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

нового для людства вірусу слугувало імпульсом, який дав поштовх для пошуку шляхів розв'язання давно назрілих технологічних і соціальних проблем. Якщо раніше в керівників урядових структур, законодавців, державних службовців та й у пересічних громадян ще були питання стосовно того, яку роль відіграють в їхньому житті та в житті певної країни інформаційні технології, то на тепер таких питань навіть не виникає. Для всіх стало очевидним, що інформаційні технології, всесвітня мережа «Інтернет», дистанційні форми діяльності в багатьох сферах соціальної практики, виробництва і навчання від керування державою та міжнародними процесами до відвідування дитячих дошкільних закладів та інші можливості впровадження комп'ютерних технологій у повсякденне життя є реальністю і звичним сьогоденням. Водночас одним із наслідків поглиблення, прискорення й удосконалення інформаційних процесів стало зростання комп'ютерної злочинності. Такі злочини становлять серйозну загрозу для будь-якого підприємства, організації, установи та й фізичної особи, котра має та використовує комп'ютерну техніку. До того ж, ідеться не тільки про високий ступінь ризику втрати інформації, користувачам комп'ютерних систем і мереж завдається й значна матеріальна шкода.

Питання протидії кіберзлочинності набуває сьогодні особливої актуальності у зв'язку з постійним розширенням сфери застосування сучасних інформаційних технологій. Експерти вказують навіть на зростаючу небезпеку для стабільності політичних систем, зумовлену протиправними посяганнями на автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку [1, с. 74]. Науковці й практики звертають увагу на те, що з розвитком інформаційних технологій стали розроблятися інструменти навіть для шпигунства з використанням як спеціалізованих пристроїв, так і програмного забезпечення. На відміну від класичних методів розвідки та шпигунства, нові технології внесли в них суттєві коригування. Іноді навіть неможливо встановити, хто саме розробив програмне забезпечення для проведення розвідувальних дій у сфері високих технологій. Розробниками такого спеціалізованого програмного забезпечення можуть бути як приватні особи, так і підприємства різної форми власності з різними джерелами фінансування. Нерідко особи, які розробили програмне забезпечення, не є тими особами, які його використовують для здійснення кібершпигунства. Це ускладнює, а іноді й унеможливлює ідентифікацію осіб, які здійснюють кібершпигунство, і як результат – притягнення їх до встановленої форми відповідальності [2, с. 11].

Водночас треба розуміти й те, що загрози кібербезпеці не можуть бути усунені повністю ні у всьому світовому просторі, ні в окремій країні. Проте їхній ризик може бути значно зменшено до рівня, який дасть змогу суспільству розвиватися й отримувати користь від інформаційних технологій. Разом із тим, розширення сфери застосування інформаційних технологій створює й нові залежності. Адже керування державою, економіка, освіта й надання основних послуг

населенню сьогодні істотно залежать від цілісності та безпеки національного й світового кіберпростору, від інформаційної інфраструктури, систем і даних, котрі його підтримують.

Аналіз останніх досліджень і публікацій. Проблеми комп'ютерної, інформаційної, кіберзлочинності привернули увагу криміналістів провідних країн із перших кроків упровадження комп'ютерної техніки у сферу виробництва та суспільних відносин. Питання виявлення й досудового розслідування злочинів у сфері інформаційних, високих, цифрових, комп'ютерних технологій досліджували відомі фахівці в галузі криміналістики, кримінального права, кримінології, теорії судової експертизи як у нашій країні, так і в ближньому та дальньому зарубіжжі. Зокрема ці питання стали предметом окремої уваги Ю. М. Батуріна, П. Д. Біленчука, В. М. Вєртузаєва, В. Б. Вєхова, В. Д. Гавловського, Ю. В. Гавриліна, В. О. Голубєва, М. В. Гуцалюка, М. Ю. Дворецького, Р. А. Калюжного, В. В. Крилова, Б. Д. Леонова, О. М. Литвинова, А. Б. Нехорошева, Ю. Ю. Нізовцева, В. І. Польового, В. Ю. Рогозіна, Б. В. Романюка, А. І. Усова, В. С. Цимбалюка, О. К. Юдіна та багатьох інших науковців. Проте, зважаючи на широкий спектр цієї проблематики, що охоплює значне коло питань з організації та здійснення протидії комп'ютерній злочинності, організації виявлення, розкриття й досудового розслідування злочинів зазначеної категорії, багато які з питань є такими, що потребують додаткового або й окремого та цілеспрямованого вивчення.

