Юридичні науки

УДК 343.983.25

Колесник Віталій Геннадійович
завідувач відділу комп'ютерно-технічних
та телекомунікаційних досліджень
Харківський науково-дослідний
експертно-криміналістичний центр МВС України
Колесник Виталий Геннадьевич
заведующий отделом компьютерно-технических
и телекоммуникационных исследований
Харьковский научно-исследовательский
экспертно-криминалистический центр МВД Украины
Kolesnyk Vitalii
Head of the Department of Computer and Telecommunication Forensics
Kharkiv Scientific Research Forensic Center of the
Ministry of Internal Affairs of Ukraine

АКТУАЛЬНІ ПРОБЛЕМИ ПРИЗНАЧЕННЯ ТА ПРОВЕДЕННЯ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ
АКТУАЛЬНЫЕ ПРОБЛЕМЫ НАЗНАЧЕНИЯ И ПРОВЕДЕНИЯ СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ
ACTUAL PROBLEMS OF APPOINTMENT AND PRODUCTION OF FORENSIC COMPUTER-TECHNICAL EXPERTISE

Анотація. *У статті розглянуто актуальні проблемні питання що виникають в процесі призначення та проведення судової комп'ютерно-технічної експертизи, розкрито проблеми чинного процесуального законодавства та окреслено деякі організаційні та технічні проблеми, що виникають при проведенні експертизи.*

Ключові слова: *комп'ютерно-технічна експертиза, кримінальне процесуальне законодавство, призначення експертизи, поставлення запитань експерту, складність отримання доступу до даних.*

Аннотация. *В статье рассмотрены актуальные проблемные вопросы, возникающие в процессе назначения и проведения судебной компьютерно-технической экспертизы, раскрыты проблемы действующего процессуального законодательства и очерчены некоторые организационные и технические проблемы, возникающие при проведении экспертизы.*

Ключевые слова: *компьютерно-техническая экспертиза, уголовное процессуальное законодательство, назначение экспертизы, постановка вопросов эксперту, усложнение получения доступа к информации.*

Summary. *The article examines topical problematic issues that arise in the process of appointing and conducting forensic computer-technical expertise, discloses the problems of the current criminal procedural legislation and outlines some of the organizational and technical problems that arise during the examination.*

Key words: *computer forensics, criminal procedural legislation, appointment of an examination, posing questions to an expert, increasing the difficulty with accessing to data.*

Постановка проблеми в загальному вигляді. На сьогоднішній день існує ряд процесуальних, організаційних, технічних та методичних проблем, що виникають в процесі призначення та проведення судової комп'ютерно-технічної експертизи. Зазначені невирішені проблеми потребують висвітлення та детального обговорення серед науковців та фахівців.

Стан дослідження наукової проблеми. Наукові роботи поняттю судових експертиз та порядку їх призначення, присвятили такі вчені, як М.В. Салтевський, О.Р. Шляхов, А.І. Вінберг, Н.Т., Грановський, М.О. Селіванов. Безпосередньо проблемні питання проведення комп'ютерно-технічної експертизи досліджували такі вчені, як О.Р. Росинська, А.І. Усов, В.Б. Вєхов, Б.К. Давлєтов, Д.В. Пашнєв та інші вчені.

Виклад основного матеріалу. Світовий технічний прогрес та діджиталізація [1, с. 182–189] неодмінно пов'язані з активним розвитком інформаційних технологій, комп'ютерів, комп'ютерних мереж, мобільних пристроїв та призводить до постійного вдосконалення комп'ютерної техніки та програмного забезпечення.

Сучасна людина вже не може ефективно навчатись, працювати, користуватись послугами та навіть комунікувати без використання комп'ютерної техніки та електронних пристроїв. Онлайн-банкінг, замовлення товарів та послуг, відправлення фінансової звітності, листування електронною поштою, онлайн-конференції та освітні програми, листування та обмін файлами у месенджерах, зберігання та обмін даними у хмарних середовищах – це далеко не повний перелік переваг, що надає світу діджиталізація [2]. Державні установи та приватні установи бізнесу, організації та підприємства вдосконалюють та організовують ефективний обмін інформацією за допомогою персональних комп'ютерів, комп'ютерних мереж та баз даних. Світова пандемія та викликані нею зміни у суспільстві, необхідність у ізоляції, віддаленій роботі з дому та, віддаленому керуванню процесами тільки підкреслили важливість розвитку цифрових послуг.

