УДК 343.98’06:004

О. В. Неня, *кандидат юридичних наук, провідний науковий співробітник Державного науково-дослідного інституту МВС України*

СУЧАСНІ ПРОБЛЕМИ КРИМІНАЛІСТИЧНИХ ДОСЛІДЖЕНЬ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ПРО КІБЕРЗЛОЧИНИ

Розглянуто особливості кіберзлочинності як суспільно-небезпечного явища, розкрито її поняття та наведено найпоширеніші її види. Окреслено та проаналізовано окремі проблемні питання криміналістичних досліджень злочинів у сфері високих технологій крізь призму розуміння поняття «матеріальний», яке застосовують до об’єктів таких досліджень.

Акцентовано увагу на необхідності розроблення сучасних комплексних криміналістичних технологій дослідження об’єктів кіберзлочинів, а також запропоновано можливі напрями розвитку таких технологій.

Ключові слова: кіберзлочинність, кіберпростір, глобалізація, матеріальний об’єкт, технології.

Рассмотрены особенности киберпреступности как общественно-опасного явления, раскрыто ее понятие и приведены самые распространенные ее виды. Определены и проанализированы отдельные проблемные вопросы криминалистических исследований преступлений в сфере высоких технологий через призму восприятия понятия «материальный», которое применяется к объектам таких исследований.

Акцентировано внимание на необходимости разработки современных комплексных криминалистических технологий исследования объектов киберпреступлений, а также предложены возможные направления развития таких технологий.

Ключевые слова: киберпреступность, киберпространство, глобализация, материальный объект, технологии.

The features of cybercrime as a socially dangerous phenomenon are considered; its concepts and most widespread types are revealed. Several specific issues of forensic crime investigations in the field of high technologies are outlined and analyzed, in view of the understanding of the concept «material» that applies to the objects of such research.

The necessity of the development of modern criminological technologies for the study of the objects of cybercrime, as well as possible directions of the development of such technologies is empathized.

Key words: cybercrime, cyberspace, globalization, material object, technology.

Не є таємницею, що процеси глобалізації та широке проникнення нових інформаційних технологій у всі сфери життя суспільства, крім їх безперечних переваг, породжують низку викликів і проблем, зокрема й у криміналістиці.

Нині на тлі зміни структури злочинності, у якій особливе місце займає діяльність добре технічно оснащених груп (що, до речі, істотно ускладнює процес ви-

явлення та розслідування злочинів), реальністю стала нова форма злочинності — злочинність у сфері високих технологій або кіберзлочинність, яка не обмежується кордонами окремих країн і активно набуває міжнародного характеру.

Інтенсивна інтелектуалізація злочинної діяльності, зокрема у сфері високих технологій, яка дедалі частіше активніше виходить за традиційні межі, породжуючи нові об'єкти криміналістичних досліджень та питання щодо їх матеріальності, вимагає адекватної протидії з боку правоохоронних органів.

Наукових робіт, присвячених суто питанням криміналістичного розслідування злочинів у сфері інформаційних комп'ютерних технологій, на жаль, обмаль. Окремі аспекти окресленої проблематики порушували науковці Д. С. Азаров, П. Д. Біленчук, О. В. Бойченко, С. М. Гусаров, А. М. Клочко, В. Д. Козюра, Є. Д. Лук'янчиков, О. В. Манжай, В. В. Марков, Л. П. Мотлях, Д. Й. Никифорчук, В. Г. Паламарчук, Д. В. Пашнєв, В. Д. Пчолкін, О. А. Севідов, Р. Л. Степанюк, О. І. Хахановський, В. О. Хорошко, Ю. А. Чаплинська, М. Г. Щербаковський, О. О. Юхно.

Водночас у сучасних умовах криміналістичне забезпечення виявлення і розслідування кіберзлочинів потребує вдосконалення з огляду на те, що традиційні заходи та прийоми нині вже не є дієвими й достатніми, дослідження проблем якого і становить мету цієї статті.

Для подальшого розгляду обраної проблематики слід визначитися з окремими поняттями, зокрема стосовно кіберпростору, у якому вчиняють кіберзлочини.