Як відомо, у науковій та спеціальній літературі злочини у сфері інформаційних технологій, що вчиняються з використанням комп'ютерних засобів і систем та їхнього програмного забезпечення, часто прийнято називати «комп'ютерними злочинами». До того ж, цю дефініцію потрібно вживати не в кримінально-правовому аспекті, оскільки це лише утруднює кваліфікацію діяння, а в криміналістичному, тому що вона пов'язана не з правовою кваліфікацією діянь, а власне із способом вчинення та приховування злочину і, відповідно, з методикою його досудового розслідування. Розслідування зазначених кримінальних правопорушень істотно відрізняється від досудового розслідування інших, так званих «традиційних» злочинів. Вивчення кримінальних проваджень цієї категорії дає підстави вважати, що певною причиною низької якості виявлення й досудового розслідування таких правопорушень є відсутність достатньої кількості відповідним чином опрацьованих і систематизованих методик розслідування. Це стає причинами багатьох помилок, які допускають слідчі під час проведення окремих слідчих (розшукових) дій, пов'язаних з отриманням та дослідженням комп'ютерної інформації, оглядом комп'ютерів, комп'ютерних мереж, окремих носіїв цифрової інформації та вивченням інших специфічних у певному відношенні об'єктів.

Метою цієї статті є розкриття сутності й значення криміналістичного аналізу специфічних об'єктів комп'ютерних злочинів як кримінальних правопорушень у сфері

інформаційних технологій, характерних слідів як наслідків їх вчинення.

Виклад основного матеріалу. Криміналісти цілком обґрунтовано вказують на те, що комп'ютерні злочини мають місце лише тоді, коли: з одного боку, комп'ютерна інформація є предметом посягання; з іншого боку, комп'ютерна інформація та засоби комп'ютерної техніки виступають у вигляді специфічного знаряддя злочину або його складової, без чого неможливе вчинення злочину [3, с. 7]. За оцінками вітчизняних і зарубіжних дослідників, що були надані ще на початку нинішнього тисячоліття, розв'язання проблем розкриття й розслідування злочинів цього виду становить завдання на декілька порядків складніше, ніж завдання із запобігання їм. Звертають увагу й на те, що в нашій країні рівень латентності комп'ютерних злочинів визначається у 90 %, а із залишку 10 % виявлених розкривається тільки 1 %. І ще менший відсоток розкритих злочинів, щодо яких винесено судом обвинувальний вирок [4, с. 76]. Із початку XXI століття і до теперішнього часу в такій невтішній статистиці мало що змінилось. Такі дані вказують не лише на складнощі виявлення й досудового розслідування кримінальних правопорушень певної категорії, а й на потребу практики мати відповідні науково обґрунтовані засоби протидії злочинам у сфері інформаційних технологій.

Складність досудового розслідування кримінальних правопорушень цієї категорії великою мірою пов'язана із складністю встановлення правоохоронними органами самого факту їх вчинення. Важко встановити матеріальні сліди як наслідки цього злочину, тому несвоєчасно вносяться відомості до Єдиного реєстру досудових розслідувань та починається кримінальне провадження. Ці наслідки не завжди пов'язані з видимими матеріальними збитками чи іншими втратами, але й у разі наявних збитків не завжди зрозумілою буває їхня причина. Наприклад, незаконне зняття копії комп'ютерної інформації найчастіше залишається невиявленим із боку законного користувача чи володаря такої інформації, навмисне введення в комп'ютер шкідливого вірусу часто вважають наслідком непередбаченої помилки користувача, який не зміг надійно захистити свій комп'ютер або своєчасно знешкодити вірус, що потрапив до системи в процесі спілкування із зовнішньою комп'ютерною мережею, тощо. Іноді це стається випадково – у результаті перешкод на лініях зв'язку, відмови або ж збоїв апаратури, помилок людини як ланки системи, схемних системних помилок розробників, до яких належать структурні, алгоритмічні помилки. Можливими також є різні аварійні ситуації й інші впливи [5, с. 14].

