3. Психологія допиту. URL: http://library.nlu.edu.ua/POLN_TEXT/KNIGI/1_DISKI/UR_PSIX/html/31.htm (дата звернення: 06.09.2020)
4. Журавель В. А. Ситуационность тактических приемов при допросе потерпевшего. Криминалистика и судебная экспертиза. К. : Вища шк., 1985. Вып. 30. С. 18–24.

Грига Марія Андріївна,
старший науковий співробітник наукової лабораторії з проблем протидії злочинності ННІ № 1 Національної академії внутрішніх справ, кандидат юридичних наук

АСПЕКТИ ПРОВЕДЕННЯ ЕКСПЕРТИЗ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Глобальні зміни, викликані пандемією коронавірусу торкнулися абсолютно всіх сфер життя людства на всіх континентах. Вплинули ці процеси і на характер злочинної діяльності. З одного боку, повсюдне закриття кордонів та соціальне дистанціювання швидко припинило чи значно уповільнило певні види злочинів. З іншого – зловмисники скористались нестабільною ситуацією та наживаються на стрімко зростаючому попиті на деякі товари та послуги.

Загалом у Європолі зафіксували швидке зростання рівня злочинності у зв'язку з пандемією [1]. Встановлено збільшення кількості шахрайств, крадіжок та фальшувань, а також злочинів, пов'язаних з використанням комп'ютерної техніки та інтернет-ресурсів. Кіберзлочинність швидко нарощує темпи, скориставшись тим, що багато людей обмежені у можливості вільно переміщуватися і значно більше часу проводять у Інтернеті. Такі активні дії криміналітету під час світової кризи становлять особливу загрозу для безпеки людей.

Необхідно зазначити, що у поняття «кіберзлочин» включаються різноманітні протиправні посягання, однак головною ознакою таких злочинів є використання комп'ютерної техніки, програмних продуктів, телекомунікаційних засобів та інших інформаційних технологій для реалізації злочинних цілей. При цьому такі прагнення можуть бути абсолютно різними: розкрадання коштів, якщо у злочинця є доступ до систем накопичення грошових ресурсів; збагачення – якщо злочинець реалізує шкідливе програмне забезпечення (віруси); розповсюдження інформації з обмеженим доступом; правопорушення, пов'язані з поширенням дитячої порнографії або расистських чи ксенофобних матеріалів; різні види шахрайств тощо.

На ефективність розслідування таких злочинів, як і будь-яких інших,впливає оперативність виявлення залишених злочинцями слідів та ефективне залучення спеціальних знань для їхнього дослідження. Унаслідок вчинення кіберзлочинів 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 зі злочинів злочинної сукупності (наприклад, економічних експертиз під час розслідування злочинів, пов'язаних із фінансово-економічною сферою відносин у кіберпросторі; психологічної, мистецтвознавчої експертизи або відповідної комплексної експертизи – злочинів, пов'язаних із соціальною сферою відносин суб'єктів у кіберпросторі; трасологічних експертиз – злочинів, що вчинені з антидержавно політичних або корисливих мотивів, лінгвістичної експертизи мовлення (семантико-текстуальний аналіз писемного й усного мовлення) – злочинів, що вчинені з антидержавно-політичних мотивів; судово-балістичних, судово-хімічних експертиз тощо – злочинів, що порушують встановлений порядок обігу певних речей) [2, с. 28].

Втім, типовою експертизою, яка призначається під час розслідування кіберзлочинів, є все ж експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна – КТЕ). У свою чергу у межах даного виду експертних досліджень виокремлюють такі її підвиди: апаратно-комп'ютерна, програмно-комп'ютерна, експертиза даних (інформаційно-комп'ютерна), комп'ютерно-мережева, а також часто призначається комплекс цих експертиз. Хоча деякі науковці чітко виокремлюють у межах КТЕ три самостійних експертних підвиди: експертиза комп'ютерної техніки, експертиза програмних продуктів та інформаційно-комп'ютерна експертиза [3, с. 141, 142]. Виходячи з наведеного, коло об'єктів даного виду експертизи є доволі широким: комп'ютери та їх складові, будь-які носії інформації (дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (на кшталт мобільних телефонів, різноманітних ґаджетів, банкоматів, гральних автоматів, принтери, сканери та ін.). Основні завдання та орієнтовний перелік питань, що вирішується під час проведення КТЕ визначені у п. 13 розділу ІІ Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень.

Не так давно з'явився ще один вид експертизи, що також вирішує завдання, пов'язані зі сферою інформаційних технологій. Йдеться про експертизу телекомунікаційних систем та засобів, об'єктами якої є телекомунікаційні системи, засоби,мережі і їх складові частини та інформація, що ними передається, приймається та обробляється. Під час розслідування кіберзлочинів дана експертиза призначається, якщо спосіб учинення (приховування або підготовки) злочину пов'язаний із втручанням у роботу мереж операторів зв'язку,

заміною, спотворенням, витіканням або втратою трафіку і спотворенням процесу його обробки; порушенням встановленого порядку маршрутизації трафіку. Об'єктами цієї експертизи під час розслідування кіберзлочинів часто є: Інтернет, IP вузли, веб-сторінки, приймачі радіосигналів, вузли комутації; первинні мережі зв'язку, наземні станції супутникового зв'язку, обставини (адресації в мережі Інтернет; передачі радіосигналів; використання доменних імен у мережі Інтернет тощо) [2, с. 30].