Основним законодавчим актом у сфері, про яку йдеться, є Закон України «Про основні засади забезпечення кібербезпеки України», який набув чинності 09.05.2018 р. Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їх діяльності із забезпечення кібербезпеки. Згідно із Законом кіберпростір — це «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [1].

Досить ємним є визначення кіберпростору, наведене в монографії за загальною редакцією А. В. Захарова [2]: кіберпростір — це інформаційний простір, що моделюється за допомогою комп'ютера, у якому містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному чи будь-якому іншому вигляді і такі, що перебувають у процесі руху локальними і глобальними комп'ютерними мережами, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, оброблення і передачі.

Згідно із Законом кіберзлочинність — це «сукупність кіберзлочинів», а «кіберзлочин (комп'ютерний злочин)» — суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1].

Фахівці ООН визначили кіберзлочинність так: у вузькому сенсі це поняття стосується виключно комп'ютерних злочинів, які є різновидом кіберзлочинів, а в широкому воно охоплює всі засоби доступу до кіберпростору. Тобто кіберзлочинність — це сукупність злочинів, що здійснюються в кіберпросторі за допомогою комп'ютерних систем або через комп'ютерні мережі, а також інших засобів доступу до кіберпростору, у межах комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Кіберзлочин — це суспільно небезпечне діяння, що здійснюється в кіберпросторі і посягає на громадську безпеку, власність, права людини, інші охоронювані законом відносини, необхідним елементом механізму підготовки, вчинення, приховування та відображення якого є комп'ютерна інформація, яка виступає в ролі предмета або засобу злочину [3].

У Конвенції про кіберзлочинність, прийнятій в Україні 23.11.2001 р., виокремлено 4 групи кримінальних правопорушень у сфері високих технологій [4]:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання в систему, зловживання пристроями);

2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами);

3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав.

На сьогодні найпоширенішими видами кіберзлочинів є [5; 6]:

– кардинг — використання в операціях реквізитів платіжних карт, отриманих з персональних комп'ютерів (безпосередньо або через програми віддаленого доступу: «троян», «боти»), платіжних і розрахункових систем тощо;

– вішинг — вид шахрайства з використанням «соціальної інженерії» та телефонної комунікації, спрямований на отримання конфіденційних даних власника платіжної карти;

– фішинг — вид шахрайства, спрямований на отримання доступу до рахунків і паролів клієнтів платіжних систем;

– онлайн-шахрайство — вид шахрайства, спрямований на отримання грошей з використанням віртуальних інтернет-аукціонів, інтернет-магазинів, сайтів тощо;

– соціальна інженерія — це злочинна руйнівна технологія управління діями людини в Інтернет-просторі, яка використовує фактор слабкостей людини;

– протиправний (деструктивний) контент (гібридні технології), спрямований на пропагування екстремізму, тероризму, наркоманії, порнографії, культів жорстокості, насильства, смерті, у тому числі з використанням гібридних технологій;

– мальваре — створення та розповсюдження вірусів і шкідливого програмного забезпечення;

– рефайлінг — незаконна підміна телефонного трафіка;

– піратство — незаконне використання та розповсюдження інтелектуальної власності в Інтернет-просторі;

– кард-шарінг — надання незаконного доступу до перегляду супутникового та кабельного телебачення;

– кібершпіонаж (комп'ютерний шпіонаж або «кіберрозвідка») — злочин, який реалізується завдяки «обходу» (зламу) систем комп'ютерної безпеки із застосу-

ванням шкідливого програмного забезпечення (наприклад, «троянський кінь») і спрямований на несанкціоноване отримання інформації з метою набуття особистої, економічної, політичної або військової переваги тощо.

Перелік найрозповсюдженіших видів кіберзлочинів не є сталим, адже постійний розвиток інформаційних технологій сприяє тому, що кіберзлочини стають дедалі багатограннішими та складнішими, а отже, їх перелік постійно розширюється.

Безперечно, проблема використання досягнень науки і техніки в злочинних цілях у сфері, про яку йдеться, пов'язана з одним із найважливіших інтеграційних процесів — створенням інтернаціональної по суті і глобальної за формою мережі Інтернет, яка об'єднує мільйони комп'ютерів.