Низьким є рівень розкриття комп'ютерних злочинів і внаслідок складного математичного й апаратного забезпечення функціонування інформаційних мереж і систем. Ще одна причина – навіть за вочевидь корисливих мотивів цих злочинів і виявлених збитків самі постраждалі не часто поспішають повідомити правоохоронні органи про встановлені ними факти кримінальних правопорушень. А винуватці таких злочинів

часто просто звільняються з роботи після вчинення злочину або переводяться до інших структурних підрозділів того ж підприємства й продовжують сумлінно та плідно працювати, не викликаючи ніяких підозр. Оскільки не встановлене покарання за злочин, закономірно, що не проводяться й заходи загальної профілактики, а безкарність породжує в особи нові замисли до вчинення інших, витонченіших злочинів у сфері кібербезпеки.

Механізм вчинення злочинів, пов'язаних з інформаційними технологіями, часто прихований від потерпілих, якими є законні користувачі комп'ютерних систем та володарі комп'ютерної інформації. Окрім того, і протиправний витік інформації може бути прихований за допомогою тих самих електронних засобів ще до того, як факт незаконного втручання в роботу комп'ютера або інформаційної системи буде встановлено. У розкритті факту вчинення злочину часто бувають незацікавленими посадові особи, обов'язком яких є забезпечення комп'ютерної безпеки. Визнання факту несанкціонованого доступу до підвідомчої їм інформаційної системи ставить під сумнів їхню професійну здатність, належну кваліфікацію, а неспроможність задіяних заходів інформаційної безпеки може викликати серйозні внутрішні ускладнення. Наприклад, представники банківської системи зазвичай ретельно приховують виявлені ними злочини, що вчинені з неправомірним втручанням у банківську комп'ютерну мережу, тому, що це може згубно вплинути на престиж конкретного банку та призвести до втрати клієнтів, порушення партнерських бізнесових зв'язків тощо. Деякі жертви комп'ютерних злочинів бояться компетентного й відкритого кримінального процесуального розслідування більше за втрати, яких зазнали. Відбувається це тому, що офіційне розслідування злочину може викрити непорядну і навіть незаконну практику ведення справ самим потерпілим. Також не повідомляють про злочини з остраху, що страхові компанії, які покривають збитки в разі настання страхових випадків, можуть збільшити розміри внесків або навіть відмовитися від надання страхового полісу, якщо комп'ютерні злочини для певної організації є регулярними явищами.

Загальним об'єктом комп'ютерних злочинів є суспільні відносини у сфері забезпечення інформаційної безпеки, а до безпосередніх об'єктів злочинного посягання належать: інформаційні бази й банки даних комп'ютерних систем або мереж, їхні окремі файли, а також комп'ютерні технології та програмні засоби їхнього забезпечення, зокрема й засоби захисту комп'ютерної інформації. То ж не даремно законодавець у Законі України «Про захист інформації в інформаційних телекомунікаційних системах» зазначив, що об'єктом захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації [6]. Предметом злочинного посягання є комп'ютерна інформація, що охороняється законом, де б вона не містилася або оберталася: в пам'яті комп'ютера, у системі, мережі на каналах електронного

зв'язку, на відокремлених від комп'ютера машинних носіях.

Особи, які винні у вчиненні зазначених злочинів, де була використана комп'ютерна техніка, новітні інформаційні технології, програмне забезпечення, несуть відповідальність за різними статтями Кримінального кодексу. Це визначається механізмом, способом вчинення й приховування злочину, загальною специфікою, зумовленою властивостями й структурою інформаційних технологій. За таких умов особливу роль відіграють юридична наука, кримінальне право, що розробляє відповідні положення кримінального законодавства, а також така наукова галузь як криміналістика, котра реалізує спеціальні юридичні знання, максимально наближені до практики боротьби із злочинністю.