У зв'язку з цим особливої актуальності у кримінальних та цивільних справах набуває проведення судових комп'ютерно-технічних експертиз. Зазначений вид експертизи є важливим ланцюгом у доказовій базі та дозволяє комплексно побудувати цілісну систему доказів, оскільки значна

кількість доказової інформації на сьогоднішній день перебуває в електронному (цифровому) вигляді та розміщується на електронних пристроях, якими користується людина в робочій, навчальній, розважальній та інших сферах повсякденного життя.

Кількість електронних пристроїв та носіїв, що надходять на комп'ютерно-технічну експертизу збільшується з кожним роком, що свідчить про підвищення уваги до доказів, що можуть зберігатися у електронній формі. Виявлення, збирання та фіксація таких доказів безпосередньо пов'язане зі потребою у застосуванні спеціальних знань експерта, як стороною обвинувачення, так і стороною захисту [4, с. 141].

Аналіз сучасної слідчої практики призначення комп'ютерно-технічних експертиз свідчить про недостатню кваліфікацію слідчих, недостатнє розуміння ними меж компетенції цього виду судової експертизи [3, с.89], та в цілому про відсутність досвіду у формуванні запитань, які слід ставити на вирішення комп'ютерно-технічної експертизи.

Оскільки однозначного та виключного переліку типових запитань, які можна поставити на вирішення комп'ютерно-технічної експертизи не існує, формувати перелік запитань що будуть ставитись експерту необхідно виходячи з кваліфікації кримінального правопорушення та обставин конкретної події. Дуже часто слідчий, що має у справі вилучені об'єкти (комп'ютерну-техніку, носії, мобільні пристрої) не може точно сформулювати експертне завдання:

– оскільки йому невідомі межі компетенції цього виду судової експертизи;

– оскільки він не може сформулювати запитання у зв'язку з недостатністю понятійної та термінологічної бази;

– оскільки він недостатньо розуміє, яка саме інформація міститься на електронному носії, чи може ця інформація мати доказове значення та

яким чином поставленим запитанням відокремити необхідну інформацію від зайвої, при цьому не упустивши нічого важливого.

Аналіз матеріалів призначених судових експертиз свідчить про те, що дуже часто у постанові про призначення експертизи відбувається штучне розширення обсягу експертного завдання, яке відбувається внаслідок поставлення загальних, нечітких, неконкретизованих запитань або запитань, результат вирішення яких охоплює значно ширший обсяг вихідних даних та відомостей, ніж це необхідно для доказування факту події чи обставин кримінального правопорушення. Таке розширення обсягу експертного завдання негативно впливає на строки проведення судової експертизи, оскільки змішує експерта витрачати час та ресурси на вирішення всіх поставлених запитань у повному обсязі, що призводить до збільшення строку виконання та утворення «черги» з невиконаних експертиз.

Зважаючи на вищенаведене, до типових правил постановки запитань під час призначення судової комп'ютерно-технічної експертизи слід віднести такі:

1) питання не мають носити правовий характер та «перекладати» доказування на судового експерта (наприклад, судовий експерт не може вирішувати запитання та вирішувати, чи містить виявлена інформація відомості про кримінальне правопорушення, або чи відноситься вона до тих чи інших його обставин);

2) питання мають бути чіткі, конкретизовані та передбачати можливість надання судовим експертом однозначної відповіді;

3) питання мають бути визначені виключно в межах експертної спеціальності та компетенції судового експерта;

4) перелік поставлених на вирішення експерта питань має бути збалансований (зокрема, з одного боку, він має бути повним, а з іншого до нього не слід включати зайві запитання, або такі запитання що будуть

потребувати виявлення та дослідження значного більшого обсягу інформації, ніж це необхідно для отримання доказів). Наприклад, при поставленні запитань щодо пошуку, вилучення та збереження листування користувача у програмах обміну повідомленнями (месенджерах) доцільно визначати у запитанні конкретних абонентів або конкретні назви чатів, які необхідно дослідити, замість поставлення запитання щодо повного копіювання всієї інформації з усіх месенджерів;

