УДК 343.985.7:343.53:343.346
DOI https://doi.org/10.32782/ln.2021.13.31

Тимчишин А.М.
кандидат юридичних наук, доцент,
завідувач кафедри права та гуманітарних дисциплін
Івано-Франківської філії Університету «Україна»

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Сучасне інформаційне суспільство – нова історична фаза розвитку цивілізації, життя та діяльність людини в якій, насамперед, пов'язані зі створенням, переробкою і використанням інформації. Інформаційне суспільство широко використовує копм'ютери, телекомунікаційні мережі, електронні бібліотеки, банки даних, автоматизовані інформаційні системи, системи штучного інтелекту тощо, як засоби зв'язку, джерела інформації. Перехід суспільства до цієї стадії розвитку практично означає перехід від паперових інформаційних технологій до комп'ютерних. Але широке впровадження комп'ютерних технологій у життєдіяльність суспільства несе як позитивні, так і негативні наслідки.

Водночас для повноправного користування благами інформаційного суспільства Україна повинна бути готова й до негативних наслідків його розвитку – змін традиційних механізмів вчинення кримінальних правопорушень. У діяльності злочинців усе частіше спостерігається отримання, опрацювання та створення інформації, яка виконує роль предмета посягання чи інструмента злочинної діяльності в інформаційному середовищі, яке отримало назву кіберпростору.

Високий рівень технічного забезпечення вчинення кримінальних правопорушень у кіберпросторі та конспірації злочинцем такої діяльності актуалізують необхідність залучення суб'єкта спеціальних знань у процес їх розслідування.. Особливістю використання спеціальних знань під час розслідування кримінальних правопорушень, вчинених із застосуванням комп'ютерних технологій полягає у залученні експертів (фахівців) із державних експертних установ та приватних лабораторій (підприємств), що спеціалізуються у сфері розслідування комп'ютерних кримінальних правопорушень.

За результатами проведеного аналізу кримінальних проваджень розпочатих за фактом кримінальних правопорушень вчинених із застосуванням комп'ютерних технологій, спеціальні знання використовували під час: проведення експертиз, проведення документальних перевірок, отримання письмових висновків спеціалістів, участі спеціалістів у проведенні слідчих (розшукових) дій (далі – СРД).

Варто зауважити, що події реальної дійсності, що пов'язані з кримінальним правопорушенням, інколи настільки складні й різноманітні, що для їх дослідження у процесі доказування потрібно використовувати знання з багатьох галузей людської діяльності. Ці знання називаються в науці спеціальними. За сучасних умов, коли виникають нові види кримінальних правопорушень, поширюються недостатньо вивчені наукою способи їх учинення, потреба залучення фахівців до розслідування в різних формах вкрай актуальна. На сучасному етапі розвитку суспільства результати протидії злочинності безпосередньо залежать від застосування досягнень науки й техніки в практиці виявлення та розслідування кримінальних правопорушень.

Провідну роль у цьому відіграють спеціальні знання [1].

До складу спеціальних засобів, що використовуються при розслідуванні кримінальних правопорушень, вчинених із застосуванням комп'ютерних технологій, слід віднести як апаратні (технічні), так і програмні засоби, а в алгоритмі програми закладений безпосередньо метод вирішення певної задачі.

Спеціальні програмно-технічні засоби, що використовуються в ході СРД повинні вирішувати не тільки задачі зі збирання слідів кримінальних правопорушень, але й дослідницькі завдання.

Одним із етапів збирання слідів кримінальних правопорушень є їх вилучення. По відношенню до комп'ютерних слідів кримінального правопорушення їх вилучення являє собою копіювання комп'ютерної інформації на інший носій, який був раніше підібраний. Подібні копії комп'ютерних слідів, як і копії традиційних слідів (рук, ніг, взуття тощо), можна віднести до похідних речових доказів. При збиранні носіїв слідів комп'ютерного кримінального правопорушення на місці проведення СРД при неможливості вилучення оригінального носія виникає необхідність створення його повної копії. Найчастіше образ знімається з основного носія інформації комп'ютера – жорсткого диска, або вінчестера.

