу створення, зміни або видалення файлів;

6) відновлення видаленої інформації;

7) встановлення змісту електронного листування;

8) визначення використаних програмних продуктів;

9) встановлення факту використання шкідливого програмного забезпечення;

10) визначення IP-адрес, MAC-адрес, мережевих параметрів;

11) встановлення користувача, який здійснював певні дії;

12) виявлення способу приховування чи знищення цифрової інформації.

Обставини, які можуть бути встановлені за результатами проведення комп'ютерно-технічної експертизи, доцільно згрупувати в кілька блоків. Перший блок пов'язаний із встановленням характеристик технічних пристроїв. У межах цього напряму вирішують питання щодо виду пристрою, його технічних параметрів, працездатності, комплектності, наявності змін конструкції, факту механічного або програмного пошкодження.

Другий блок стосується дослідження програмного забезпечення. Експерт може встановити, які програми було встановлено на пристрої, яке їх функціональне призначення, чи є вони ліцензійними, чи використовували програми для віддаленого доступу, приховування інформації, шифрування, знищення даних або обходу засобів захисту.

Третій блок охоплює дослідження цифрової інформації. Ідеться про встановлення змісту документів, листування, журналів активності, історії пошуку, інформації про підключення зовнішніх носіїв, факту копіювання, видалення чи передачі файлів.

Четвертий блок пов'язаний з дослідженням мережевої активності й телекомунікаційних процесів. Експерт може встановити маршрути передавання даних, використані IP-адреси, геолокацію підключень, факти використання VPN-сервісів, проксі-серверів чи інших засобів анонімізації.

Для проведення комп'ютерно-технічної експертизи обов'язково направляють постанову про призначення експертизи або ухвалу слідчого судді, об'єкти дослідження, протоколи огляду, обшуку або тимчасового доступу, фототаблиці, відомості про спосіб вилучення пристроїв, інформацію про паролі доступу, логіни, PIN-коди, ключі шифрування, відомості про облікові записи й інші матеріали кримінального провадження, які можуть мати значення для дослідження.

Специфіка підготовки матеріалів для проведення комп'ютерно-технічної експертизи полягає в необхідності забезпечення цілісності цифрової інформації та недопущення її зміни. Саме тому під час вилучення комп'ютерної техніки необхідно: 1) зафіксувати поточний стан пристрою; 2) задокументувати підключення периферійних засобів; 3) сфотографувати екран й активні програми; 4) відобразити наявні мережеві з'єднання; 5) здійснити копіювання інформації із застосуванням спеціалізованих програмно-апаратних засобів; 6) забезпечити використання write-blocker-пристроїв; 7) окремо пакувати носії інформації; 8) уникати самостійного перегляду файлів чи запуску програм.

Посиленої уваги потребує вилучення мобільних пристроїв і комп'ютерної техніки, що знаходиться у ввімкненому стані. У таких випадках доцільно залучати спеціаліста, який може зафіксувати відкриті вікна програм, поточні мережеві з'єднання, вміст оперативної пам'яті, інформацію про активні процеси й інші дані, що можуть бути втрачені після вимкнення пристрою.

Водночас вагомим є значення цих висновків. Наприклад, у судовій справі № 174/491/21 комп'ютерно-технічну експертизу призначено з метою підтвердження факту використання персонального комп'ютера та конкретного програмного забезпечення для пошуку, завантаження, зберігання й подальшого розповсюдження файлів через мережу Інтернет. Важливим було також з'ясування особливостей налаштування програми «eMule», зокрема визначення папки обміну

файлами, до якої мали доступ інші користувачі мережі, а також встановлення того, чи забезпечували зроблені налаштування можливість автоматичного поширення файлів порнографічного змісту. Під час проведення комплексної комп'ютерно-технічної та мистецтвознавчої експертизи вирішували питання щодо наявності на жорсткому диску персонального комп'ютера відеофайлів і графічних файлів порнографічного змісту, часу їх завантаження, створення, зберігання та передачі іншим користувачам. Експерти також встановлювали факти використання конкретних IP-адрес, наявності доступу до мережі Інтернет, функціонування програми «eMule», способу розміщення файлів у папці спільного доступу й можливості їх неодноразового завантаження іншими користувачами. Крім того, під час дослідження було встановлено, що один із відеофайлів містив ознаки дитячої порнографії.

