УДК 343.98
DOI https://doi.org/10.24144/2788-6018.2023.04.77

СУДОВІ ЕКСПЕРТИЗИ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ДЕЯКІ ПРОБЛЕМИ ПІДГОТОВКИ ТА ПРОВЕДЕННЯ

Курман О.В.,
кандидат юридичних наук,
доцент кафедри криміналістики
Національного юридичного університету
імені Ярослава Мудрого,
ORCID ID: https://orcid.org/0000-0002-5432-7215

Курман О.В. Судові експертизи у сфері інформаційних технологій: деякі проблеми підготовки та проведення.

Статтю присвячено проблемам підготовки та проведення судових експертиз у сфері інформаційних технологій. Зокрема, розглядаються такі види експертних досліджень, як дослідження комп'ютерної техніки і програмних продуктів, а також телекомунікаційних систем та засобів. Кримінальний кодекс України містить Розділ XVI, яким передбачено відповідальність за кримінальні правопорушення у сфері інформаційних технологій. Криміналістична методика розслідування вказаних кримінальних правопорушень передбачає призначення та проведення зазначених видів судових експертиз як де-факто обов'язкових. Також зазначені судові експертизи призначаються і при розслідуванні інших кримінальних правопорушень, під час вчинення яких використовувалися як знаряддя або засоби комп'ютери, мобільні телефони (смартфони), флеш-накопичувачі інформації (шпигунство, вбивство, ухилення від сплати податків, зборів (обов'язкових платежів), фінансування тероризму, масові заворушення тощо).

Зазначені експертизи проводяться у випадках, коли необхідно встановити фактичні дані та вчинені за допомогою електронних технічних засобів певні дії, що мають значення для кримінального провадження. Окрім можливостей вказаних експертиз, паралельно в роботі висвітлюються і деякі проблеми, пов'язані з підготовкою та проведенням експертних досліджень. Так, зазначається, що для того, щоб створити на своєму комп'ютері образ або копію досліджуваного жорсткого диска, експерт повинен мати у своєму розпорядженні носій інформації щонайменше такої самої ємності. А якщо на експертизу направлено декілька персональних комп'ютерів або серверів з дисковими масивами за технологію RAID, то вартість змінних носіїв інформації для копіювання даних може стати на заваді успішного проведення експертизи. Визначається, що особливістю експертизи є те, що у разі дослідження програмних об'єктів та неможливості роботи з їх копіями майже завжди відбуваються зміни у файлових системах та реєстрах технічних пристроїв (наприклад, під час його включення). Така ситуація вимагає отримання експертом дозволу на застосування так званих руйнівних (частково руйнівних) методів. Також у роботі розглядаються особливості підготовки матеріалів для експертного дослідження.

Ключові слова: судові експертизи, комп'ютерно-технічна експертиза, криміналістична методика розслідування, призначення експертизи, методика експертного дослідження.

Kurman O.V. Forensic examinations in the field of information technology: some problems of preparation and conduct.

The article is devoted to the problems of preparing and conducting forensic examinations in the field of information technology. In particular, the author examines such types of expert studies as the study of computer hardware and software products and telecommunication systems and facilities. The Criminal Code of Ukraine contains Chapter XVI, which provides for liability for criminal offences in the field of information technology. The forensic methodology for investigating these criminal offences provides for the appointment and conduct of these types of forensic examinations as de facto mandatory. These types of forensic examinations are also appointed in the investigation of other criminal offences in which computers, mobile phones (smartphones), flash drives were used as tools or means (espionage, murder, tax evasion, duties (mandatory payments), terrorist financing, mass riots, etc.)

These examinations are carried out in cases where it is necessary to establish factual data and certain actions committed with the help of electronic technical means that are relevant to criminal proceedings. In addition to the possibilities of these examinations, the article also highlights some problems related to the preparation and conduct of expert studies. For example, it is noted that in order to create an image or copy of the investigated hard drive on his computer, the expert must have a storage medium of at least the same capacity. And if several personal computers or servers with RAID-

based disc arrays are sent for examination, the cost of replaceable storage media for copying data may hinder the successful conduct of the examination. It is determined that the peculiarity of the examination is that in the case of the study of software objects and the impossibility of working with their copies, changes almost always occur in file systems and registers of technical devices (for example, when they are switched on). This situation requires the expert to obtain permission to use so-called destructive (partially destructive) methods. The paper also discusses the peculiarities of preparing materials for expert research.