Крім того, інтеграція телекомунікаційних мереж та їх конвергенція, поява можливості мобільного доступу до мережі Інтернет і постійне вдосконалення пристроїв доступу до неї (у тому числі портативних мобільних телефонів, комунікаторів тощо), створює нові можливості для зловживання інформаційними технологіями.

Таким чином, стрімкий розвиток комп'ютерних технологій та мереж і проникнення їх у різні сфери людської діяльності змінили характер злочинних посягань і породили нові їх форми, а отже, нові об'єкти криміналістичних досліджень, які значною мірою можуть відрізнятися від «звичайних» об'єктів як за формою, так і змістом [7].

Проведення таких досліджень (зокрема, судових експертиз) під час розслідування кіберзлочинів дає змогу встановити причинно-наслідковий зв'язок між вчиненим діянням і його негативними наслідками. З огляду на те, що поняття предмета й об'єкта судової експертизи належать до числа ключових у теорії та практиці судової експертології, доцільно докладніше зупинитися на їх визначенні, тим паче, що, зокрема, поняття об'єкта судової експертизи є неоднозначним з точки зору науки і практики.

З позиції наукової галузі знання об'єкт судової експертизи являє собою рід (вид) об'єктів, будь-який клас, категорію предметів, що характеризуються загальними властивостями [8].

З погляду практичної діяльності думки вчених щодо визначення поняття об'єкта в спеціальній літературі різняться. Основні визначення зводяться до того, що об'єкти — це [9]:

– тільки матеріально фіксовані об'єкти: предмети, речова обстановка або її елементи;

– матеріальні об'єкти і процеси.

При цьому науковці розуміють властивість «матеріальності» у кількох вимірах, серед яких філософське розуміння стосується поняття «матерія» (існує незалежно від свідомості, протилежне духовному) та розуміння ознаки матеріальності у вигляді набуття відчутної форми, речової, предметної властивості [10]. Тобто сигнал і фізичний процес є матеріальними в першому розумінні, але не мають ознак матеріальності в другому розумінні. Очевидно, що саме друге розуміння матеріальності покладено в основу, наприклад, поняття документа як речового доказу — певного предмета або речі (матеріального об'єкта).

Деякі криміналісти, зокрема А. І. Вінберг, Т. В. Авер'янова, М. М. Ростов, Т. В. Сахнова, розглядаючи об'єкти судової експертизи як системні утворення, зазначають, що всі вони характеризуються матеріальною природою (у тому числі матеріальна ре-

чова обстановка) [11; 12]. Інші вчені, у тому числі Ю. К. Орлов, Р. С. Бєлкін, уважають, що експерт може вивчати такі об'єкти як процес, подію, явище [13; 14].

Проте, коли йдеться про кіберзлочини, коли глобальний інформаційний простір, інформаційне мегасередовище нематеріальні і за своєю суттю не можуть бути зведені до фізичного носія, у якому втілені, об'єктами криміналістичного (експертного) дослідження таких злочинів можуть бути нематеріальні «продукти». Зокрема, до таких нематеріальних об'єктів можуть належати утворена за допомогою комп'ютерних технологій віртуальна або додаткова (доповнена) реальність, віртуальні співтовариства, наприклад «Синій кит», криптовалюти тощо.

Віртуальна реальність (англ. — virtual reality (VR), штучна реальність) — створений технічними засобами світ (об'єкти та суб'єкти), який передається людині через її відчуття: зір, слух, нюх, дотик тощо. Віртуальна реальність імітує як вплив, так і реакції на вплив. Для створення переконливого комплексу відчуттів реальності комп'ютерний синтез властивостей і реакцій віртуальної реальності проводиться в реальному часі [15].

На відміну від віртуальної реальності, доповнена реальність лише вносить окремі штучні елементи в сприйняття реального світу.

Криптовалюта — різновид цифрової валюти, створення і контроль за якою базуються на криптографічних методах [16].

Зазначені нематеріальні об'єкти за формою можна порівняти з таким узагальненим об'єктом, як психічна діяльність людини в судово-психіатричній, судово-психологічній та комплексній психолого-психіатричній експертизі. Йдеться саме про узагальнений об'єкт, адже психічну діяльність людини можна представити як сукупність певних властивостей, які характеризують психічні процеси, психічні якості, психічні стани та властивості. Тому психічна діяльність людини в кожному з цих видів експертиз розглядається в комплексі з матеріальними джерелами інформації: документами, характеристиками, особистими записами, щоденниками, малюнками тощо.

