УДК 343.9
DOI https://doi.org/10.32782/2521-1196.17.2023.36-40

В. П. Любавіна,
кандидат юридичних наук,
доцент кафедри кримінальної юстиції,
Державний податковий університет
e-mail: viktoriya.liubavina@gmail.com
ORCID ID: 0000-0003-4715-1749

Г. В. Скляренко,
здобувач другого (магістерського) рівня вищої освіти,
Державний податковий університет
e-mail: sklayrenko07angel@ukr.net
ORCID ID: 0009-0009-5389-7855

ПРОВЕДЕННЯ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Стаття присвячена особливостям проведення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. Зазначено, що даний вид кримінальних правопорушень не залишає видимої слідової картини на місці вчинення, є складними в контексті виявлення та розкриття, що зумовлено як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним (у традиційному криміналістичному значенні) місцем учинення злочину – кібернетичним простором. Крім того, встановлено, що об'єкти експертизи можна поділити на апаратні (персональні комп'ютери у будь-яких варіантах виконання; периферійні пристрої до персональних комп'ютерів; мережеві апаратні засоби; інтегровані системи; будь-які комплектуючі цих компонентів), програмні (системне програмне забезпечення; прикладне програмне забезпечення) та інформаційні (текстові й графічні файли, створені з використанням комп'ютерів або мобільних пристроїв; аудіовізуальні (мультимедійні) дані; інформація у форматах баз даних та іншого прикладного програмного забезпечення).

Ключові слова: *комп'ютерно-технічна експертиза, кіберзлочин, досудове розслідування, кримінальне провадження.*

Постановка проблеми та її актуальність. Активне використання кіберпростору для вчинення протиправних та злочинних дій призводить до необхідності і правоохоронним органам йти у ногу з часом та пристосовувати і вдосконалювати свою знання, вміння та навички. Однак, як відомо, жоден слідчий під час досудового розслідування будь-якого виду кримінальних правопорушень не може обійтися без залучення спеціалістів та експертів. На сьогодні особливо важливою судова експертиза стає для розслідування кіберзлочинів, які вчиняються за допомогою можливостей комп'ютерної техніки та мереж, оскільки під час їхнього розслідування слідчий не може обійтися без спеціальних знань та навичок.

Аналіз останніх досліджень і публікацій. Питання призначення та проведення комп'ютерно-технічної експертизи, в тому числі й під час розслідування кіберзлочинів, досліджувало багато вчених, серед яких: А.А. Вознюк, О.Ю. Довженко, М.А. Погорецький, О.В. Рибальський, О.В. Сабадаш, Б.Б. Теплицький, П.П. Харківський та інші.

Метою статті є дослідження питань, пов'язаних з проведенням комп'ютерно-технічної експертизи під час розслідування кіберзлочинів.

Виклад основного матеріалу дослідження. На жаль, досліджуваний вид кримінальних правопорушень не залишає видимої слідової картини на місці вчинення, є складними в контексті виявлення та розкриття, що зумовлено як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним (у традиційному криміналістичному значенні) місцем учинення злочину – кібернетичним простором. Зазначений простір становить «штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене внаслідок функціонування кібернетичних комп'ютерних систем управління та обробки інформації, забезпечує доступ користувачів до обчислювальних та інформаційних ресурсів систем, вироблення електронних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи» [1, с. 87–88].

Однак ані слідчий, ані прокурор чи суддя не володіють достатніми знаннями, а отже, необхідно обов'язково призначати та проводити відповідні експертні дослідження.

Відповідно до ч. 1 ст. 242 Кримінального процесуального кодексу (далі – КПК) України експертною установою, експертом або експертами, яких залучають сторони кримінального провадження або слідчий суддя за клопотанням сторони захисту у випадках та порядку, передбачених ст. 244 КПК України, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання [2].

При цьому найчастіше під час розслідування кіберзлочинів призначається саме комп'ютерно-технічна експертиза, спрямована на отримання віртуальної інформації з огляду на специфіку об'єкта й предмета її дослідження.