Враховуючи положення чинного КПК України, як вважають фахівці-науковці, можна виокремити три процесуальні форми використання спеціальних знань під час досудового розслідування:

1) залучення спеціаліста для надання письмової консультації;

2) залучення спеціаліста для надання безпосередньої технічної допомоги під час процесуальних дій;

3) залучення експерта для проведення судової експертизи й виконання обов'язків судового експерта [1].

Залучення спеціаліста для надання письмової консультації (згідно зі ст. 71 КПК України). Консультації традиційно можуть бути письмовими й усними, однак процесуальною є лише письмова форма консультації (ч. 2 ст. 105 чинного КПК України регламентує процесуальний спосіб надавання консультації спеціаліста – це письмове пояснення спеціаліста, який брав участь у проведенні відповідної процесуальної дії, що є додатком до протоколу такої дії) [10].

Залучення спеціаліста для надання безпосередньої технічної допомоги. Відповідно до ст. 71 КПК України, спеціаліст залучається під час проведення процесуальної дії для фотографування, складення схем, планів, креслень, відбору зразків для проведення експертизи тощо [10]. Специфіка цієї форми полягає в тому, що її реалізація слідчим фактично дає змогу оформити в процесуальне джерело доказів результат залучення в кримінальне провадження спеціаліста як суб'єкта спеціальних знань [2].

У документі як джерелі доказів у значенні ст. 99 КПК України спеціаліст утілює свої спеціальні знання, зокрема через:

1) створення матеріалів фотозйомки, звукозапису, відеозапису й інших носіїв інформації (стосовно досліджуваної категорії злочинів під час огляду чи обшуку спеціаліст найчастіше створює копії комп'ютерної інформації на спеціально підготовленому для цього електронному носії);

2) постановку з дозволу слідчого питань, що відображаються в протоколах слідчих (розшукових) дій (актуально з позицій психолога, педагога, лікаря, спеціаліста економічного фаху);

3) подання зауважень щодо протоколів процесуальних дій, чим акцентує увагу учасників процесу на обставинах й особливостях речей і документів, що стосуються відповідної сфери спеціальних знань [10].

Залучення спеціаліста для надання усної консультації. У процесуальному законі немає згадок про отримання усних консультацій спеціаліста під час досудового розслідування; усні консультації та роз'яснення спеціаліста законодавець регламентує лише стосовно

стадії судового розгляду (у ст. 360 КПК України) [10]. Ефективність цієї непроцесуальної форми використання спеціальних знань з метою подальшого залучення експерта для проведення судової експертизи не викликає сумніву в жодного практика. Такі усні консультації проводять здебільшого з керівниками й експертами (за погодженням із керівником) лабораторій експертних служб, зокрема: лабораторій комп'ютерно-технічних і телекомунікаційних досліджень; лабораторій досліджень у сфері інформаційних технологій; лабораторій економічних досліджень [1–3].

Сутність експертизи полягає в тому, що експерт самостійно на підставі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо досліджує надані йому об'єкти, явища й процеси з метою надання висновку з питань, що є або будуть предметом судового розгляду. Унаслідок вчинення кримінальних правопорушень у кіберпросторі утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди, що потребує проведення в таких провадженнях широкого спектру судових експертиз, а саме: експертизи комп'ютерної техніки і програмних продуктів; експертизи телекомунікаційних систем (обладнання) та засобів; технічної експертизи документів; експертизи відеозвукозапису; експертизи у сфері інтелектуальної власності; інших видів експертиз, без проведення яких неможливо отримати необхідні відомості, що свідчать про ознаки складу одного з кримінальних правопорушень злочинної сукупності [3, с. 111].

