УДК 343.983.25

ГОРА Ірина Віталіївна

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У ГАЛУЗІ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ В ДОСУДОВОМУ РОЗСЛІДУВАННІ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. Протягом останніх 20 років інформаційні технології внесли суттєві зміни у всі сфери людського життя. Сьогодні можна говорити не лише загалом про розповсюдження інформаційних технологій, а конкретно про їх безпосереднє впровадження в бізнес, юридичні й соціальні процеси тощо. Водночас необхідно брати до уваги наявність соціальних проблем у сучасному технократичному суспільстві, одною з яких є поява комп'ютерної злочинності, що завдає колосальної шкоди суспільним відносинам в інформаційній сфері.

Переваги сучасного цифрового світу та розвиток інформаційних технологій зумовили виникнення нових загроз національній і міжнародній безпеці. Разом з інцидентами природного (ненавмисного) походження зростають кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Кібератаки дедалі частіше стають інструментом швидкого досягнення необхідних результатів як в економічній, так і політичній сферах. Кібератаки здійснюються зокрема з метою викрадання конфіденційної інформації, персональних даних або їх знищення, блокування роботи інфраструктури тощо. Основними об'єктами протиправних спрямувань є інформаційно-комунікаційні системи органів державної влади, державні реєстри та бази даних, а також автоматизовані системи управління технологічними процесами об'єктів критичної інфраструктури енергетичного, транспортного та фінансового секторів [1, с. 105]. Вразливість усіх елементів суспільства, ураховуючи характер можливих кіберзагроз, досить висока.

Оскільки на сучасному етапі розвитку суспільства комп'ютерний елемент може бути практично в будь-якого злочину проти основ національної безпеки, обізнаність про можливості судової комп'ютерно-технічної експертизи є обов'язковою не лише для слідчого, а й оперативних співробітників контррозвідувальних та оперативно-розшукових підрозділів СБ України. Злочинці часто намагаються приховати докази, які їх викривають. Тому для виявлення

необхідної інформації й відтворення ходу подій, що мають значення для кримінального провадження, необхідним є застосування методів судово-комп'ютерної експертизи. Експертні висновки фахівців-комп'ютерщиків мають високу орієнтовну та доказову значущість. Вони дають змогу: розшифрувати закодовану інформацію; виявити інформацію, яка вважалася відсутньою, втраченою, знищеною; відтворити механізм злочинної події за інформаційними слідами; встановити modus operandi злочинця; встановити загальне джерело походження даних і документів (у складі комплексного дослідження) тощо. Якщо виникають такі проблеми, правозастосовувачі можуть використовувати цифрові докази та покладатися на них, діючи в межах надійного судово-експертного дослідження при автентифікації, реконструкції, оцінюванні. Сьогодні судові експерти в галузі комп'ютерно-технічної експертизи отримують усе більше запитів на проведення таких досліджень. Можна передбачити, що одним із наслідків поглиблення й прискорення цифровізації стане різке зростання комп'ютерної злочинності, а тому необхідні будуть експертні дослідження в межах судової комп'ютерно-технічної експертизи.

Аналіз останніх досліджень і публікацій. Судова комп'ютерно-технічна експертиза є самостійним родом судових експертиз, належить до класу інженерно-технічних, що проводяться з метою всебічного дослідження інформації, яка отримується з електронних носіїв. У 1979 році Інтерпол визнав проблему вчинення комп'ютерних злочинів глобальною. При розкритті таких видів злочинів стали широко використовуватися цифрові докази. Вперше правоохоронцям у різних країнах світу довелося вирішувати низку складних питань, пов'язаних із суттєвою особливістю нових об'єктів. Окрім речових доказів у вигляді матеріальних предметів (комп'ютерів, дискет, флешкарт та ін.), об'єктами дослідження стали й нематеріальні об'єкти – програмні продукти та власне інформація в різноманітних проявах, а не лише її носії.

Спеціальні знання у сфері сучасних інформаційних технологій можуть використовуватися у процесуальній формі (судова експертиза, участь спеціалістів у галузі комп'ютерно-технічних досліджень у проведенні слідчих і негласних слідчих (розшукових) дій) та в непроцесуальній формі (довідково-консультативна діяльність спеціаліста, експертні дослідження за матеріалами оперативно-розшукових і контррозвідувальних справ). До того ж, ці форми використання спеціальних знань тісно взаємопов'язані. Залежно від того, як повно й глибоко при проведенні процесуальних дій та оперативних заходів виявлені, зафіксовані й вилучені сліди злочинної діяльності в зазначеній сфері, як зібрані зразки для порівняльного дослідження, залежить успіх експертного дослідження сучасних комп'ютерних об'єктів. Особливе значення в проведенні нових видів комп'ютерно-технічної експертизи має їхнє методичне забезпечення. Сьогодні багато хто із вітчизняних і зарубіжних науковців у своїх працях розглядає науково-методичні, науково-