Як зазначає О.Ю Довженко, судова комп'ютерно-технічна експертиза під час розслідування кіберзлочинів часто призначається на початковому етапі розслідування, коли вже проведені огляд місця події та обшук, однак інформації для подальшого розслідування недостатньо. Слідчий ухвалює рішення про необхідність призначення судової комп'ютерно-технічної експертизи об'єктів, знайдених та (або) вилучених під час виконання зазначених слідчих дій. Після прийняття рішення про здійснення такої експертизи слідчий стикається з проблемою визначення її різновиду. Однак саме вказання слідчим того чи іншого різновиду комп'ютерної експертизи може привести до зайвого ускладнення призначення експертизи або складнощів під час проведення експертизи чи відповіді на поставлені питання [3, с. 125].

Крім того, деякі науковці вважають, що відповідно до своїх завдань і специфіки дослідження можна виокремити такі види експертиз:

1) апаратно-комп'ютерна експертиза, предметом якої є фактичні дані, що встановлюються при дослідженні технічних (апаратних) засобів комп'ютерної системи;

2) програмно-комп'ютерна експертиза, предметом якої є закономірності створення і використання програмного забезпечення комп'ютерної системи, представленої на дослідження;

3) інформаційно-комп'ютерна експертиза як основний різновид комп'ютерно-технічної експертизи, в предмет якої входить встановлення фактичних даних у ході «пошуку, виявлення, аналізу та оцінки інформації, підготовленої користувачем або породженої програмами для організації інформаційних процесів у комп'ютерній системі»;

4) комп'ютерно-мережева експертиза, предмет якої охоплює дослідження фактів та обставин, пов'язаних з використанням мережевих і телекомунікаційних технологій, за завданням слідчого (суду) для встановлення істини у справі;

5) телекомунікативна експертиза, «предметом якої є фактичні дані, що встановлюються на основі застосування спеціальних знань при дослідженні засобів телекомунікацій та зв'язку як матеріальних носіїв інформації про факт або подію будь-якої кримінальної або цивільної справи» [4, с. 86].

Відповідно до підпункту 1.2.2 Інструкції про призначення та проведення судових експертиз видом експертизи є інженерно-технічна, а підвидом – комп'ютерно-технічна [5], тобто під час призначення експертизи експерту може вказуватись лише інженерно-технічна експертиза (вид) та комп'ютерно-технічна (підвид).

Таким чином, у повноваженнях слідчого є лише визначення виду, а конкретний характер експертизи, як й експерт, якому вона буде доручена, визначається керівником експертної установи. Через керівника відбувається також взаємодія слідчого з експертом. Отже, слідчий має приділити увагу встановленню такої комунікації задля гарантування якості та відповідності експертизи поставленим запитанням. Зокрема, слід переконатися в тому, що поставлене завдання може бути розв'язане експертом в рамках призначеної експертизи, експерт забезпечений всім обсягом матеріалів, доказів та об'єктів дослідження, що необхідні йому для повного та всебічного дослідження й відповіді на поставлені запитання [3, с. 125].

На думку Б.Б. Теплицького, «основними завданнями комп'ютерно-технічної експертизи варто вважати лише такі: 1) діагностування апаратних засобів комп'ютерної системи; 2) визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану представленого програмного системного й прикладного забезпечення; 3) пошук, виявлення, аналіз та оцінка кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі» [6, с. 306].

Крім того, вкрай важливим є коректне складення переліку питань, поставлених на вирішення експерта, що проводить комп'ютерно-технічну експертизу. Це може породжувати певні складнощі в слідчого. Зокрема, за використання методичних посібників для постановлення питань чи затверджених наказом Міністерства юстиції методичних рекомендацій нерідко слідчому важко визначити, які саме зі вказаних питань слід поставити на розгляд експерта. Нестача знань й неповне розуміння слідчим сутності проблеми, що підлягає дослідженню, може приводити до винесення на розгляд експерта питань, що не стосуються злочину безпосередньо. Зрештою, це приводить до затягування розслідування та зниження його ефективності [7, с. 98].

Крім того, на нашу думку, не варто ставити перед судовим експертом ті запитання, на які він не зможе дати відповідь взагалі, з точки зору сучасного стану судово-експертної діяльності та розвитку криміналістичної науки в цілому. Саме розроблення універсального переліку питань, які можуть бути поставлені перед комп'ютерно-технічною експертизою, навряд чи можливе. Оскільки кожен з кіберзлочинів має свої особливості та вимагає спеціального підходу, а характер кримінальних правопорушень постійно змінюється.