5) питання повинні бути поставлені таким чином, щоб при вирішенні конкретних завдань розслідування фінансові, технічні, часові та інші витрати на проведення дослідження були мінімальними (наприклад, замість конкретного невеликого інтервалу відео з носія відеореєстратора, що безпосередній запис події, експерту ставиться завдання у копіюванні всього обсягу відео, що у ньому збережене);

6) питання не повинні мати довідковий характер (наприклад «чи є мобільний телефон інформаційною системою?»);

7) при постановці питань слід використовувати усталений понятійний апарат (термінологію), визначений законами України, державними стандартами та іншими нормативно-правовими актами, та виключати жаргонні, напівпрофесійні терміни або розмовні слова, як «вінчестер», «логи», «флешка» тощо.

Дотримання зазначених типових правил виключить некоректну постановку питань експерту, мінімізує труднощі при підготовці та призначенні комп'ютерно-технічної експертизи, позитивно вплине на повноту, об'єктивність експертного дослідження та оперативність його проведення. Вкрай 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.

Наступна проблема, що суттєвим чином впливає на проведення комп'ютерно-технічних експертиз, пов'язана з обмеженням доступу всіх судових експертів до експертних методик та відсутністю єдиного порядку їх використання експертними установами різних міністерств. Офіційного обміну методиками та спільних заходів різних міністерств щодо їх узгодження та прийняття на практиці фактично не відбувається, що призводить до того, що судовими експертами однієї експертної спеціальності використовуються різні методики або взагалі не використовується методичний матеріал окремих методик у зв'язку з їх недоступністю. Означена проблема неодноразово висвітлювалася як науковцями так і практиками. На сучасному етапі діджиталізації суспільства найбільш доцільним вбачається відповідне нормативне врегулювання та створення на базі вже існуючого Реєстру методик проведення судових експертиз Міністерства Юстиції України єдиної захищеної електронної бази даних експертних методик для кожного атестованого судового експерта по ключу його електронного цифрового підпису, із розмежованим доступом до методик своєї експертної спеціальності (спеціальностей).

Постійний розвиток систем апаратного та програмного захисту інформації та збільшення розміру даних є одними із основних технічних проблем при проведенні судової комп'ютерно-технічної експертизи. Наявність засобів повнодискового шифрування, 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.

Окрім того, протягом останніх років значно зросла якість засобів шифрування та забезпечення безпеки сучасних мобільних пристроїв. З кожним роком можливості комп'ютерно-технічної експертизи у подоланні

(навіть з використанням сучасних програмних та апаратних засобів) систем логічного захисту зменшуються, звужується вікно можливостей повного та якісного вилучення інформації. Таким чином, все частіше проведення експертизи стає неможливим у зв'язку з технічною неможливістю, за відсутності пароля, отримати доступ до інформації, що розташована на електронному носії (у пам'яті) об'єкта дослідження.

У зв'язку з розвитком технологій 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 якого об'єкт має бути фізично наданий експерту на матеріальному носії. Таким чином, значна частина даних (файли вкладення електронної пошти, файли збережені на Google Drive, Google Docs, One Drive, Dropbox і т.ін.) якими користувався власник пристрою, але які не були фізично збережені на електронному носії та перебувають у віддалених сховищах, лишаються недоступними для експерта. Спостерігаючи за розвитком властивостей та опцій експертного програмного забезпечення для вилучення даних, 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. Все вищезазначене дозволяє дійти до висновку, що законодавство багатьох держав вже адаптоване та дозволяє здійснення таких експертних досліджень [7, с. 641]. Нажаль, сучасне українське законодавство та науковці у своїх дослідженнях визначають об'єктами дослідження виключно матеріальні та матеріалізовані носії інформації, що досліджуються експертом засобами спеціальних наукових знань в межах предмета експертного дослідження. Тобто, вилучення віддалених даних наразі можливе лише шляхом слідчого огляду, оскільки в судовій експертизі

неможлива практика проведення дослідження інформації, яка фізично не перебуває на матеріальному об'єкті, який ініціатор надає експерту.