Об'єктами дослідження в цьому випадку були системний блок персонального комп'ютера, накопичувач на жорсткому магнітному диску марки «GoodRam» моделі SSDPR-CL100, програмне забезпечення «eMule», файли, що містилися в папці обміну, журнали активності програми, IP-адреси, що використовували під час підключення до мережі Інтернет, а також оптичні носії, які містили результати проведених слідчих дій і додатки до експертних висновків. Для проведення експертизи експертам були надані системний блок, цифрові носії інформації, матеріали обшуку, відомості про IP-адреси, а також інші матеріали кримінального провадження, необхідні для дослідження цифрових слідів і встановлення механізму вчинення кримінального правопорушення[1].

За результатами проведення експертизи було підтверджено факт зберігання та розповсюдження порнографічних матеріалів за допомогою програми «eMule», а також встановлено використання комп'ютерної техніки як безпосереднього знаряддя вчинення кримінального правопорушення.

В іншому кримінальному провадженні комп'ютерно-технічну експертизу призначали для підтвердження факту використання комп'ютерної техніки та шкідливого програмного забезпечення під час вчинення кримінальних правопорушень, передбачених ч. 3 ст. 190 та ч. 1 ст. 361-1 КК України. Основною метою дослідження було встановлення факту придбання, зберігання, використання та розповсюдження шкідливого програмного забезпечення «Heur:trojan-downloader.msoffice.agent.gen», а також визначення способу його передачі через месенджер «Telegram».

У межах експертизи вирішували питання щодо наявності на комп'ютерній техніці обвинуваченого шкідливих програмних засобів, часу їх завантаження, встановлення, запуску та використання, наявності листування в месенджері «Telegram», яке підтверджувало передачу шкідливого програмного забезпечення іншому користувачеві, а також встановлення зв'язку між конкретними цифровими носіями, акаунтами, IP-адресами й особою обвинуваченого. Крім того, експертиза мала встановити, чи використовували вилучену комп'ютерну техніку для незаконних операцій з використанням електронно-обчислювальної техніки, пов'язаних із продажем неіснуючої бази даних громадян України.

Об'єктами експертного дослідження стали: два системні блоки, ноутбук марки «Lenovo», мобільний телефон «Iphone 7+», жорсткі диски марок «Seagate» та «Hitachi», вісім флешносіїв, SIM-карти різних операторів мобільного зв'язку, банківські картки, а також інші цифрові носії та засоби комунікації, вилучені під час обшуку. Додатково на дослідження могли направляти журнали активності програм, дані акаунтів у месенджері «Telegram», інформацію про IP-адреси, електронне листування, а також чорнові записи, що містили відомості про паролі, логіни або інші дані для доступу до електронних ресурсів.

За результатами проведення комп'ютерно-технічних експертиз було підтверджено використання обвинуваченим комп'ютерної техніки для розповсюдження шкідливого програмного забезпечення та здійснення шахрайських дій через мережу Інтернет. Значний обсяг вилученої техніки й цифрових носіїв, а також складність дослідження цифрових слідів обумовили суттєві процесуальні витрати на проведення експертизи в сумі понад 33 тис. грн[2].

Суттєво підвищився попит органів досудового розслідування на призначення комп'ютерно-технічних експертиз у воєнних злочинах (Serhieieva, 2025). Наприклад, у справі № 202/8539/23 судову комп'ютерно-технічну експертизу призначали для підтвердження факту використання мобільного телефону та месенджера «Telegram» для передачі інформації про місця дислокації підрозділів ЗСУ, військової техніки, складів боєприпасів і військового устаткування. Основним завданням експертизи було встановлення наявності на мобільному пристрої електронних даних, які підтверджують листування з користувачем, пов'язаним із представниками держави-агресора, а також збереження, передачу й отримання повідомлень, фотографій, геолокаційних позначок і посилань на карти місцевості.

Для проведення дослідження експерту було надано мобільний телефон марки «Xiaomi Redmi Note 9 (M2003J15SG)» із зазначенням IMEI-кодів,

[1] Вирок Вільногірського міського суду Дніпропетровської області від 1 верес. 2021 р. Справа № 174/491/21. Провадження 1-кп/174/46/2021. URL: https://reyestr.court.gov.ua/Review/99343820

[2] Вирок Здолбунівського районного суду Рівненської області від 9 трав. 2023 р. Справа № 562/1245/23. Провадження 1-кп/562/180/23. URL: https://reyestr.court.gov.ua/Review/110723248

який належав обвинуваченій. Під час дослідження експерт перевіряв технічний стан пристрою, наявність інстальованих застосунків, можливість доступу до мережі Інтернет, функціонування месенджерів і журналів активності користувача. Увагу було зосереджено на додатку «Telegram», де виявлено листування між акаунтом обвинуваченої та користувачем «ОСОБА_7», що містило текстові повідомлення, скріншоти Google-карт, фотографії та позначення конкретних місць розташування військових об'єктів.