Так, Б.Б. Теплицький, серед іншого, сформулював основні вимоги до питань, які ставлять для проведення комп'ютерно-технічної експертизи, серед яких виділив такі:

1. Під час постановки питань необхідно використовувати усталений понятійний апарат, уникаючи жаргонізмів та напівпрофесійних термінів (наприклад, «вінчестер», «логи» тощо). Слід уживати термінологію, визначену законами України, державними стандартами й іншими нормативно-правовими актами. Лише в разі відсутності офіційно закріплених термінів можна оперувати категоріями, які вживають безпосередньо розробники технічних засобів, програмних продуктів у супровідній документації.

2. Питання мають бути максимально чіткими та передбачати можливість надання судовим експертом однозначної відповіді.

3. Формулювання питання не повинно стосуватися етапів дослідження інформації (опис характеристик носіїв інформації та особливостей розміщення інформації на них, відновлення та дослідження інформації серед знищених файлів є обов'язковим етапом дослідження інформації).

4. Питання не повинні мати довідковий характер.

5. Питання не повинні мати правовий характер і сягати за межі компетенції судового експерта певної експертної спеціальності (спеціальних знань).

6. Питання мають відповідати наявній на сьогодні методичній і технічній базі, доступній судовому експерту.

7. Питання повинні бути спрямовані на встановлення конкретних обставин події, що належать до предмета доказування.

8. Питання повинні бути поставлені так, щоб під час виконання конкретних завдань розслідування витрати (фінансові, технічні, часові тощо) на проведення досліджень були мінімальними [6, с. 309].

Проте методичними рекомендаціями Міністерства юстиції України визначено завдання експертизи комп'ютерної техніки та орієнтовний перелік питань. До завдань віднесено встановлення робочого стану комп'ютерно-технічних засобів; встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; встановлення відповідності програмних продуктів повним версіям чи вимогам на його розроблення [5]. Слід зазначити, що орієнтовний перелік питань в методичних рекомендаціях сформульований у досить загальних термінах, а формулювання питань є відкритим. Наприклад, питання про те, чи можливим є вирішення певного завдання за допомогою певного програмного продукту, дає змогу слідчому пристосовувати інформацію, що була отримана в рамках розслідування, до визначеного питання.

На нашу думку, варто погодитись, що всі об'єкти комп'ютерно-технічної експертизи можна розділити на апаратні, програмні та інформаційні. Так, до апаратних об'єктів належать:

– персональні комп'ютери (у будь-яких варіантах виконання);

– периферійні пристрої до персональних комп'ютерів;

– мережеві апаратні засоби (сервери, робочі станції, комутатори, модеми, роутери та інше серверне обладнання);

– інтегровані системи (наприклад, мобільні телефони);

– будь-які комплектуючі всіх зазначених вище компонентів (апаратні блоки, блоки живлення, плати розширення тощо).

Програмні об'єкти:

– системне програмне забезпечення;

– прикладне програмне забезпечення.

Інформаційні об'єкти (електронні дані):

– текстові й графічні файли, створені з використанням комп'ютерів або мобільних пристроїв;

– аудіовізуальні (мультимедійні) дані;

– інформація у форматах баз даних та іншого прикладного програмного забезпечення [6, с. 307].

Крім того, на думку деяких науковців, важливим під час оформлення об'єктів для експертизи є їхнє пакування. Якщо це зовнішній носій інформації, його необхідно упакувати й опечатати по місцях відкриття упаковки. Якщо це внутрішній носій інформації, який є частиною спецтехніки, його необхідно за можливості відокремити від техніки й також підготувати до передачі експерту або передати разом з обладнанням, яке необхідно упакувати [3, с. 126].

Відібрані зразки й матеріали оформлюються згідно з процесуальними нормами. Зокрема, для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний носій, а за потреби – комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій). Для збереження даних на досліджуваних носіях вони

надаються в окремих пакуваннях. Системні блоки персональних комп'ютерів надаються в таких пакуваннях, що роблять неможливим доступ до носіїв інформації безпосередньо чи підключення системного блоку до мережі живлення. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду. Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них. Задля визначення того, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки [5].