Найважливішим фактором своєчасного встановлення ознак кримінальних правопорушень, вчинених із застосуванням комп'ютерних технологій є ефективне застосування спеціальних знань при перевірці інформації про кримінальне правопорушення [3, с. 125].

Проведення перевірочних досліджень елементів комп'ютерних технологій у взаємодії зі слідчим набуває великого значення при збиранні комп'ютерних слідів. Іноді неможливо без дослідження інформації на комп'ютерному носії виявити сліди підключень з віддаленого доступу до комп'ютерної системи, під час яких було вчинено кримінальне правопорушення, на їх основі прослідити мережний маршрут між елементами комп'ютерних технологій, що були засобом та предметом кримінального правопорушення, і зібрати всі сліди цього кримінального правопорушення на всіх точках маршруту [4].

Рекомендовано розпочати пошук слідів з виявлення мережних підключень засобів комп'ютерної техніки, що знаходяться на місці події і в яких виявлені сліди кримінального правопорушення, та дослідження інформації, що пов'язана з цими підключеннями. А далі діяти наступним чином:

Ситуація 1. Якщо ЕОМ апаратно не підключена до мережі, або в інформації про мережні підключення не містяться ознаки, що вказують на віддалений доступ до неї під час вчинення кримінального правопорушення, то, скоріш за все, ця ЕОМ є і предметом злочинного посягання, і засобом вчинення кримінального правопорушення [5].

Ситуація 2. Якщо ЕОМ має підключення до мережі й в інформації про мережні підключення містяться ознаки, що вказують на віддалений доступ до неї під час вчинення кримінального правопорушення, то залежно від інформації, що міститься в записах підключень, слід визначити наступну точку пошуку слідів і діяти спочатку. У результаті пошук приведе до ЕОМ, які є кінцевими точками маршруту [6].

Всі сліди на точках маршруту фіксуються, при потребі досліджуються та вилучаються за допомогою фахівця. Загальною методичною основою перевірочних досліджень є так звані експрес-методи дослідження об'єктів, метою яких є встановлення носіїв і місць знаходження комп'ютерних слідів.

За допомогою стандартних функцій операційної системи Windows (як найбільш розповсюдженої) можна виявити необхідну інформацію.

1. Операційна система Microsoft Windows 10 зберігає в директоріях і файлах:

\Windows\History\ – всі файли історії, тобто відомості про те, які дії здійснювалися на даному комп'ютері в певний період часу;

\Windows\name.pwl – імена, телефони і паролі для з'єднання з Інтернет, всі вони легко (за допомогою спеціальних програм) розшифровуються;

\Windows\Profiles\name\ – (де name ім'я користувача) зберігає профілі і всі установки конкретних користувачів (це, до речі, справедливе і для Windows NT);

\windows\temp – тимчасові файли програм комп'ютера, відомості про інсталяції програм;

user.dat – параметри користувача;

user.da0 – резерв [7].

2. Стандартний засіб роботи в Інтернет Microsoft Internet Explorer також зберігає інформацію про свою роботу в каталогах операційної системи. В папці C:\windows\ temporary internetfiles\ зберігаються ярлики до html-файлів, які відкривалися в Інтернет-браузерах комп'ютера. Крім того, Microsoft Internet Explorer в директорії \Windows\ Cookies\ зберігає файли Cookies. Це файли, що зберігають різноманітну інформацію про користувача Інтернет. Річ у тому, що протокол HTTP, так би мовити, є одноразовим. Тобто кожного разу заходячи на сторінку в Інтернеті, користувач починає спочатку, що б він не вводив, і які зміни б не робив. Технологія Cookies допомагає створити ілюзію, що користувача «пам'ятають» на сайті. Користувачу не потрібно вводити сотню раз одну і ту ж інформацію від сесії до сесії, вона зберігається у нього на диску. До зручності використання цієї технології можна віднести ще й те, що цю інформацію користувач завжди може змінити у себе на диску «на льоту». В Cookies також можуть зберігатися інші різноманітні дані. Наприклад, кількість відвідин якоїсь сторінки, час відвідин. В теках \Favorites\ або \Обране\ – зберігаються файли закладок Інтернет (тобто посилання на сторінки, до яких користувач виявив цікавість.