Key words: Forensic examinations, computer-technical examination, forensic investigation methodology, appointment of examination, expert research methodology.

Постановка проблеми. Розвиток науково-технічного прогресу зумовив широке поширення стаціонарних та портативних комп'ютерів, смартфонів, планшетів в усіх галузях діяльності людини. Практично всі сучасні електронні пристрої мають постійне чи періодичне підключення до електронних комунікаційних мереж передачі та отримання інформації. В Україні всі реєстри та бази даних державних установ та органів влади та управління переведені чи переводяться на електронні носії із розміщенням інформації у локальних мережах чи з доступом до них через всесвітню мережу Інтернет. Державне управління, медицина, наука, військова сфера, правоохоронна діяльність, товарне виробництво, зв'язок тощо – все перейшло на електронний документообіг, цифрову обробку, збереження та використання інформації. Сотні мільйонів користувачів у всьому світі мають власні сайти або сторінки в соціальних мережах. У нашій країні запущено онлайн-сервіс державних послуг «Дія» і проєкти електронної державної реєстрації речових прав на нерухоме майно та їхніх обтяжень; для юридичних і фізичних осіб (підприємців і громадських формувань) – е-Бізнес; для актів цивільного стану – е-ДРАЦС; для цифрової трансформації вищої, фахової передвищої і професійної (професійно-технічної) освіти – е-Університет; для системи управління запасами лікарських засобів і медичних виробів – створення/модернізація Державного реєстру лікарських засобів і Державного реєстру медичних виробів, розвиток застосування електронних рецептів. Така зручність у збиранні, обробці та використанні інформації створює велику спокусу незаконного отримання конфіденційних відомостей про конкретну особу, об'єднання громадян, підприємства, установи, організації, їх діяльність з метою використання надалі у протиправних цілях. За цих умов виникли і набули широкого поширення дії, що створюють небезпеку та загрозу нормальній роботі електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Кримінальний кодекс України містить Розділ XVI, яким передбачено відповідальність за кримінальні правопорушення у сфері інформаційних технологій. Криміналістична методика розслідування вказаних кримінальних правопорушень передбачає призначення та проведення таких видів судових експертиз, як комп'ютерно-технічної (комп'ютерної техніки і програмних продуктів) та телекомунікаційної (телекомунікаційних систем та засобів). Також зазначені судові експертизи призначаються і при розслідуванні інших кримінальних правопорушень, під час вчинення яких використовувалися як знаряддя або засоби комп'ютери, мобільні телефони (смартфони), флеш-накопичувачі інформації (шпигунство, вбивство, ухилення від сплати податків, зборів (обов'язкових платежів), фінансування тероризму, масові заворушення тощо)

Стан опрацювання питання. Проблематиці отримання, збирання матеріалів для комп'ютерно-технічної експертизи, її призначення, проведення та оцінки результатів в криміналістичній науці приділялася досить вагома увага з боку вчених. Так, зокрема, свої наукові дослідження цим питанням присвятили такі вчені, як: Бутузов В. [1], Довженко О. [2], Коршенко В. [3], Мотлях О. [4], Пашнєв Д. [5], Теплицький Б. [6] тощо. Також деякі аспекти зазначеної проблематиці в своїх роботах розглядали Карпінська Н., Крикунов О. [7], Манжай О. [8], Харківський П. [9]. Однак, з урахуванням швидкісних змін в законодавстві, науково-технічному прогресі (створення нейромереж, розроблення нового програмного забезпечення, виробництва нових, потужних та одночасно компактних комп'ютерних засобів, мобільного устаткування, виникнення нових способів вчинення кримінальних правопорушень, питання, пов'язані з призначенням та проведенням комп'ютерно-технічної експертизи залишаються актуальними й потребують постійного дослідження та оновлення наукових знань.