технічні й організаційні питання призначення та проведення комп'ютерно-технічних експертиз (далі – СКТЕ), проблеми використання спеціальних методів у дослідженні нових об'єктів цього виду експертиз. Зокрема, це наукові праці В. Вєхова, В. Гавла, О. Довженка, Д. Зав'ялова, Н. Зозулі, В. Зубахи, О. Мотляха, Ю. Нізовцева, Д. Пашнєва, В. Полякова, Р. Сабадаша, О. Усова, П. Харківського й ін. Наукові праці згаданих дослідників є вагомим внеском у розвиток теоретичних засад використання спеціальних знань у галузі комп'ютерно-технічної експертизи в кримінальному провадженні. Водночас питання щодо застосування спеціальних знань у формі проведення СКТЕ при дослідженні нових видів комп'ютерних об'єктів під час розслідування злочинів проти основ національної безпеки досліджені недостатньо.

Метою статті є розгляд сучасного стану й можливостей одного з найвитребуваніших на цей час родів із класу інженерно-технічних експертиз – комп'ютерно-технічної. Специфіка об'єктів комп'ютерно-технічної експертизи зумовлює окремий порядок їх підбору, підготовки, зберігання, направлення на дослідження та самого проведення експертних досліджень і застосування з цією метою методик. Адже об'єкт експертизи є невід'ємною і визначальною ознакою видової належності судово-експертного дослідження. У зв'язку із зростанням кіберзлочинності в сучасних умовах розвитку українського суспільства ставляться нові завдання перед експертними службами МВС та СБ України. Поява нових об'єктів, які використовують для вчинення злочину, і розширення кола експертних завдань потребують удосконалення експертних технологій, упровадження в експертну діяльність сучасних апаратних приладів, які застосовують у міжнародній практиці, постійного підвищення професійного рівня експертів-комп'ютерщиків.

Виклад основного матеріалу. Метою проведення комп'ютерно-технічної експертизи є: визначення статусу об'єкта як комп'ютерного засобу, встановлення й вивчення його ролі в розслідуваному злочині, а також отримання доступу до інформації, що міститься на електронних носіях, із подальшим всебічним її дослідженням. Необхідно зазначити, що судова експертиза призначається лише в разі дійсної потреби у спеціальних знаннях для встановлення фактичних даних, що входять до предмета доказування, тобто в разі, якщо висновок експерта не можуть замінити інші засоби доказування. Висновок експерта являє собою важливе джерело доказів і, як будь-який інший доказ, підлягає відповідному оцінюванню. Призначаючи таку експертизу, слідчий має враховувати специфіку методів дослідження та наданих об'єктів. Крім того, кожний етап призначення такої експертизи має свої особливості, зумовлені сферою спеціальних знань та організацією експертних досліджень у судово-експертних установах України. Обираючи експертну установу, слідчий має враховувати такі обставини: наявність установ, які проводять дос-

лідження в галузі комп'ютерно-технічної експертизи, та їхні можливості; реальну можливість провести експертизу в певні терміни; територіальне розташування експертного підрозділу; можливість проведення судової комп'ютерної експертизи за місцем знаходження електронних носіїв та інших об'єктів експертизи; наявність в експертів допуску до проведення цього роду експертиз; компетентність експертів. На цей час із метою вдосконалення таких, що є у судових експертів, методичних матеріалів для дослідження різних комп'ютерних об'єктів, а також у зв'язку з постійно зростаючими потребами органів досудового розслідування й оперативних підрозділів СБ України та МВС України в проведенні судових експертиз і експертних досліджень у цих судово-експертних установах та експертних установах Міністерства юстиції України активно формується судова комп'ютерно-технічна експертиза та її підвиди.

Зазвичай нова експертна спеціальність з'являється як результат диференціації або інтеграції знання, проте стихійний розвиток інформаційних технологій призвів до того, що практика випередила теорію, її вимоги змусили діяти на випередження, без проведення наукових пошуків, що стало тенденцією в усьому світі. Тривалий час точилися дискусії щодо назви експертиз із дослідження комп'ютерів і комп'ютерних технологій, програмного забезпечення, обсягу спеціальних знань, якими мали б володіти експерти з цього роду експертиз. У наукових публікаціях указуються різні назви цієї експертизи – судова комп'ютерно-технічна, комп'ютерна експертиза, інформаційно-аналітична технічна експертиза, експертиза електронно-обчислювальної техніки та її комплектуючих тощо.