Аналогічно кіберзлочини містять графічну, звукову та іншу інформацію (на певних носіях) і дають змогу експерту в галузі комп'ютерно-технічних та телекомунікаційних досліджень допомогти слідчому (суду) установити обставини, які становлять об'єктивну сторону складу кримінального чи адміністративного правопорушення (наприклад, тексти, відео-, фотоматеріали можуть містити ознаки насилля, спонукання до самогубства або насилля, екстремізму тощо). Тобто самі по собі такі явища, як утворена за допомогою комп'ютерних технологій віртуальна або додаткова (доповнена) реальність, криптовалюти тощо, не можуть бути об'єктом дослідження. Об'єктами дослідження є інформаційні дані: текст, графіка, звук, відеоряд тощо, які розміщені на певних матеріальних носіях: жорстких дисках, серверах тощо [17].

Отже, вивчення подій, фактів, явищ та інших нематеріальних об'єктів здійснюється шляхом дослідження матеріальних носіїв інформації про них.

З огляду на те, що криміналістичне дослідження (у тому числі судова експертиза) об'єктів кіберзлочинів є одним із нових напрямів дослідження, а спектр об'єктів досліджень постійно збільшується та урізноманітнюється, теоретичні та методологічні основи криміналістичного дослідження кіберзлочинів остаточно не сформовано. Зокрема, серед криміналістів немає єдності поглядів на предмет, завдання і об'єкти криміналістичного дослідження кіберзлочинів.

Інформація, яку містять кіберзлочини, хоча і вважається об'єктом матеріального світу, водночас є елементом штучного середовища, створеним людиною, а отже, може існувати лише за допомогою спеціально пристосованих технічних засобів: електронно-обчислювальної техніки і електронних засобів зв'язку (системи телекомунікацій) тощо. Це, у свою чергу, зумовлює певні її властивості, зокрема:

– інформація в кіберпросторі є недоступною для безпосереднього людського сприйняття;

– певний зміст інформації не може бути однозначно закріплений за певним матеріальним носієм;

– матеріальний носій інформації в кіберпросторі (електромагнітне поле) неможливо індивідуалізувати;

– зміст інформації, як і її матеріальний носій можуть бути відокремлені один від одного без їх зміни;

– можливість швидкої зміни і видалення інформації, у тому числі шляхом віддаленого доступу і поза контролем осіб, що правомірно користуються цією інформацією;

– неможливість виділення точних і таких, що допускають єдине трактування, ознак, притаманних інформації в кіберпросторі тощо [18].

Підбиваючи підсумок, можна дійти висновку, що кіберзлочини за своєю суттю належать до злочинів високого інтелектуального рівня, тому ефективність і всебічність процесу криміналістичного пізнання такої злочинної діяльності багато в чому зумовлені його методологічною підготовленістю.

Криміналістичні дослідження забезпечуються конкретними методиками досліджень, які зазвичай містять дані про завдання дослідження, об'єкти, методи, алгоритми проведення робіт, критерії оцінки результатів і форми висновків.

Таким чином, в умовах глобалізації суспільства в межах єдиної стратегії боротьби з кіберзлочинами важливим завданням є розроблення сучасних комплексних криміналістичних технологій дослідження об'єктів цих злочинів. Основними напрямами розвитку таких технологій, на нашу думку, є пошук способу матеріалізації нематеріальних об'єктів дослідження або зміни підходів до дослідження об'єктів нематеріального характеру з добре виваженим вибором критеріїв для оцінки їх характеристик і властивостей.

Цікавим прикладом зміни підходів до дослідження окремих об'єктів нематеріального характеру може бути такий загальновідомий метод експертних оцінок, як суб'єктивна оцінка нелінійних спотворень звукового сигналу на основі суб'єктивного сприйняття. Цей метод уособлює серію суб'єктивних експертиз, організованих так: тридцять чотири експерти з перевіреними порогами слуху (середній вік — 21 рік) беруть участь у великій серії експериментів з оцінки якості звучання музикальних уривків (наприклад, чоловічий вокал з симфонічною музикою), до яких уведено різні види нелінійних спотворень.