У межах комп'ютерно-технічної експертизи було вирішено питання щодо наявності на телефоні контактів, журналів викликів, SMS-повідомлень, електронного листування, а також щодо встановлення факту інсталяції та використання застосунків «Telegram», «Viber», «Instagram», «OK» і браузерів, які забезпечували передачу інформації через Інтернет. Експерт також здійснив копіювання виявлених відомостей у форматах .html та .xls, що дало змогу зберегти цифрові докази в незмінному вигляді та використати їх під час судового розгляду.

Крім мобільного телефону, на дослідження направляли оптичні диски з додатками до висновку експерта, які містили файли з фотознімками листування, журналами активності й іншими цифровими даними. Також використовували результати огляду інтернет-ресурсів, інформацію про телефонні з'єднання та текстові повідомлення, а також протоколи огляду речей і документів. За результатами експертизи підтверджено, що на мобільному телефоні містилися дані, які мають доказове значення для кримінального провадження, зокрема листування в «Telegram», пов'язане з передачею інформації про місця дислокації ЗСУ[1].

Практика призначення комп'ютерно-технічних експертиз засвідчує наявність низки проблемних питань. Однією з найпоширеніших проблем є неправильне визначення виду експертизи та формулювання запитань експерту. Нерідко слідчі ставлять перед експертом питання правового характеру, які виходять за межі його компетенції, або формулюють надто загальні питання, що унеможливлює отримання конкретного висновку.

Серед порушень правил підготовки об'єктів дослідження слід виокремити пошкодження носіїв інформації, порушення правил пакування, самостійний перегляд файлів слідчим чи оперативним працівником, барк інформації про паролі доступу, облікові записи та ключі шифрування, що можуть істотно ускладнювати або навіть унеможливлювати проведення експертизи.

Суттєві складнощі також виникають у випадках використання хмарних сервісів, месенджерів, VPN-технологій, криптовалютних платформ, шифрування інформації та багаторівневого логічного захисту. У таких ситуаціях проведення лише комп'ютерно-технічної експертизи часто є недостатнім, що зумовлює необхідність призначення комплексних досліджень із залученням експертів у галузі телекомунікацій, криптографії, економіки й інших спеціальних знань.

Окремою проблемою є швидка зміна цифрових технологій, поява нових програмних продуктів, платформ і способів приховування інформації. Це потребує постійного оновлення методик експертного дослідження, підвищення кваліфікації експертів і вдосконалення нормативного регулювання у сфері використання цифрових доказів.

Висновки

Комп'ютерно-технічна експертиза на сучасному етапі є однією з найзатребуваніших форм використання спеціальних знань у кримінальному провадженні, оскільки цифрові сліди залишаються майже в будь-якому кримінальному правопорушенні незалежно від його кримінально-правової характеристики. Її значення виходить далеко за межі розслідування кіберзлочинів, оскільки результати таких експертиз дедалі частіше використовують у справах про шахрайства, незаконне втручання в роботу інформаційних систем, фінансування тероризму, злочини проти основ національної безпеки, воєнні злочини, незаконний обіг порнографічних матеріалів, організовану злочинну діяльність й інші кримінальні правопорушення, де доказове значення мають цифрові носії, електронне листування, історія мережевої активності, геолокаційні дані та інші цифрові сліди.

Предмет комп'ютерно-технічної експертизи охоплює не лише технічний стан комп'ютерної техніки, а й зміст програмного забезпечення, цифрової інформації, особливості функціонування телекомунікаційних систем, способи створення, модифікації, збереження, передавання та видалення інформації. Встановлено, що найдоцільнішим є поділ об'єктів такої експертизи на апаратні, програмні й інформаційні, оскільки це дає змогу точніше визначати межі експертного дослідження, формулювати питання експерту й обирати оптимальний алгоритм проведення дослідження. До об'єктів експертизи можуть належати комп'ютери, ноутбуки, смартфони, сервери, жорсткі диски, флешносії, програмне забезпечення, електронне листування, хмарні сервіси, журнали подій, мережеві параметри, історія браузерів, акаунти, резервні копії та інші цифрові сліди.