Об'єктом судової комп'ютерно-технічної експертизи є комп'ютерні засоби, апаратні, програмні й інформаційні об'єкти. Родовим предметом судової комп'ютерно-технічної експертизи є факти й обставини, що встановлюються на підставі дослідження закономірностей розробки та експлуатації комп'ютерних засобів, котрі забезпечують реалізацію інформаційних процесів і зафіксовані в матеріалах кримінального провадження.

У теорії судової експертизи виокремлюють такі самостійні експертні підвиди експертизи комп'ютерної техніки і програмних продуктів: комп'ютерно-мережеву; програмно-комп'ютерну; апаратно-комп'ютерну; інформаційно-комп'ютерну [2, с. 41]. Ці види комп'ютерно-технічної експертизи доволі часто взаємопов'язані, проводяться послідовно й використовуються комплексно, тому при призначенні експертизи інколи доцільно вказувати її родову назву – комп'ютерно-технічна експертиза. Вітчизняні експертні установи ДНДЕКЦ МВС, ІСТЕ СБ України й НДІСЕ Міністерства юстиції виконують роль головних судово-експертних установ (СЕУ) із науково-методичного забезпечення проведення судової експертизи й активно впроваджують у судово-експертну діяльність інноваційні механізми її вдосконалення, зокрема й сертифікацію, валідацію та верифікацію судово-експертних методик, міжлабораторне професійне

тестування. Проте необхідно зазначити, що немає жодної лабораторії з проведення судової комп'ютерно-технічної експертизи ані в державній, ані в недержавній судово-експертній установі, котра могла б забезпечити комп'ютерно-технічні дослідження всього спектру комп'ютерних об'єктів. Тому слідчий, обираючи судово-експертну установу для проведення певного виду комп'ютерно-технічної експертизи, має пересвідчитися, чи виконується той або інший вид цієї експертизи в СЕУ, звідки слідчий має намір залучити відповідного фахівця.

У відповідному процесуальному документі, який передбачає залучення експерта для проведення судової комп'ютерно-технічної експертизи, мають обов'язково бути зазначені об'єкти, що надаються експерту на дослідження. Всі об'єкти СКТЕ можна умовно поділити на три класи: клас апаратних об'єктів, клас програмних і клас інформаційних об'єктів. До класу апаратних об'єктів належать: персональні комп'ютери; периферійні пристрої (принтери, модеми, сканери тощо); мережеві апаратні засоби (сервери, робочі станції, активне обладнання, мережеві кабелі тощо); інтегровані системи (органайзери, пейджери, мобільні телефони тощо); вбудовані системи на основі мікропроцесорних контролерів (імобілайзери, транспондери, круїз-контролери тощо); будь-які комплектуючі всіх перелічених компонентів (апаратні блоки, плати розширення, мікросхеми тощо). До класу програмних об'єктів належать: системне програмне забезпечення та прикладне програмне забезпечення. Інформаційні об'єкти – це текстові і графічні документи, що виготовлені з використанням комп'ютерних засобів; дані у форматах мультимедіа; інформація у форматах баз даних та інших додатків, що мають прикладний характер, та інше [3, с. 14].

Типовими завданнями апаратно-комп'ютерної експертизи як виду СКТЕ є: визначення виду, типу, марки, властивостей апаратного засобу, а також його технічних і функціональних характеристик; визначення фактичного стану і справності апаратного засобу, наявності в ньому фізичних дефектів; визначення структури, механізму, обставин події за її результатами за рахунок використання виявлених апаратних засобів; визначення умов застосування апаратних засобів; встановлення причинового зв'язку між користувачем конкретних можливостей апаратних засобів і результатами їх застосування. Типовими завданнями програмно-комп'ютерної експертизи можуть бути: визначення основних характеристик операційної системи; виявлення та дослідження функціональних властивостей і настроювання програмного забезпечення, визначення часу його інсталяції; визначення фактичного стану програмного об'єкта; виявлення ознак належності програмного забезпечення до системного або прикладного; встановлення первинного стану програми; діагностування алгоритму програмного продукту, видів інструментальних засобів, що використані для його розробки, а також типів апаратно-програмних платформ, які підтримуються програмою; визначення мети й умов змін властивостей і станів програмного забезпечення.

Типовими завданнями інформаційно-комп'ютерної експертизи є такі: встановлення властивостей і виду наданої інформації в комп'ютерній системі при її безпосередньому використанні; визначення фактичного стану інформації, з'ясування наявності або відсутності в ній відхилень від типового об'єкта СКТЕ; встановлення первісного стану інформації на носії даних; визначення часу, хронологічної послідовності впливу на інформацію; визначення умов зміни властивостей досліджуваної інформації тощо.