Пропонуючи криміналістичні рекомендації з досудового розслідування злочинів, що вчинені з використанням комп'ютерних технологій, слід ураховувати, що існують розроблені на підставі криміналістичного аналізу окремі методики їх розслідування, але доцільно виокремити дещо спільне, що можна використати в спеціалізованих методиках. На наш погляд, природа цього спільного прихована в особливостях обчислювальної техніки й інформації, у жорстких алгоритмах функціонування та відкритих стандартах інформаційного обміну, котрими й визначаються специфічні риси комп'ютерних злочинів. Науковці та практики звертають увагу на те, що в процесі роботи правоохоронних органів України під час виявлення й досудового розслідування таких злочинів виникають певні криміналістичні проблеми, що характеризують водночас і специфіку цього процесу, а саме: складність у встановленні факту вчинення комп'ютерного злочину та вирішенні питання про початок здійснення досудового розслідування; складність у кваліфікації злочинних діянь кожної з винних осіб; складність у підготовці й проведенні окремих слідчих і негласних слідчих (розшукових) дій; відсутність необхідних спеціалістів з окремих питань, яких потрібно залучати до проведення слідчих дій; не завжди враховуються особливості вибору й підготовки матеріалів та призначення й проведення необхідних судових експертиз; не визначається доцільність використання слідчим надсучасних засобів комп'ютерної техніки під час розслідування злочинів цієї категорії; у значної кількості слідчих та оперативних співробітників немає достатніх знань у галузі комп'ютерної техніки та програмного забезпечення інформаційних процесів; не проводиться цілеспрямоване узагальнення слідчої та судової практики з розслідування злочинів цієї категорії; немає цілісної методики розслідування комп'ютерних злочинів [4, с. 76].

Для вивчення й пізнання об'єкта (явища, дійсності) його треба поділити на складові та розглядати ці окремі елементи, щоб виокремити істотне, відокремити його від другорядного, звести складне до простого. При цьому виникає необхідність у використанні такого наукового методу пізнання як аналіз. У кожній науці аналіз має свій специфічний і конкретний зміст, наприклад, математичний,

логічний, статистичний, юридичний, психологічний тощо. Досліджуючи будь-який злочин, вивчають сукупність дій осіб, які його вчиняють, приховують, отже, аналізу підлягає діяльність злочинця. Для криміналістів важливим є криміналістичні аспекти цього аналізу та можливість використання отриманих результатів у виявленні, розкритті, досудовому розслідуванні злочинів. У криміналістиці, як і в теорії оперативно-розшукової діяльності, загальним об'єктом дослідження вважають злочинну діяльність як певне соціальне явище. Предметом аналізу виступають закономірності, відносини, зв'язки й інші об'єктивні сторони, що характерні для об'єкта її дослідження. Криміналістика вивчає зв'язки механізму утворення інформації, що має криміналістичне значення, правила та процедури її пошуку, фіксації, оцінки й використання як фактичних даних для прийняття правильних процесуальних та оперативних рішень за фактами підготовки чи вчинення злочину й стосовно осіб, які причетні до нього.

Аналіз, незважаючи на його специфічність у криміналістиці, є логічним методом пізнання об'єктивної дійсності. Специфікою є те, що ця об'єктивна дійсність певною мірою пов'язана з подією злочину, його підготовкою, вчиненням, приховуванням слідів, протидією розслідуванню. Розрізняють два рівні криміналістичного аналізу: теоретичний і практичний. Останній безпосередньо пов'язаний із досудовим розслідуванням. Криміналістичний аналіз злочинів ґрунтується на концепції, згідно з якою кожний злочин правомірно розглядати як певну систему – сукупність взаємопов'язаних елементів, що мають внутрішні і зовнішні зв'язки. У тих випадках, коли невідомий який-небудь елемент цієї системи, він може бути встановлений шляхом дослідження та використання інформації про інші відомі елементи, що перебувають із ним у закономірному кореляційному зв'язку.

Стосовно завдання встановлення особи, яка вчинила комп'ютерний злочин, криміналістичному аналізу підлягає сукупність різноманітних об'єктів, що пов'язані з цим злочинним проявом. Встановлення й аналіз таких об'єктів дають змогу отримати дані щодо особи злочинця, способу його злочинних дій, застосованих для цього знарядь, обстановки та механізму вчинення злочину, матеріальних і віртуальних слідів як наслідків злочинних дій та інших обставин вчиненого. Проведення такого аналізу дає змогу визначити найдоцільніші напрями розслідування, завданнями яких є встановлення факту злочинного діяння та причетності до його вчинення конкретної особи.

Стосовно криміналістичного аналізу злочинів доцільно вести мову про аналіз складових злочинної діяльності та її наслідків, а також супутніх обставин, дослідження криміналістичних ознак яких має значення для виявлення, розкриття й здійснення розслідування з використанням засобів і методів криміналістики. Вчинення кожного з комп'ютерних злочинів – це завжди сукупність складних дій, що мають як кримінально караний, так і некримінальний характер.