На підставі аналізу нормативно-правових актів і правозастосовної практики визначено, що типовими завданнями комп'ютерно-технічної експертизи є встановлення технічного стану обладнання, виявлення ознак несанкціонованого доступу, визначення часу створення, зміни або видалення

[1] Вирок Індустріального районного суду м. Дніпра від 24 трав. 2023 р. Справа № 202/8539/23. Провадження № 1-кп/202/810/2023. URL: https://reyestr.court.gov.ua/Review/111089320

файлів, відновлення видаленої інформації, дослідження електронного листування, виявлення шкідливого програмного забезпечення, встановлення IP-адрес, геолокаційних параметрів, фактів використання певних програмних продуктів, а також способів приховування чи знищення цифрової інформації. Встановлено, що ефективність виконання таких завдань безпосередньо залежить від повноти та якості підготовки матеріалів, які направляють на дослідження.

Однією з ключових умов результативності комп'ютерно-технічної експертизи є належна організація вилучення, пакування, транспортування та зберігання цифрових носіїв інформації. Встановлено, що порушення цілісності носіїв, самостійний перегляд файлів слідчим, неналежне пакування, відсутність паролів доступу, логінів, PIN-кодів, ключів шифрування та інших відомостей про облікові записи можуть істотно ускладнювати або навіть унеможливлювати проведення експертного дослідження. Посиленої уваги потребують випадки вилучення увімкнених пристроїв, мобільних телефонів, серверів і мережевого обладнання, коли без участі спеціаліста може бути втрачена інформація про активні процеси, оперативну пам'ять, мережеві з'єднання та відкриті сеанси користувача.

Проведений аналіз емпіричного матеріалу засвідчує, що комп'ютерно-технічна експертиза є особливо ефективною під час розслідування злочинів, пов'язаних із використанням месенджерів, шкідливого програмного забезпечення, програм для обміну файлами, соціальних мереж і цифрових платформ. У справах про розповсюдження порнографічних матеріалів, шахрайство, поширення шкідливого програмного забезпечення та передачу інформації про місця дислокації ЗСУ саме результати комп'ютерно-технічних експертиз дали змогу встановити факти використання конкретних програмних засобів, зміст листування, маршрути передачі даних, наявність геолокаційних позначок, IP-адрес, історії пошуку та інших цифрових слідів, які стали ключовими доказами в кримінальному провадженні.

Сучасна практика призначення комп'ютерно-технічних експертиз супроводжується низкою проблемних аспектів, серед яких найпоширенішими є неправильне визначення виду експертизи, постановка правових або надто загальних запитань експерту, недооцінювання значення попередньої консультації зі спеціалістом, неналежна підготовка матеріалів, а також складність дослідження хмарних сервісів, VPN-технологій, криптовалютних платформ, месенджерів із наскрізним шифруванням та інших сучасних цифрових систем. У зв'язку з цим актуалізовано необхідність подальшого вдосконалення методичних рекомендацій щодо призначення комп'ютерно-технічних експертиз, розроблення спеціалізованих алгоритмів роботи із цифровими доказами й активнішого використання комплексних експертних досліджень із залученням фахівців у галузі телекомунікацій, криптографії, програмування й цифрової криміналістики.

Подяки

Немає.

Фінансування

Дослідження не фінансувалося.

Конфлікт інтересів

Немає.

References

[1] Avdieieva, H.K. (2021). Digital evidence in criminal proceedings: Problems of theory and practice. *Law and Safety,* 2(81), 175-182. Retrieved from https://ibn.idsi.md/sites/default/files/imag_file/370-374_5.pdf

[2] Demydova, Ye.Ye. (2024). Digital traces of criminal offenses: Concept and features. *Scientific Bulletin of Uzhhorod National University. Series "Law",* 4(85), 71-75. DOI: 10.24144/2307-3322.2024.85.4.10

[3] Dovzhenko, O.Yu. (2019). Some issues of appointing computer and technical examination during the investigation of cybercrimes. *Uzhhorod National University Herald. Series "Law",* 55(2), 124-127. Retrieved from http://nbuv.gov.ua/UJRN/nvuzhpr_2019_55%282%29__30

[4] Hora, I.V., Kolesnyk, V.A., & Popovych, I.I. (2024). Digital forensics in the provision of crime prevention activities. *Uzhhorod National University Herald. Series "Law",* 4(85), 63-70. DOI: 10.24144/2307-3322.2024.85.4.9