Окремо ми виділяємо комп'ютерно-мережеву експертизу, об'єкти якої можуть бути найрізноманітнішими – від персональних комп'ютерів користувачів, що підключені до мережі «Інтернет», до різних ресурсів постачальників мережевих послуг (провайдерів) і наданих інформаційних послуг (електронна пошта, служба електронних оголошень, телеконференції, різні сервіси тощо). Також об'єктами експертних досліджень можуть бути сервери, робочі станції, активне мережеве обладнання. Типовими завданнями цієї експертизи є: визначення властивостей і характеристик апаратного та програмного засобу; виявлення властивостей і характеристик обчислювальної мережі, встановлення її архітектури, конфігурації; визначення причин зміни властивостей обчислювальної мережі; дослідження, що пов'язані з інтернет-технологіями.

Серед об'єктів судової комп'ютерно-технічної експертизи значне місце займають мобільні телефони, ноутбуки та їхні жорсткі диски, флешкарти й планшети, а також окремі жорсткі диски, сервери, системні блоки, відеореєстратори й інші пристрої та носії інформації. Із розвитком інформаційних технологій певний інтерес викликають і об'єкти IoT – інтернету речей (різноманітна «розумна» техніка промислового й побутового призначення, хмарні сервіси збереження інформації, 3D-принтери та деякі інші технології виробництва й обробки інформації (штучний інтелект, машинне навчання, Big Data)). Розвиток нанотехнологій і технологій географічних інформаційних систем, зростання нейротехнологій із мікроелектронікою, активне впровадження нових технологій свідчать про важливість удосконалення вже існуючих та формування нових напрямів судової комп'ютерно-технічної експертизи.

Важливим аспектом призначення судової комп'ютерно-технічної експертизи є перелік питань, які ставляться експерту на вирішення. У посібнику «Експертизи у судочинстві України» нами пропонувався перелік типових запитань, які вирішуються експертами при проведенні цього роду експертиз [4, с. 315–316]. Також типовий перелік завдань для проведення різних видів комп'ютерно-технічної експертизи запропоновано в різних довідниках і наукових посібниках. Зазвичай питання, що ставляться на вирішення експертам у галузі комп'ютерно-технічної експертизи, залежать від обставин, які підлягають доказуванню, переліку досліджуваних об'єктів, наявності зразків для порівняльного дослідження тощо. У деяких, особливо нетипових, випадках слідчому бажано попередньо

отримати консультативну допомогу від експерта для визначення правильних і чітких формулювань запитань, визначення такої, що підлягає встановленню, інформації.

За кримінальними провадженнями про шпигунство, державну зраду, за злочинами на об'єктах критичної інфраструктури судова комп'ютерно-технічна експертиза призначається здебільшого з метою пошуку й дослідження на комп'ютерних об'єктах інформації користувачів. У такому разі на вирішення судовому експерту ставлять питання щодо: наявності на комп'ютерному об'єкті користувача файлів (графічних, текстових, відео, аудіо), зокрема й знищених; можливості їх відтворення, з'ясування питання щодо їх зміни; встановлення на об'єкті файлів, які містять певні ключові слова; виконання запитів щодо виходу пристрою в інтернет чи роботи в мережі, з'ясування питання щодо визначення сайтів, на які здійснювався вихід із конкретного пристрою, звідки здійснювався вихід (включаючи запити про IP-адреси), щодо історії браузера, щодо вирішення питання про скачування чи передачу файлів. Також слідчих можуть цікавити питання: щодо працездатності об'єкта, наданого на експертизу; чи є на об'єкті певне програмне забезпечення, наприклад, програми віддаленого доступу; чи можна використовувати об'єкт із певною метою (для виходу в інтернет, користування певними інформаційними системами чи базами даних); які дані користувача містяться на об'єкті (облікові записи, логіни, паролі й ін.).

При вирішенні питання щодо обрання певної експертної установи, яка буде проводити судову комп'ютерно-технічну експертизу певного виду, слідчому бажано з'ясувати й наявність в експертів необхідних спеціалізованих технічних засобів і програмних комплексів. Так, у деяких експертних підрозділах можуть використовуватися апаратно-програмні комплекси для досліджень, які дають можливість вилучати, декодувати й аналізувати доказові дані, що отримані з різних модулів мобільних пристроїв. Наприклад, для вилучення важливих криміналістично значущих даних (книг, фотографій, відеозаписів, текстових повідомлень, журналів викликів, даних IMEI), а також для оформлення їх у звіти для проведення досліджень і збирання доказів може застосовуватися універсальний прилад Universal forensic extraction device (UFED). Цей прилад дає можливість виконати вилучення даних на фізичному, логічному рівнях і на рівні файлової системи, а також відтворення паролів (уже видалених) із найрізноманітніших пристроїв, включаючи застарілі мобільні телефони, смартфони, портативні пристрої GPS та планшетні комп'ютери. Завдяки власному апаратному обладнанню, вбудованому акумулятору, інтуїтивно зрозумілому графічному інтерфейсу й сенсорному екрану UFED прискорює процес розслідування. Комплексне рішення UFED стандартної чи підвищеної міцності містить повний набір периферійних пристроїв і додаткового обладнання для роботи фахівців не лише в лабораторних, а й польових умовах. До складу