Аналогічно гучність звуку можна оцінити за рівнем звукового тиску в децибелах або в суб'єктивних одиницях, за психоакустичним критерієм: фон, сон [19].

Список використаної літератури

1. *Закон* України «Про основні засади забезпечення кібербезпеки України» : станом на 09 трав. 2018 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/2163-19.

2. *Государство*, право, общество в условиях глобализирующегося мира : монографія / [под ред. А. В. Захарова]. — Тамбов : ООО «Проспект», 2016. — 413 с.

3. *Crimes* related to computer networks [Електронний ресурс] // Background paper for the workshop on crimes related to the computer Network A/CONF.187/10 // Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Vienna, 10—17 April 2000). — Режим доступу : https://www.asc41.com/UN_Congress/10th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/013%20ACONF.187.10%20Crimes%20Related%20to%20Computer%20Networks.pdf. — Пер. з англ. — Режим доступу : https://www.asc41.com/UN_Congress/Russian/10R%20Desyatij%20Kongress/A_CONF187_10.pdf).

4. *Конвенція* про кіберзлочинність від 23.11.2001 : станом на 01. липня 2006 р. [Електронний ресурс]. — Режим доступу : http:// zakon4.rada.gov.ua/laws/show/994_575.

5. *Голуб А.* Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс] / А. Голуб/ — Режим доступу : https://www.gurt.org.ua/articles/34602/.

6. *Энциклопедии* & Словари [Электронный ресурс]. — Режим доступа : http://enc-dic.com/word.

7. *Номоконов В. А.* Киберпреступность как новая криминальная угроза [Электронный ресурс]. / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста. — 2012. — № 1 (24). — С. 45—55. — Режим доступа : http://cripo.com.ua/?sect_id=1&aid=164985.

8. *Зинин А. М.* Судебная экспертиза : учебник / А. М. Зинин, Н. П. Майлис. — М. : Право и закон, 2002. — 320 с.

9. *Надгорный Г. М.* Объект автотехнической экспертизы / Г. М. Надгорный // Криминалистика и судебная экспертиза. — 1972. — Вып. 9. — С. 391—395.

10. *Словник* української мови : в 11 т. / за ред. І. К. Білодіда. — К. : Наукова думка, 1970—1980.

11. *Винберг А. І.* Гносеологический, информационный и процессуальный аспекты учения об объекте судебной экспертизы / Винберг А. І., Мирский Д. Я., Ростов М. М. // Вопросы теории и практики судебной экспертизы : сб. науч. трудов ВНИИСЭ. — М. : ВНИИСЭ, 1983. — С. 3—21.

12. *Аверьянова Т. В.* Судебная экспертиза. Курс общей теории / Т. В. Аверьянова. — М. : Норма, 2009. — 480 с.

13. *Орлов Ю. К.* Проблемы теории доказательств в уголовном процессе / Ю. К. Орлов. — М. : Юристъ, 2009. — 175 с.

14. *Белкин Р. С.* Криминалистическая энциклопедия / Р. С. Белкин. — 2-е изд. доп. — М. : Мегатрон XXI, 2000. — 334 с.

15. *Большая* политехническая энциклопедия [Электронный ресурс]. — Режим доступа : https://polytechnic_dictionary.academic.ru/315.

16. *Щербик Е. Е.* Феномен криптовалют: опыт системного описания / Е. Е. Щербик // Концепт. — 2017. — № S1. — С. 56—64.

17. *Дьяконова О. Г.* Теоретические основы судебной экспертологии : монография / О. Г. Дьяконова. — М. : Проспект, 2017. — 480 с.

18. *Криминалистическое* исследование компьютерной информации [Электронный ресурс]. — Режим доступа : http://textbook.news/kriminalistika_889/kriminalisticheskoe-issledovanie-kompyuternoy-103044.html.

19. *Алдошина И. А.* Субъективная оценка нелинейных искажений [Электронный ресурс] / И. А. Алдошина. — Режим доступа : http://albus-pro.ru/articles/20.html.

Стаття надійшла до редакції 21.02.2018 р.