Зі збільшенням у складі досліджуваних комп'ютерних пристроїв замість класичних жорстких дисків (HDD), кількості твердотілих накопичувачів (SSD), з підтримкою функції затирання TRIM [6, с. 51], значно зменшується ефективність та результативність відновлення видаленої інформації. Окрім того, у зв'язку з технічними особливостями роботи контролерів твердотільних накопичувачів SSD та виконання ними некерованих операцій з внутрішнього переміщення видалених даних у комірках флеш-пам'яті (Garbage Collection) [6, с. 54], при повторному підрахуванні контрольна сума інформації на носії може відрізнятися, що є викликом «класичному» затвердженому у експертних методиках підходу у комп'ютерно-технічній експертизі, згідно якого саме контрольна сума інформації на носії є головним засобом для підтвердження її незмінності та неспростовності. У зв'язку з вищенаведеним, є доцільним здійснювати підрахування не єдиної контрольної суми всього носія, а підрахування контрольної суми кожного файлу під час створення експертного файлу-образу або створення вибіркового файлу-образу з окремих файлів та каталогів [8].

Підсумовуючи наведені вище проблеми призначення експертизи, слід зазначити, що головним чинником що визначає результативність комп'ютерно-технічної експертизи наразі є якість зібраного та вилученого матеріалу (речових доказів), оскільки тепер, крім вилучення безпосередньо електронних носіїв в ініціатора дослідження є необхідність фіксації волатильних даних [8] та отримання процесуальним шляхом паролів від систем логічного захисту. Без зазначених додаткових даних, проведення судової експертизи захищеного належним чином об'єкта буде неможливим.

Висновки. Постійний та стрімкий розвиток комп'ютерних технологій вимагає від комп'ютерно-технічної експертизи адекватного та відповідного

розвитку, що викликає ряд проблем, а саме: відповідної адаптації законодавчої бази, оновлення експертних методик, методів та засобів, необхідність розробки єдиного підходу у використанні експертних методик. Дуже важливою є підтримання постійного розвитку та підвищення професійного рівня як самих судових експертів, так і оновлення освітніх програм підвищення кваліфікації для органів досудового розслідування. Значну роль для успішного проведення експертизи відіграє якість зібраного первинного матеріалу (речових доказів) та додаткових даних, необхідних для подолання систем логічного захисту захищених пристроїв.

Література:

1. Устенко М.О., Руських А.О. Діджиталізація: основа конкурентоспроможності підприємства в реаліях цифрової економіки. Вісник економіки транспорту і промисловості. 2019. № 68. С. 182–189.
2. Кібенко О.Р. Діджиталізація як нова ера розвитку корпоративного права. // Судебно-юридическая газета: сайт: 16.07.2019. URL: https://sud.ua/ru/news/blog/145948-didzhitalizatsiya-yak-nova-era-rozvitku-korporativnogo-prava (дата звернення: 01.12.2021).
3. Россинская Е.Р. Судебная компьютерно-техническая экспертиза: монография / Е.Р. Россинская, А.И. Усов. М. : Юристъ, 2005. 625 с.
4. 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 [Текст] : наук.-практ. посіб. / [Б. Б. Теплицький та ін.]. Київ : Паливода А. В. [вид.], 2019. 167 с. ISBN 978-966-437-550-1.
5. Карпінська Н., Крикунов О.. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві.

Історико-правовий часопис: науковий журнал. Луцьк, 2017. №1 (9). С. 140-143.

6. Nimmala, Rusvika Reddy Forensic Research on Solid State Drives using Trim Analysis. 2020. Culminating Projects in Information Assurance. 106. URL: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1141&context=msia_etds (дата звернення: 11.12.2021).
7. 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). Online ISSN : 2395-602X, March-April 2021. Volume 8 Issue 2. P. 639-646. doi: https://doi.org/10.32628/IJSRST2182118. URL: https://ijsrst.com/paper/7979.pdf (дата звернення: 11.12.2021).
8. Колесник В.Г. Особливості збирання та фіксації інформації з цифрових носіїв під час першочергових слідчих дій // Міжнародний науковий журнал "Інтернаука". 2019. №17. URL: https://www.inter-nauka.com/uploads/public/15761565182208.pdf (дата звернення: 11.12.2021).