комплекту входить набір легких телефонних з'єднувачів, вбудований акумулятор, вбудована робоча поличка, а також жорсткий диск, вбудований у корпус підвищеної міцності, завдяки чому забезпечується швидка й ефективна дослідницька робота фахівця. До комплекту цього пристрою входять UFED Physical Analyzer – найпотужніше програмне забезпечення для поглибленого декодування й аналізу даних, а також створення детальних звітів і UFED Phone Detective – програмне забезпечення для миттєвої ідентифікації мобільного телефону [5]. Прилад UFED дає змогу проводити вилучення даних на логічному рівні, має можливість отримувати дані додатків, паролі, дані щодо переписки в месенджерах та електронній пошті, інформацію мультимедіа, список контактів, службову інформацію телефону, інформацію про переміщення та робити клонування sim-карт для ізоляції телефону від мережевої активності під час аналізу. UFED Camera – засіб, який дає можливість вручну збирати докази, знімаючи зображення даних або роблячи скріншоти безпосередньо з пристрою.

Швецькі розробники запропонували програмно-апаратний комплекс для проведення комп'ютерно-технічної експертизи мобільних телефонів і пристроїв MSAB Office, який поєднує в собі можливості як логічного, так і фізичного вилучення даних із мобільних пристроїв в одному наборі, ця система дозволяє експертам повний доступ до різних способів отримання необхідних даних. Ще одним програмним забезпеченням, яке розроблене спеціально для проведення комп'ютерно-технічних експертиз за завданнями правоохоронних органів і яке використовує кіберполіція багатьох країн світу, є Belkasoft Evidence Center. Воно значно полегшує отримання, пошук, аналіз, збереження й передачу цифрової інформації, що знаходиться всередині комп'ютерів і мобільних пристроїв. Ця програма швидко вилучає цифрові дані з різних джерел шляхом аналізу жорстких дисків, зразків, хмарних додатків, вмісту робочої пам'яті, резервних копій iOS, Blackberry і Android, UFED, JTAG і chip-off дампів. Використання в експертній практиці такого комплексу надає можливість виявити понад 1 000 типів інформації, включаючи понад 200 мобільних додатків, усі основні формати документів, браузери, поштових клієнтів, десятки графічних та відеоматеріалів, програми обміну миттєвими повідомленнями, соціальні мережі, системні файли, файли реєстратора, додатки для обміну файлами тощо. Ці й інші подібні програмні та технічні комплекси можуть ефективно використовуватися в експертній практиці ІСТЕ СБ України й інших судово-експертних підрозділах України.

Також важливим напрямом науково-методичного забезпечення діяльності з проведення судових комп'ютерно-технічних експертиз є розробка й впровадження в експертну практику сучасних науково обґрунтованих експертних методик дослідження різноманітних комп'ютерних об'єктів. Проте експерту інколи важко обрати необхідну методику.

Методики проведення судових експертиз (окрім судово-медичних та судово-психіатричних) підлягають атестації та державній реєстрації в державному Реєстрі методик проведення судових експертиз (далі – Реєстр). Реєстрацію методик проводить Міністерство юстиції, котре є утримувачем Реєстру та визначає організаційні й методологічні принципи його ведення. На цей час у державному Реєстрі методик проведення судових експертиз за відповідними кодами зареєстровано: методики з дослідження інформації на жорстких дисках; дослідження поштових програм і програм обміну електронними повідомленнями; методику пошуку та дослідження графічної інформації на комп'ютері; методику дослідження комп'ютерної інформації; криміналістичний аналіз файлових систем; проведення комп'ютерно-технічних досліджень носіїв цифрової інформації; методику дослідження інформації на цифрових носіях; дослідження роботи користувача персонального комп'ютера в мережі «Інтернет»; методичні рекомендації з дослідження реляційних баз даних при проведенні судових комп'ютерно-технічних експертиз; методику комп'ютерно-технічного дослідження інформації в пам'яті SIM-карток; методику комплексних досліджень комп'ютерних та телекомунікаційних систем у справах, пов'язаних із виявленням фактів спотворення процесу обробки інформації та порушення правил маршрутизації в мережах електрозв'язку з використанням технології VoIP; методику комп'ютерно-технічних досліджень у справах, пов'язаних із встановленням фактів втручання в роботу автоматизованих систем; методику дослідження носіїв інформації, створених із застосуванням напівпровідникової технології; методику дослідження у віртуальному середовищі налаштувань програмного забезпечення, встановленого на персональному комп'ютері; методику з використання спеціальних знань експертів у галузі комп'ютерно-технічних досліджень при проведенні комплексних досліджень цифрової інформації; методику комп'ютерно-технічного дослідження інформації в пам'яті SIM (USIM) та R-UIM карток; методику дослідження інформації у пам'яті портативних комп'ютерних засобів, керованих операційною системою ANDROID; методику дослідження файлових систем і службової інформації оптичних дисків однократного та багатократного запису; методику визначення фактів знищення інформації на цифрових носіях [6].