3. Програма електронної пошти Microsoft Outlook Express всі листи, які користувач коли-небудь відправляв, одержував або видаляв, береже в своїй базі, як і іншу значущу інформацію. Розташована вона в директоріях:

\Windows\Aplication\Microsoft\Outlook Express\Mail\ – пошта – файли з розширеннями IDX і MBX (вхідні, відправлені, видалені, чернетки).

\Windows\Aplication\Microsoft\Outlook Express\News\ – новини – файли з розширеннями NCH [8].

3. Більшість інших програм (модемні, факсні, FTP-клієнти, браузери тощо) ведуть лог-файли (на які адреси і коли заходив користувач, які дії виконував), кеші тощо. Файли, що містять дану інформацію, можна знайти в каталогах відповідних програм в загальному каталозі \ProgramFiles\.

4. Прийоми роботи із засобами комп'ютерної техніки, що можуть використовуватися в ході проведення СРД, що дозволяють обійти простий захист комп'ютера і з'ясувати необхідну на первинному етапі розслідування інформацію про користувача, його діяльність (операційна система Windows):

4.1. У Провіднику (C:\windows\explorer.exe) є функція пошуку файлів (Клавіша F3 або меню «Пуск/Пошук/Файли та папки…»), де є можливість знайти файли за датою та часом створення чи зміни, символам або словам, що входять в назву або в текст документу.

4.2. У меню «Пуск/Документи» відображаються 15 документів, які відкривалися останніми. Також в Microsoft Word 2000/ XP/2003 у вікнах відкриття, збереження документа є пункт «Журнал», де відображаються ярлики до файлів, які відкривалися останніми.

4.3. У Інтернет-браузерах (Internet Explorer, Netscape Navigator, Opera тощо) також є папка «Журнал», в яку записуються адреси Інтернету, які відкривалися за певний період, папка «Обране», де зберігаються улюблені Інтернет-адреси користувача.

4.4. Програма для роботи з електронною поштою Outlook Express має функцію ство-

рювання контактів, де вказується деяка інформація про респондентів користувача. Також можна проглянути листи, які прийшли (папка «Вхідні»), відправлені, видалені, редагуються. Якщо електронна пошта отримується за протоколом POP3, то є можливість перегляду користувача без вводу пароля.

4.5. Щоб проглянути приховані файли, потрібно в меню провідника «Вид/Властивості» папки поставити позначку на пункті «Показувати всі файли».

4.6. Існують програми: записники, органайзери (Microsoft Outlook, Reminder, Birthday тощо), запустивши які можна знайти корисну інформацію про користувача, його розпорядок дня, зустрічі, спільників.

5. Шкідливі програми (в основному віруси) виявляються антивірусними засобами. Троянські програми та закладки іноді включають в себе механізм відключення дії або видалення вказаних засобів.

Сліди наявності таких шкідливих програм у ОС Windows можна виявити наступними способами:

5.1. Запустити «Диспетчер задач» (2000/XP) або натиснути клавіші Ctrl+Alt+Del (95-Me) і в переліку виконуваних процесів виявити програми, що не повинні виконуватись в даний час.

5.2. З метою виявлення ярликів підозрілих програм перевірити пункт меню «Автозагрузка», файли autoexec.bat, config.sys. Запустити стандартну для Windows 2000/XP/7/8/10 команду msconfig (з пункту головного меню «Виконати»), у вікні, що відкриється, перевірити перелік «Автозагрузка».

Таким чином, можна виявити місце розташування основної шкідливої програми, скопіювати її для подальшого дослідження, та видалити з метою усунення шкідливих впливів.