Висновки. Отже, під час розслідування кіберзлочинів необхідно використовувати спеціальні знання й залучати відповідних фахівців в галузях комп'ютерної криміналістики, медицини, лінгвістики, психології, соціології тощо. Взаємодія із зазначеними фахівцями можлива як на стадії отримання необхідних консультацій, так і за їх безпосередньою участю в проведенні слідчих дій, під час встановлення ознак, що свідчать про мотиви злочинів та осіб, причетних до їх вчинення. Особливості розслідування кіберзлочинів пов'язані з фіксацією та виїмкою віртуальної інформації, правильною упаковкою виявленої комп'ютерної техніки та інших засобів вчинення кримінального правопорушення, а також інформаційною взаємодією з експертом та фахівцем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.

2. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 21.09.2023 року).

3. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України від 08.10.1998 року № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 21.09.2023 року).

4. Рибальський О.В., Тимошенко Л.М., Мушак А.Я. Комп'ютерно-технічна експертиза та інформаційна безпека. *Сучасна спеціальна техніка*. 2014. № 1. С. 85–89.

5. Словник термінів з кібербезпеки / за заг. ред. О.В. Копана, Є.Д. Скулиша. Київ : Аванпост-Прим, 2012. 214 с.

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

7. Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. № 2. С. 97–100.

REFERENCES

1. Dovzhenko, O.Yu. (2019). Deiaki pytannia pryznachennia kompiuterno-tekhnichnoi ekspertyzy pid chas rozsliduvannia kiberzlochyniv [Some issues of the appointment of computer and technical expertise during the investigation of cybercrimes]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*. vol. 55 (2). S. 124-127 [in Ukrainian].

2. Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code]: Zakon Ukrainy vid 13 kvitnia 2012 r. № 4651-VI. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651-17#Text (data zvernennia 21.09.2023 roku) [in Ukrainian].

3. Pro zatverdzhennia Instruktsii pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen ta Naukovo-metodychnykh rekomendatsii z pytan pidhotovky ta pryznachennia sudovykh ekspertyz ta ekspertnykh doslidzhen [On the approval of the Instructions on the appointment and conduct of forensic examinations and expert studies and Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert studies]: Nakaz Ministerstva yustytsii Ukrainy vid 08.10.1998 roku № 53/5. Retrieved from: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (data zvernennia 21.09.2023 roku) [in Ukrainian].

4. Rybalskyi, O.V., Tymoshenko, L.M., & Mushak, A.Ya. (2014). Kompiuterno-tekhnichna ekspertyza ta informatsiina bezpeka [Computer and technical expertise and information security]. *Suchasna spetsialna tekhnika*. 1. S. 85-89 [in Ukrainian].

5. *Slovnyk terminiv z kiberbezpeky [Glossary of cyber security terms].* (Kopan, O.V., & Skulysha, Ye.D. Eds.). Kyiv: Avanpost-Prym, 2012. 214 s. [in Ukrainian].

6. Teplytskyi, B.B. (2018). Zavdannia, obiekty y pytannia kompiuterno-tekhnichnoi sudovoi ekspertyzy [Tasks, objects and issues of computer-technical forensic examination]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav*. 3. S. 303-315 [in Ukrainian].

7. Kharkivskyi, P.P. (2014). Kompiuterno-tekhnichna ekspertyza: problemni pytannia [Computer and technical expertise: problematic issues]. *Kryminalistychnyi visnyk*. 2. S. 97-100 [in Ukrainian].

V. P. Liubavina, G. V. Sklyarenko. Conducting computer and technical examination during the investigation of cybercrimes

The article is devoted to the specifics of conducting a computer and technical examination during the investigation of cybercrimes. It is noted that this type of criminal offense does not leave a visible trace at the scene of the crime, is difficult in the context of detection and disclosure, which is due to both the use of remote access tools and the specific, immaterial (in the traditional forensic sense) place of the crime – cyberspace. In addition, it was established that the objects of examination can be divided into hardware (personal computers in any version; peripheral devices for personal computers; network hardware; integrated systems; any components of these components), software (system software; application software) and information (text and graphic files created using computers or mobile devices; audiovisual (multimedia) data; information in the formats of databases and other application software).

Key words: *computer and technical expertise, cybercrime, pretrial investigation, criminal proceedings.*