У деяких випадках експерт, якого залучено для проведення комп'ютерно-технічної експертизи, не визначившись із необхідною методикою чи не знайшовши її в державному Реєстрі, може використовувати наукові посібники з цієї галузі й адаптувати вже розроблені методичні рекомендації під конкретну ситуацію чи об'єкти, представлені на експертизу слідчим. Основне, що треба враховувати в разі розроблення певних або інших експертних методик із дослідження комп'ютерних об'єктів, а в особливості електронної інформації та її носіїв, – це максимальне збереження цілісності та незмінності таких речових доказів. Під незмінністю

речових доказів слід розуміти не тільки незмінність стану машинозчитуваного носія інформації, але й забезпечення повного збереження інформації, що зафіксована на такому носієві. Завдання-максимум полягає в тому, щоб забезпечити збереженість і незмінність як досліджуваної, так і усієї інформації, що зафіксована на магнітному носієві, навіть якщо вона прямо не стосується фактів, які цікавлять орган, що призначив експертизу, і не стає предметом експертного дослідження. Звідси й специфічні вимоги до будь-якої методики з проведення цієї експертизи: експерт повинен досліджувати не власне наданий речовий доказ (магнітний носій або інформацію на машинному носієві), а точну копію цієї інформації, що перенесена на спеціально підібраний експертом магнітний носій. Крім того, важливо, щоб створювані методики містили й методи та засоби, доступні для відтворення іншим експертом і такі, що дають можливість повторити за необхідності всі етапи експертного дослідження. У такому разі можна буде вести мову про виключення суб'єктивізму при провадженні нового виду експертиз та зменшення залежності результатів дослідження від особистого досвіду й інтуїції експерта. Отже, необхідно розробляти типові методики, призначені для вирішення типових експертних завдань у судовій комп'ютерно-технічній експертизі.

Неабияке значення в розробленні науково-методичного забезпечення проведення судово-комп'ютерних експертиз має експертна практика різних країн світу. Так, наприклад, експертні підрозділи таких провідних країн Європи як Велика Британія, Нідерланди, Франція, Німеччина проводять експертні дослідження таких об'єктів СКТЕ як інтегровані та вбудовані системи, відкриті системи, системи зв'язку, а також мультимедійні об'єкти. Здебільшого метою дослідження цих об'єктів є вирішення діагностичних та ідентифікаційних завдань при дослідженні інформаційної системи, отриманні доступу до електронного обладнання та інформації. Особлива увага при дослідженні мобільних терміналів приділяється телекомунікаційним сервісам SMS, EMS, MMS, оскільки вони можуть надавати відомості про осіб, причетних до вчинення кримінальних дій, зокрема й у мережі мобільного зв'язку [7, с. 203–217].

Значний обсяг роботи судових експертів у Нідерландах, Чехії, Італії та інших країнах ЄС пов'язаний із дослідженням відкритих систем. Відкриті системи охоплюють різні операційні системи, їхні архітектуру, апаратно-програмні комплекси. Апаратними об'єктами експертизи в цих випадках є різні комп'ютерні системи: від мініатюрних персональних комп'ютерів до суперкомп'ютерів. Для цих систем характерною є наявність різних електронних накопичувачів даних: від жорстких та флоппідисків, стрічок, CD-ROM, DVD, магнітооптичних накопичувачів до RAID-масивів. Загалом криміналісти ЄС успішно застосовують при розслідуванні злочинів та отриманні доказової інформації з електронних носіїв за допомогою апаратно-програмного інструментарію такі операції як злам захисту паролів, моделювання

пам'яті вилучених електронних апаратів у пам'яті комп'ютера: електронних записних книжок (органайзерів), стільникових телефонів, сім-карток і модулів, смартфонів та інших носіїв інформації. Експерти Празького інституту криміналістики займаються розробленням експертних методів та інструментальних засобів для вилучення інформації з більшості моделей електронних органайзерів Casio та Sharp. Вони створили спеціалізоване програмне забезпечення CasioTool, котре здатне моделювати на персональному комп'ютері експерта органайзер такого самого типу. Модель функціонує в інтерактивному режимі й дає можливість читати вміст всієї пам'яті досліджуваного пристрою, зокрема і його протоколи, а також проводити аналіз даних і відображати знайдений пароль [8, с. 190–192].