Мета статті. Дослідити особливості виконання комп'ютерно-технічної експертизи (телекомунікаційних систем та засобів), визначити тактичні помилки під час призначення та виділити організаційно-технічні проблеми проведення.

Виклад основного матеріалу. Експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна) або телекомунікаційних систем та засобів призначається у випадках, коли необхідно встановити фактичні дані та вчинені за допомогою електронних технічних засобів певні дії, що мають значення для кримінального провадження. Зокрема, результати експертизи можуть бути використані для: 1) встановлення фактів використання ноутбука, комп'ютера, смартфона для зберігання та розповсюдження певних файлів,

пов'язаних з порнографією, сепаратизмом, торгівлею наркотичними засобами, зброєю, людьми тощо; 2) підтвердження факту знайомства, спілкування, взаємодії між особами за допомогою застосунків обміну повідомленнями через мережу Інтернет; 3) вилучення та відновлення історії відвідування сайтів в мережі Інтернет.

Об'єктами зазначених судових експертиз є персональні комп'ютери, сервери, периферійне обладнання (сканери, принтери, карт-рідери), мобільні телефони, планшети, будь-які комплектуючі вказаних засобів, магнітні та оптичні диски, флеш-карти, службова системна інформація, програмні продукти (операційні системи, утиліти, засоби розробки та налагодження програм, текстові та графічні редактори, системи управління базами даних, електронні таблиці, редактори презентацій). До об'єктів дослідження цієї експертизи також можуть бути пристрої, що не є комп'ютерами в класичному розумінні цього слова, наприклад, електронні касові апарати, гральні автомати, пристрої дистанційного контролю доступу та ідентифікації людини, відео реєстратори, імобілайзери, транспондери, круїз-контролери, квадрокоптери тощо.

Методика судової експертизи містить як загальні правила досліджень, притаманні всім видам експертних досліджень, так і особливі, специфічні. Під час експертної роботи важливою є фіксація апаратної конфігурації та інформації, що міститься в представленому комп'ютері, в незмінному вигляді.

Методика експертного дослідження складається з таких основних етапів: 1) зовнішній огляд і детальний опис вигляду системного блока та його апаратної конфігурації при знятій кришці; 2) візуальний огляд внутрішніх апаратних компонентів системного блоку; 3) вилучення із системного блока жорсткого диска (HDD) або твердотілого накопичувача (SSD) та його подальше дослідження на лабораторному обладнанні; 4) під'єднання системного блока досліджуваного комп'ютера до додаткових пристроїв – монітору, клавіатури, «миші», підключення до живлення і його подальше дослідження (без HDD або SSD) і переривання його завантаження для визначення установок програми SETUP BIOS; 5) визначення системної дати та часу, інших конфігураційних установок у програмі SETUP BIOS. Перегляд установок системного блока за допомогою програми SETUP виявляє встановлення головних позицій і параметрів пристроїв на материнській платі, результати детектування – автоматичного пошуку та визначення стану контролерів HDD або SSD, наявність парольного захисту тощо; 6) завантаження операційної системи із системної флешки (диска) експерта та діагностування відповідними програмними засобами апаратних компонентів системного блока (без HDD або SSD); 7) приведення досліджуваного системного блоку до первинного вигляду (підключення HDD або SSD, закриття кожуха тощо).

Для досліджень вилученого HDD або SSD зазвичай використовується стендовий комп'ютер з ОС, аналогічною встановленій на системному блоці, що досліджується. Дослідження додаткового диску відбувається за допомогою програмних інструментальних засобів, попередньо інстальованих на лабораторному комп'ютері. Використання конкретних методів експертного дослідження залежить від завдань, що були поставлені перед експертом. Обов'язковою умовою є забезпечення незмінності первинних даних на досліджуваному HDD або SSD. Це реалізується за допомогою виготовлення точної копії даних, що зберігається на носіях даних, наприклад, шляхом створення копії жорсткого диску

Недоліком такого методу (копіювання інформації на інший носій) є фінансова складова, а саме вартість змінних носіїв. Для того, щоб створити на своєму комп'ютері образ або копію досліджуваного жорсткого диска, експерт повинен мати у своєму розпорядженні носій інформації щонайменше такої самої ємності. А якщо на експертизу направлено декілька персональних комп'ютерів або серверів з дисковими масивами за технологію RAID, то вартість змінних носіїв інформації для копіювання даних може стати на заваді успішного проведення експертизи. В такій ситуації вирішенням проблеми є робота безпосередньо з жорстким диском досліджуваного комп'ютера.