Виявлення ознак комп'ютерного кримінального правопорушення завершується відкриттям кримінального провадження. Як свідчить практика, обставини вчиненого такого кримінального правопорушення не можуть бути встановлені у повному обсязі без залучення до проведення СРД відповідних спеціалістів [9].

Таким чином, застосування спеціальних знань у розслідуванні кримінальних правопорушень, вчинених із застосування комп'ютерних технологій є достатньо ефективним, на чому наголосили опитані слідчі Національної поліції України (83 %). Такі знання під час розслідування кримінальних правопорушень, вчинених у кіберпросторі, використовуються у процесуальних та непроцесуальних формах. До процесуальних форм відносимо: залучення спеціаліста для надання письмової консультації; залучення спеціаліста для безпосередньої технічної допомоги під час процесуальних дій; залучення експерта для проведення судової експертизи й виконання обов'язків судового експерта. До непроцесуальних – усне консультування слідчого зі спеціалістом; залучення спеціаліста під час перевірки оперативної інформації про злочини, що вчинені або готуються. Специфіка залучення спеціаліста визначається через нормативно окреслене коло повноважень останнього та спосіб його залучення.

Надання доручення працівнику спеціальних підрозділів кіберполіції в порядку ст. 41 КПК України для проведення СРД не визнається формою залучення спеціаліста. Спеціаліст з інформаційних технологій, електроніки й телекомунікацій може залучатися для технічної допомоги, слідчий при цьому залишається основним виконавцем СРД.

Анотація

У статті зазначено, що використання спеціальних знань під час розслідування кримінальних правопорушень учинених з використанням комп'ютерних технологій складається із двох блоків, для реалізації кожного з яких виокремлено певні особливості. Зазначено, що особливістю використання спеціальних знань полягає у залученні експертів (фахівців) із державних експертних установ та приватних лабораторій (підприємств), що спеціалізуються у сфері розслі-

дування таких кримінальних правопорушень. Виокремлено призначення основних експертиз (комп'ютерно-технічних, телекомунікаційних експертиз), тобто обов'язкових експертиз, які призначаються під час розслідування таких кримінальних правопорушень для встановлення обставин кримінального провадження та факультативних (мистецтвознавчих та лінгвістичних експертиз), які обумовлені об'єктом та об'єктивною стороною кримінального правопорушення (розповсюдження порнографії, творів екстремістського, терористичного характеру).

Встановлено, що особливістю використання спеціальних знань під час розслідування кримінальних правопорушень, вчинених із застосуванням комп'ютерних технологій полягає у залученні експертів (фахівців) із державних експертних установ та приватних лабораторій (підприємств), що спеціалізуються у сфері розслідування комп'ютерних кримінальних правопорушень. Вивчення матеріалів слідчої практики дає підстави для висновку, що письмові пояснення спеціаліста є додатковим способом підтвердження джерела формування такого доказу, як документ – електронний носій інформації. В більшості проваджень пояснення надають штатні працівники кіберполіції, які є фахівцями з інформаційних технологій або електроніки й телекомунікацій, і в процесуальному статусі спеціаліста були залучені під час проведення огляду, обшуку тощо. У письмовому поясненні такий спеціаліст описує методи так званого експрес-аналізу (процес встановлення фактичних даних, що мають значення для конкретного факту правопорушення); методи вилучення (копіювання) та збереження нетрадиційних (цифрових) слідів кримінальних правопорушень.

За результатами аналізу судово-експертної практики, виокремлено типові помилки, що допускають ініціатори проведення експертиз комп'ютерної техніки та програмних продуктів, що як наслідок ускладнює, або унеможливлює її проведення.

Ключові слова: спеціальні знання; кримінальне судочинство; кримінальне провадження; кримінальні правопорушення; комп'ютерні технології.