Географічні інформаційні системи та комунікаційні інформаційні системи є також перспективним полем діяльності судових експертів, які спеціалізуються на мережевій та міжмережевій взаємодії у відкритих системах. Найцікавішими розробками в цій галузі є дослідження експертів Франції та Німеччини. Основними завданнями є дослідження різних інформаційних потоків із метою їх виявлення, інтерпретації повідомлень, відтворення інформації, розкодування даних, виявлення використаних різноманітних алгоритмів. Головним в експертному дослідженні є вивчення протоколів передачі даних, зокрема й повного стеку протоколів за рівнями OSI. Така модель включає в себе маршрутизовані та транспортні протоколи. Окремим видом є проведення досліджень телекомунікаційних мереж забезпечення стільникового зв'язку GSM, GPS, GPRS-комунікацій. Проте дії фахівців із перехоплення сигналів зв'язку, їх аналізу, ідентифікації системи окремого та глобального зв'язку, географічної області, локалізації користувача й адресата часто пов'язані з проведенням контрозвідувальної та оперативно-розшукової діяльності і застосовуються експертами в галузі комп'ютерно-технічної експертизи лише з прикладною метою для вирішення певних завдань. Така ситуація спостерігається і в дослідженнях, пов'язаних із розслідуванням різних злочинів у глобальних мережах. Ця галузь спеціальних знань дає можливість вирішувати завдання ідентифікації та діагностики користувачів мережі, їхніх ресурсів, аналізувати роботу провайдерів, характеристики досліджуваних трафіків та інформаційних систем Internet (електронна пошта, телеконференції, архіви на серверах, багатоканальна розмова за допомогою служби IRQ, служба WWW), активне застосування різноманітних програм-браузерів. Сучасні інтернет-технології, технології розробки програмного забезпечення (OLE, ActiveX), різні plug-ins, Java-апплети та ін. значно розширюють список імовірних форматів даних та об'єктів програмного забезпечення, що надходять до експертів [7, с. 203–204; 2, с. 228–229].

У процесі проведення експертного дослідження фахівці в галузі комп'ютерно-технічної експертизи здійснюють різні за складністю дії: від діагностики й аналізу апаратного середовища, встановлення його

характеристик до аналізу сигналів та електронного аналізу на рівні дослідження мікросхем, аналізу спеціалізованого мікропроцесорного обладнання. У разі аналізу пошкодженого пристрою чи його частини іноді виникає потреба розроблення моделі цілісної системи в апаратному або електронному вигляді. У подальшому в процесі моделювання функціонування досліджуваного об'єкта вирішуються питання експертизи. У Нідерландах та Німеччині розробляються методики апаратної експертизи інтегрованих систем та вбудованих комп'ютерних пристроїв. Така робота часто спрямована на апаратно-програмне вирішення завдання подолання захисних функцій комп'ютерних пристроїв, що надані на експертне дослідження. У професійному середовищі судових експертів ці дії інколи називають «експертний злам» [9, с. 286–287].

Судова комп'ютерно-технічна (цифрова) експертиза повністю залежить від програмного забезпечення додатків та інструментів, які розроблені й використовуються для збирання, відображення та розшифровки цифрових даних. Результати будь-якого дослідження, у процесі якого використовувалися ці засоби, мають бути вірогідними, відтворюваними й одночасно такими, що сприяють встановленню факту, котрий можна буде використати для встановлення вини чи невинуватості конкретної особи. Не дивлячись на велике значення цифрових засобів дослідження, на сьогодні в цій галузі недостатньо стандартів і процедур тестування, які б давали змогу ефективно обґрунтовувати їхнє застосування в ході досудового розслідування. Проте проведення судово-комп'ютерної експертизи надає слідчому додаткову можливість правильно зрозуміти наявні на досліджуваних пристроях цифрові сліди, що сприяє прийняттю правильних та обґрунтованих рішень.

Висновки. На сучасному етапі у зв'язку із специфікою комп'ютерних об'єктів, появою їхніх нових видів і необхідністю залучення осіб, які володіють спеціальними знаннями в галузі інформаційно-обчислювальних технологій та інформаційно-обчислювальної техніки, подальший розвиток окремого роду судових експертиз – комп'ютерно-технічної – є вкрай витребуваним. Встановлені при її проведенні відомості можуть бути використані як доказова або як орієнтовна інформація, що має значення для досудового розслідування багатьох злочинів, зокрема й проти основ національної безпеки. Розвиток системи судово-експертних установ, які можуть проводити комп'ютерно-технічні експертизи, надає можливість використовувати високі технології в протидії злочинам. Удосконалення методів і форм проведення таких експертиз розширить можливості виявлення, доказування та припинення багатьох злочинів проти основ національної безпеки.