[5] Kalancha, I.H., & Harkusha, A.M. (2021). Copy of electronic information as evidence in criminal proceedings: Procedural and technical aspects. *Juridical scientific and electronic journal,* 8, 336-339. DOI: 10.32782/2524-0374/2021-8/77

[6] Karpets, Yu.V. (2025). Digital evidence and computer-technical examinations in criminal proceedings on war crimes. *Juridical scientific and electronic journal,* 11, 226-230. DOI: 10.32782/2524-0374/2025-11/46

[7] Kharkivskyi, P.P. (2014). Computer-technical examination: Problematic issues. *Criminalistics Bulletin,* 2, 97-100. Retrieved from https://elar.navs.edu.ua/server/api/core/bitstreams/32a5f766-8e02-4ac6-86fd-bc54bd67ea12/content

[8] Liubavina, V. P., & Skliarenko, H.V. (2023). Conducting computer and technical examination during the investigation of cybercrimes. *International Law Herald: Actual Problems of the Present (Theory and Practice),* 17, 36-40. DOI: 10.32782/2521-1196.17.2023.36-40

[9] Pohoretskyi, M.A. (2025). Judicial control in ensuring fair and admissible evidence in the criminal procedure of Ukraine. *Analytical and Comparative Jurisprudence,* 4(3), 269-279. DOI: 10.24144/2788-6018.2025.04.3.40
[10] Pohoretskyi, M.A. (2026). Digital (electronic) evidence and the digital (electronic) form of evidence: Delimitation of concepts and its significance for criminal procedural proof. *Analytical and Comparative Jurisprudence,* 3(1). DOI: 10.24144/2788-6018.2026.01.3.18
[11] Serhieieva, D.B. (2025). Use of special knowledge in the investigation of war crimes and crimes against humanity: Procedural aspects, expert interaction, and digital criminalistics. *Analytical and Comparative Jurisprudence,* 6(3), 234-247. DOI: 10.24144/2788-6018.2025.06.3.36
[12] Shepitko, V.Yu. (Eds.). (2025). *Digital forensics and its role in the formation of evidentiary activity in wartime conditions*. Kharkiv: Pravo. Retrieved from https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=5983&download_id=2127&srsltid=AfmBOorWS8SwrY--sKGeEaaPgkOcAOZR6eQ8lyafo-CSCYbSLp8unLTE
[13] Stepaniuk, R.L., & Kolesnyk, V.H. (2023). Forensic computer and technical examination: Current state and development prospects. *Bulletin of Luhansk State University of Internal Affairs Named after E.O. Didorenko,* 2(102), 289-305. DOI: 10.33766/2524-0323.102.289-305
[14] Teplytskyi, B.B. (2018). Tasks, objects and questions of forensic computer and technical examination. *Scientific Bulletin of the National Academy of Internal Affairs,* 3, 303-315. Retrieved from http://nbuv.gov.ua/UJRN/Nvknuvs_2018_3_27
[15] Udovenko, Zh.V., & Udovenko, V.V. (2024). Appointment of computer and technical examination during the investigation of criminal offenses committed in the field of computer information. *Forensic examination during martial law: problems of theory and practice:* materials of the 1st All-Ukrainian Scientific and Practical Conference (pp. 91-96). Vinnytsia: Erhard and Partners Expert and Consulting Center.