У разі неможливості отримання резервної копії накопичувача вживаються заходи для забезпечення збереження досліджуваної інформації, наприклад, шляхом використання відповідних програмних блокіраторів запису. Результатом такого прийому може бути утворення, виникнення великої кількості файлів, створених після дати вилучення комп'ютера, що в майбутньому, у разі проведення повторної експертизи, може створити слідчому певні проблеми процесуального характеру.

Виявлення ознак виконання несанкціонованих дій або використання спеціальних програм віддаленого несанкціонованого адміністрування здійснюється шляхом: 1) пошуку програм, призначених для підбору паролів, і результатів їх роботи (файлів результатів і файлів налаштувань програм); 2) пошуку фактів роботи з використанням чужих облікових записів або інших системних ресурсів; 3) встановлення вмісту рукописних і друкованих матеріалів, текстових файлів і файлів електронної пошти; 4) пошуку програм із деструктивними (шкідливими) функціями та їхнього експериментального дослідження на стендах, що моделюють передбачувані умови їхнього функціонування; 5) виявлення текстових файлів, що містять ключові слова; 6) виявлення файлів

користувачів (звукових, графічних, текстових, виконуваних модулів), що мають відношення до заданої тематики (обставин справи); 7) з'ясування діагностичних параметрів налаштування програм (реєстраційні ім'я користувача та назва організації в програмах підготовки документів Microsoft Office або системах програмування); 8) дослідження захищених паролями файлів; визначення особливостей підготовки текстового файлу з урахуванням середовища підготовки, реєстраційних параметрів текстового редактора, який використовували, часу створення документа, часу редагування та кількості редакцій; 9) виявлення і визначення призначення програм з мінімальним користувацьким інтерфейсом, які не містять пояснювальних вказівок і коментарів; 10) вивчення протоколів роботи користувача (або програм) та інтерпретації їхніх дій тощо.

Відповідно до ч. 5 ст. 69 КПК України експерт зобов'язаний забезпечити збереження об'єкта експертизи. Якщо специфіка дослідження передбачає повне або часткове знищення об'єкта експертизи або зміну його властивостей, експерт повинен одержати на це дозвіл від суб'єкта, який призначив експертизу. Особливістю комп'ютерно-технічної експертизи є те, що у разі дослідження програмних об'єктів та неможливості роботи з їх копіями майже завжди відбуваються зміни у файлових системах та реєстрах технічних пристроїв (наприклад, під час його включення). Така ситуація вимагає отримання експертом дозволу на застосування так званих руйнівних (частково руйнівних) методів.

Використання тільки неруйнівних методів (за відсутності необхідних апаратно-програмних засобів) може призвести до затягування термінів виконання СКТЕ і мати негативні наслідки для розслідування, а також для судового розгляду кримінальних проваджень [10, с. 298]

Закон України «Про судову експертизу» визначає у ст. 3 принципи судово-експертної діяльності, серед яких принцип законності посідає перше місце, що в контексті методики проведення комп'ютерно-технічної експертизи (телекомунікаційних систем та засобів) означає заборону та неприпустимість використання експертами контрафактного програмного забезпечення і застосування тільки ліцензійного програмного продукту або спеціальних програм власного розроблення, зареєстрованих у встановлений законом спосіб.