Проте потенціал даного виду експертних досліджень вкрай обмежено використовується під час розслідування кіберзлочинів через цілу низку факторів. По-перше – це дефіцит кадрів, адже проведення даного виду досліджень передбачає наявність у експерта вузької спеціалізації і володіння комплексом знань щодо інформаційних процесів у комп'ютерних мережах, мережах зв'язку та спеціалізованих телекомунікаційних пристроях. При чому така спеціалізація, зважаючи на темпи розвитку даної галузі, передбачає постійне оновлення згаданих знань, а також вимагає високого рівня матеріально-технічного забезпечення роботи такого спеціаліста, що зумовлює високу вартість даних експертиз.

По-друге, вкрай низьким залишається рівень науково-методичного підґрунтя для проведення даного виду експертиз. Так, якщо Реєстр методик судових експертиз передбачає 14 методик проведення комп'ютерно-технічної експертизи, то стосовно дослідження телекомунікаційних систем та засобів розроблено лише одну. Це знову ж таки свідчить про її новизну та недостатню дослідженість [4].

Очевидно, можна констатувати, що вказаної науково-методичної бази недостатньо для вирішення усіх можливих питань, які можуть бути поставлені перед експертом при розслідуванні кіберзлочинів. Водночас основною роботою експерта залишається виконання судових експертиз. Відповідно підготовка науково-методичних матеріалів не є пріоритетним завданням, тому кількість і якість такої методичної роботи не завжди відповідає нагальним потребам [5].

Таким чином, на тлі стрімкого збільшення кількості кіберзлочинів в умовах пандемії затребуваність у проведенні експертних досліджень, пов'язаних з вирішенням завдань у сфері інформаційних технологій значно зросла. Основними проблемами, які на сьогодні вимагають невідкладного вирішення з метою збільшення ефективності таких експертних досліджень є покращення якості підготовки та залучення кваліфікованих експертних кадрів, а також підвищення рівня методичного та матеріально-технічного забезпечення роботи експертів. Уявляється, що ефективність вирішення зазначених проблем напряму залежить від об'єднання зусиль та можливостей всіх суб'єктів використання спеціальних знань

в галузі комп'ютерно-технічної експертизи та вироблення спільної стратегії дій у кризових умовах.

Список використаних джерел

1. Європол: Під час коронавірусної кризи активізуються кіберзлочинці та шахраї. URL: https://www.dw.com/uk/європол-під-час...

2. Самойленко О.А. Виявлення та розслідування кіберзлочинів [Текст]: навч.-метод. посіб. Одеса. 2020. 112 с.

3. КарпінськаН., КрикуновО. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. Історико-правовий часопис. Р. IV. Кримінальне та кримінально-виконавче право, кримінологія, кримінальний процес і криміналістика. 2017. №1 (9). С. 140–144.

4. Шапошнікова І. Основні аспекти вибору типу і проведення експертизи у справах про кіберзлочинність. URL: https://yur-gazeta.com/publications/practice/inshe/osnovni-aspekti-viboru-tipu-i-provedennya-ekspertizi-u-spravah-pro-kiberzlochinnist.html.

5. Надіжко М.М. Деякі питання науково-методичного забезпечення судово-експертної діяльності в системі СБ України (на прикладі комп'ютерно-технічних досліджень). URL: http://www.academy.ssu.gov.ua/ua/page/page_1581425700.htm.

Гриненко Катерина Вікторівна,
ад'юнкт кафедри криміналістики та судової медицини Національної академії внутрішніх справ

ТАКТИКА ПРЕД'ЯВЛЕННЯ ОСОБИ ДЛЯ ВПІЗНАННЯ В РЕСПУБЛІЦІ ПОЛЬЩА

Як в українському, так і в польському кримінальному процесі пред'явлення для впізнання розглядається як одне з найбільш істотних процесуальних дій, що має важливе доказове значення. Пред'явлення для впізнання проводиться в процесі розслідування кримінальних правопорушень, де позитивний результат у більшості випадків являється основою підозри (обвинувачення) у кримінальному провадженні. Результатами впізнання можуть бути розпізнання, нерозпізнання або констатація того, що впізнаючий не запам'ятав об'єкт, при цьому в кожному випадку буде отримано результат процесуальної дії, що має різне та водночас важливе значення для розслідування.

Не дивлячись на те, що пред'явлення особи для впізнання вважається слідчою дією в кримінальному процесі, та таким що має суттєве, а іноді вирішальне доказове значення, його форма та тактика детально не прописані в КПК Республіки Польща, на відміну від КПК України (ст. 228).