Список використаних джерел

1. Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право.* 2019. № 3 (30). С. 105–110.

2. Усов А. И. Судебно-экспертное исследование компьютерных средств и систем: основы методического обеспечения : учебное пособие. Москва : Экзамен: Право и закон, 2003. 366 с.

3. Усов А. И. Методы и средства решения задач компьютерно-технической экспертизы : учебное пособие. Москва : ГУ ЭКЦ МВД России, 2002. 200 с.

4. Експертизи у судочинстві України : навч.-наук. посіб. / за заг. ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2018. 504 с.

5. Комплексное решение для мобильной криминалистики UFE DTOUCH ULTIMATER. URL: http://www.bnti.ru?des.asp?itm=6495&tbl=01.02.01.01 (дата звернення: 07.05.2021).

6. Про затвердження порядку атестації та державної реєстрації методик проведення судових експертиз : Постанова Кабінету Міністрів України від 02.07.2008 № 595. *Офіційний вісник України*. 2008. № 49. Ст. 1585.

7. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография. Волгоград : Волгоградская академия МВД России, 2008. 401 с.

8. Васильев А. А., Дёмин К. Е. Электронные носители данных как источники получения криминалистически значимой информации : учебно-методическое пособие. Москва : МГОУ, 2009. 200 с.

9. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях. Москва : Норма, 2004. 432 с.

Аннотация. В современном судопроизводстве важное значение имеют различные формы использования судебно-экспертных знаний. В статье анализируется современное состояние проведения судебных компьютерно-технических экспертиз и действующая судебно-экспертная практика в этой сфере, рассматривается вопрос о необходимости специальных знаний для проведения такого вида экспертиз. Обосновывается, что судебная компьютерно-техническая экспертиза является самостоятельным родом судебных экспертиз и относится к классу инженерно-технических. Представлены определения объекта, предмета компьютерно-технической экспертизы, сформулированы типовые задачи. Рассмотрены вопросы, которые ставятся перед экспертами при назначении судебных компьютерно-технических экспертиз по исследованию новых компьютерных объектов.

Abstract. In modern legal proceedings, the use of various forms of forensic expert examination is important. The article analyzes the current state of forensic computer-technical expert examination and the current forensic expert practice in this area, considers the issue of the need for special knowledge to conduct this type of examinations. It is substantiated that forensic computer-technical expert examination is an independent type of forensic expert examination and belongs to the class of engineering and technical examination. The definitions of the object, the subject of computer-technical examination are presented, typical tasks are formulated. The issues, faced by the experts when assigning forensic computer-technical examinations for the study of new computer objects are considered. Determination of the expert's assignment and the formulation of questions are considered as an

Определение задания эксперту и формулировка вопросов рассматриваются как важный этап назначения экспертизы, от которого зависит правильный выбор методики исследования. С развитием информационных технологий для следователей представляют интерес новые объекты, по которым необходима подготовка отдельных методических разработок, рекомендаций по определению последовательности проведения различных видов исследований. Обосновано, что выводы судебных экспертов по компьютерно-технической экспертизе имеют большое доказательственное значение. Они дают возможность: расшифровать закодированную информацию; обнаружить информацию, считавшуюся отсутствующей, утерянной или уничтоженной; восстановить механизм преступного события по информационным следам.

Ключевые слова: судебно-экспертная деятельность, криминалистические исследования, информационно-телекоммуникационная система; компьютерные преступления; судебная компьютерно-техническая экспертиза; электронные носители информации.

important stage in the planning of an examination, on which the correct choice of research methodology depends. With the development of information technologies, investigators are interested in new objects for which it is necessary to prepare individual methodological recommendations, manuals for determining the sequence of conducting various types of examinations. It has been substantiated that the conclusions of forensic experts on computer-technical examination are of great evidentiary value. They make it possible to: decipher the encoded information; find information that was considered missing, lost or destroyed; restore the mechanism of a criminal event based on information traces.

Key words: forensic activity, forensic research, information and telecommunication system; computer crimes; forensic computer-technical examination; electronic media.

УДК 343.98.

КОЛЕСНИК Валерій Аркадійович

КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Постановка проблеми. З кінця XX і протягом останніх десятиліть XXI століття у зв'язку з розвитком інформаційних технологій, комп'ютеризацією державно-управлінських, промислових і соціальних процесів відбулися значні зміни в усіх сферах суспільного життя не лише в Україні, а й в інших країнах світу. Сьогодні не сприймається як перебільшення те твердження, що виникнення та розвиток всесвітньої пандемії Covid-19 і поширення планетою швидко змінюваних модифікацій небезпечного й