У відповідності до загальних правил призначення судових експертиз на вирішення експертів не повинні ставитися питання правового характеру. У контексті комп'ютерно-технічної експертизи (телекомунікаційних систем та засобів) таким правовим питанням визначається, наприклад, наступне – «чи використовується на комп'ютері контрафактне (неліцензоване) програмне забезпечення?» Експерт може лише визначити характеристики програмних, апаратних та інформаційних продуктів, представлених на експертизу в якості об'єкта дослідження, і вказати на ознаки, які вказують на контрафактність. Сам же факт контрафактності програмного забезпечення встановлюється під час досудового розслідування слідчим та остаточно визначається судом. Також некоректним буде питання «який розмір завданої матеріальної шкоди від використання конкретного програмного забезпечення» або «яка загальна вартість програмного забезпечення, встановленого на комп'ютері», адже визначення розміру шкоди чи вартості чогось – це прерогативний предмет дослідження інших видів судових експертиз. Вирішення питання щодо віднесення конкретної програми до шкідливих також не в компетенції експерта, адже один і той самий програмний продукт може використовуватися для незаконного таємного пошуку, моніторингу, збирання інформації на «зараженому» комп'ютері чи мобільному телефоні, так і під час комп'ютерно-технічної експертизи з метою пошуку прихованих файлів або в рамках проведення негласних слідчих (розшукових) дій, зокрема, під час зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України). Експерт у цій ситуації компетентний тільки визначити можливість виконання певних дій, вирішення конкретних завдань за допомогою програмного продукту, а також встановити реалізацію конкретних функцій у програмному коді.

Під час винесення постанови про призначення експертизи слід уникати використання жаргонізмів у формулюванні питань («вінчестер», «гаджет», «хакнуть» тощо). Під час постановки питань необхідно користуватися сталим понятійним апаратом, закріпленим в нормативно-правових актах. За відсутності таких офіційно визначених термінів необхідно застосовувати термінологію, що використовується розробниками в інструкціях до технічних засобів.

Невирішеним залишається питання спрощення пошуку окремих експертних методик проведення комп'ютерно-технічної експертизи. Експертам для дачі повного, достовірного, науково обґрунтованого висновку необхідно використовувати експертні методики, які відповідають часу. Натомість, існуючі методики швидко застарівають і вимагають доопрацювання [11, с. 5].

Висновки. Важливість комп'ютерно-технічної експертизи в сучасних умовах не викликає сумнівів, що в свою чергу потребує постійного вдосконалення існуючих методик судово-експертних досліджень. Адже швидкісні процеси в розвитку комп'ютерних, телекомунікаційних технологій вимагають «тримати руку на пульсі», що в свою чергу, покращує ефективність боротьби з кримінальними правопорушеннями, під час вчинен-

ня яких використовуються комп'ютерно-технічні засоби, телекомунікаційні пристрої та відповідне програмне забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки: наук.-практ. посіб. / В.М. Бутузов та ін. / ред. Л.П. Скалозуб, І.В. Бондаренко. Київ, 2010. 245 с.
2. Довженко О.Ю. Основи методики розслідування кіберзлочинів: автореф. дис. ... канд. юрид. наук (д-ра філософії): 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2020. 20 с.
3. Коршенко В.А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореф. дис. ... канд. юрид. наук: 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2017. 20 с.
4. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: автореф. дис. ... канд. юрид. наук: 12.00.09 / Акад. адвокатури України. Київ, 2005. 20 с.
5. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій»: автореф. дис. ... канд. юрид. наук: 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2007. 18 с.
6. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз: наук.-практ. посіб. / Б.Б. Теплицький та ін. Київ: Паливода А.В. [вид.], 2019. 167 с.
7. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис.* 2017. № 1 (9). С. 140–144.
8. Манжай О.В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського нац. ун-ту внутр. справ*. 2016. № 3 (74). С. 111–120.
9. Харківський П.П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. № 2 (22). С. 97–100.
10. Стецик Б.В, Марко С.І. Методика проведення судової комп'ютерно-технічної експертизи*. Юридичний науковий електронний журнал*. 2022. № 1. С. 296–299.
11. Климчук М.П., Коміссарчук Ю.А., Марко С.І., Стецик Б.В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні: навч. посіб. Львів: Львівський держ. ун-т внутрішніх справ, 2022. 112 с.