Tymchyshyn A.M. Use of special knowledge in the investigation of criminal offenses committed with the application of computer technologies

A feature of the use of special knowledge during the investigation of criminal offenses committed with the use of computer technologies is the involvement of experts (specialists) from state expert institutions and private laboratories (enterprises) specializing in the field of investigation of computer criminal offenses.

According to the results of the analysis of criminal proceedings initiated on the basis of the fact of criminal offenses committed with the use of computer technologies, special knowledge was used during: conducting examinations, conducting documentary checks, obtaining written conclusions of specialists, participation of specialists in conducting investigative (search) actions

The study of materials of investigative practice gives grounds for the conclusion that the written explanations of a specialist are an additional way of confirming the source of the formation of such evidence as a document - an electronic information carrier. In most proceedings, full-time employees of the cyber police, who are specialists in information technologies or electronics and telecommunications, and were involved in the procedural status of a specialist during the inspection, search, etc., give explanations. In a written explanation, such a specialist describes the methods of the so-called express analysis (the process of establishing factual data relevant to a specific fact of an offense); methods of extraction (copying) and preservation of non-traditional (digital) traces of criminal offenses.

The article states that the use of special knowledge during the investigation of criminal offenses committed with the use of computer technologies consists of two blocks, for the implementation of

each of which certain features are singled out. It is noted that a feature of the use of special knowledge is the involvement of experts (specialists) from state expert institutions and private laboratories (enterprises) specializing in the investigation of such criminal offenses. The assignment of basic examinations (computer technical, telecommunications examinations), i.e. mandatory examinations, which are appointed during the investigation of such criminal offenses to establish the circumstances of criminal proceedings and optional (artistic and linguistic examinations), which are determined by the object and about objective side of the criminal offense (distribution of pornography, works of an extremist, terrorist nature).

Based on the results of the analysis of forensic expert practice, typical mistakes made by the initiators of conducting examinations of computer equipment and software products have been singled out, which, as a result, complicates or makes it impossible to carry out.

Key words: special knowledge; criminal justice; criminal proceedings; criminal offenses; Computer Technology.

Список використаних джерел:

1. Використання спеціальних знань під час розслідування несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку: метод. рек. / С. С. Охріменко, О. С. Тарасенко, О. М. Стрільців. Київ: Нац. акад. внутр. справ, 2017. 74 с.
2. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням в мережі Інтернет забороненого контенту: метод. рек. / О. С. Тарасенко, О. М. Стрільців, О. О. Волков та ін.; за заг. ред. Ю. Ю. Орлова. Київ: ГСУ, Нац. акад. внутр. справ, 2016. 78 с.
3. Ревака В. М. Форми використання спеціальних пізнань у досудовому провадженні: дис. … канд. юрид. наук . Харків, 2006. 180 с.
4. Пашнєв Д. В., Рудик М. В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом. URL: http://www.pravoznavec.com.ua/period/article/19906/ %CF
5. Захарова О. В. Особливості проведення огляду, вилученої комп'ютерної техніки під час розслідування комп'ютерних злочинів. URL: http://nbuv.gov.ua/j-pdf/Nzlubp_2011_7_53.pdf.
6. Рекомендації щодо особливостей досудового розслідування та процесуального керівництва у кримінальних провадженнях про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. URL: https://www.gp.gov.ua/userfiles/metodichka_Kiber_11_07_17.doc.
7. Пашнєв Д. В. Особливості виявлення і фіксації криміналістично значимої комп'ютерної інформації при розслідуванні злочинів. *Право і безпека*. 2003. № 1. С. 108–111.
8. Пашнєв Д. В. Особливості виявлення і фіксації криміналістично значимої комп'ютерної інформації при розслідуванні злочинів. *Право і безпека*. 2003. № 1. С. 108–111.
9. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис.* 2017. № 1 (9). С. 140–144.
10. Кримінальний процесуальний кодекс України: Закон від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text