Список використаних джерел

[1] Авдєєва Г. К. Цифрові докази у кримінальному провадженні: проблеми теорії та практики. *Право і безпека.* 2021. № 2 (81). С. 175–182. URL: https://ibn.idsi.md/sites/default/files/imag_file/370-374_5.pdf
[2] Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2024. Т. 4. № 85. С. 71–75. DOI: 10.24144/2307-3322.2024.85.4.10
[3] Довженко О. Ю. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2019. Вип. 55(2). С. 124–127. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2019_55%282%29__30
[4] Гора І. В., Колесник В. А., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2024. Т. 4. № 85. С. 63–70. DOI: 10.24144/2307-3322.2024.85.4.9
[5] Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. 2021. № 8. С. 336–339. DOI: 10.32782/2524-0374/2021-8/77.
[6] Карпець Ю. В. Цифрові докази та комп'ютерно-технічні експертизи у кримінальних провадженнях про військові злочини. *Юридичний науковий електронний журнал*. 2025. № 11. С. 226–230. DOI: 10.32782/2524-0374/2025-11/46
[7] Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник.* 2014. № 2. С. 97–100. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/32a5f766-8e02-4ac6-86fd-bc54bd67ea12/content
[8] Любавіна В. П., Скляренко Г. В. Проведення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2023. № 17. С. 36–40. DOI: 10.32782/2521-1196.17.2023.36-40
[9] Погорецький М. А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство.* 2025. № 4. Ч. 3. С. 269–279. DOI: 10.24144/2788-6018.2025.04.3.40
[10] Погорецький М. А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесуального доказування. *Аналітично-порівняльне правознавство.* 2026. Т. 3. № 1. DOI: 10.24144/2788-6018.2026.01.3.18
[11] Сергєєва Д. Б. Використання спеціальних знань у розслідуванні воєнних злочинів і злочинів проти людяності: процесуальні аспекти, експертна взаємодія та цифрова криміналістика. *Аналітично-порівняльне правознавство.* 2025. № 6. Ч. 3. С. 234–247. DOI: 10.24144/2788-6018.2025.06.3.36.

[12] Цифрова криміналістика та її роль у формуванні доказової діяльності в умовах війни : монографія / за ред. В. Ю. Шепітька. Харків : Право, 2025. 200 с. URL: https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=5983&download_id=2127&srsltid=AfmBOorWS8SwrY--sKGeEaaPgkOcAOZR6eQ8lyafo-CSCYbSLp8unLTE
[13] Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2023. Вип. 2 (102). С. 289–305. DOI: 10.33766/2524-0323.102.289-305.
[14] Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. *Науковий вісник Національної академії внутрішніх справ.* 2018. № 3. С. 303–315. URL: http://nbuv.gov.ua/UJRN/Nvknuvs_2018_3_27
[15] Удовенко Ж. В., Удовенко В. В. Призначення комп'ютерно-технічної експертизи під час розслідування кримінальних правопорушень, що вчиняються у сфері комп'ютерної інформації. *Судова експертиза в період дії воєнного стану: проблеми теорії та практики* : матеріали І Всеукр. наук.-практ. конф. (Вінниця, 29 лют. 2024 р.). Вінниця : Твори, 2024. С. 91–96. URL: https://ekmair.ukma.edu.ua/handle/123456789/33685

KARAMAN Kostiantyn
Doctor of Philosophy in Political Science, Doctoral Student of the National Scientific Center «Hon. Prof. M.S. Bokarius Forensic Science Institute»
61177, 8a Zolochivska St., Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-2965-9661

Purpose of Computer-Technical Examination during the Investigation of Crimes

Abstract. The article presents a comprehensive study of the organizational, tactical, and procedural principles underlying the purpose of computer-technical examination during the investigation of criminal offenses. It is substantiated that, given the rapid spread of digital technologies and the growing role of electronic evidence, computer-technical examination is becoming one of the most common ways to apply special knowledge in criminal proceedings. It is established that its results are used not only during the investigation of cybercrimes but also in criminal proceedings regarding fraud, financing of terrorism, crimes against the foundations of national security, distribution of pornographic materials, transmission of information about the locations of the Armed Forces of Ukraine, and other offenses where digital traces have evidentiary value. The article defines the subject, objects, and main types of computer-technical examination and characterizes its place in the system of engineering and technical forensic examinations. It is found that the most expedient approach is to divide the objects of research into hardware, software, and information. Typical tasks solved during a computer-technical examination include, in particular, assessing the technical condition of devices, examining electronic correspondence, detecting malicious software, recovering deleted information, establishing the time of creation or modification of files, IP addresses, geolocation parameters, and facts about the use of specific software products. The features of preparing materials for examination, as well as the specifics of removal, packaging, transportation, and storage of digital media, are determined. It is emphasized that improper removal of devices, independent viewing of files by the investigator, and the absence of passwords, PIN codes, encryption keys, or other information about account access can significantly reduce the effectiveness of the expert examination or make it impossible to conduct it at all. Based on the analysis of judicial practice, the most common circumstances for which computer-technical expertise is assigned are summarized, and typical errors made during its assignment are identified. The need for further improvement of methodological recommendations for working with digital evidence, for more active involvement of specialists during the seizure of digital media, and for the wider use of complex examinations involving specialists in telecommunications, programming, and digital forensics is substantiated.

Keywords: digitalization; cyberspace; special knowledge; forensic examination; assignment of examination; computer technology.