Така злочинна діяльність породжує сукупність слідів, створюючи своєрідну слідову картину, в якій матеріальні та ідеальні сліди розосереджені в часі й просторі та не мають єдиного матеріального й ідеального носія. Крім того, ці сліди можуть відбивати різні сторони дій різних індивідів. Отже, слідова картина комп'ютерного злочину – це сукупність слідів та інших об'єктів, яка хоча й виявляється сучасними криміналістичними засобами, але у свідомості суб'єктів, що виявляють і розслідують злочин, формується як єдина система лише за наявності в особи розвинутого криміналістичного мислення.

У методиці розслідування комп'ютерних злочинів важливе значення має криміналістичний аналіз об'єктів цих злочинів. Адже специфіка таких об'єктів зумовлює й особливості методики розслідування злочинів цієї категорії. До того ж, мову треба вести не про об'єкт злочину як складову складу злочину в кримінально-правовому розумінні, а про ті комп'ютерні об'єкти, що мають відношення до вчинення злочину і можуть бути як об'єктами посягання, так і знаряддями вчинення злочинів. Злочинці використовують комп'ютер не як матеріальний предмет, що має вартість і завдяки цьому становить матеріальну цінність, а як носій чи технічну систему, що містить носії певної інформації, або ж використовують його як знаряддя доступу до операційної системи чи мережі з метою викрадення чужої інформації, спостереження за нею, внесення змін в інформаційні телекомунікаційні системи, або використовують комп'ютер для доступу до інших комп'ютерних засобів, мереж, систем із метою відповідного інформаційного впливу. Таке використання комп'ютера можна визнавати злочином лише в тому разі, якщо це завдає шкоди або порушує будь-чиї права щодо володіння й розпорядження інформацією. Характерною рисою комп'ютерної злочинності є її безпосередній зв'язок з інформаційною діяльністю, що пов'язана з використанням зловмисниками інформаційних технологій. Саме тому злочинні посягання на суспільні відносини, що базуються на використанні інформаційних технологій, спрямовані насамперед на завдання шкоди інформаційній безпеці соціальних систем чи об'єктів.

Одним із базових питань при розробленні науково обґрунтованих рекомендацій із розслідування злочинів у сфері інформаційних технологій є чітке з'ясування природи комп'ютерних об'єктів і, виходячи з цього, визначення закономірностей їх створення, збереження та використання, що само по собі має важливе криміналістичне значення. Розслідування таких злочинів пов'язане з дослідженням різних об'єктів, що становлять предмет дослідження оперативного співробітника, слідчого, прокурора чи судді. Багато які з об'єктів є традиційними в їх криміналістичному розумінні. Це й сліди рук, і сліди знарядь фізичного зламу, і сліди підробки документів на паперових носіях, і сліди нашарування речовин тощо. Проте розслідування злочинів цієї категорії завжди пов'язане з дослідженням специфічних об'єктів, які мають безпосереднє відношення до

створення, обробки, використання, вилучення чи копіювання інформації за допомогою засобів електронно-обчислювальної техніки та цифрового зв'язку. Правильне розуміння змісту застосовуваних понять дає можливість правильно визначити призначення, значущість і значення кожного з об'єктів, що застосовані злочинцем або є предметом його посягання чи допоміжними засобами у вчиненні комп'ютерних злочинів.

Виявлення та досудове розслідування комп'ютерних злочинів завжди пов'язані з пошуком, вилученням і дослідженням різних комп'ютерних об'єктів, зокрема й тих, що можуть бути визнані речовими доказами. Майже завжди певна, якщо не більша частка таких об'єктів стосується застосування інформаційних технологій. Вчинення злочинів із використанням комп'ютерної техніки в більшості випадків має на меті здійснення впливу на інформацію. До того ж, такий вплив здійснюється також комп'ютерною інформацією, що недосяжна для безпосереднього сприйняття й огляду без застосування відповідних засобів комп'ютерної техніки та програмного забезпечення. У слідчого виникає потреба збирання доказів, для чого використовуються такі об'єкти дослідження як комп'ютер, комп'ютерна мережа, телекомунікаційна мережа тощо. Дослідженню підлягає не просто предмет чи пристрій, а комп'ютерна інформація, що зберігається на конкретному комп'ютерному об'єкті як носієві. Найчастіше місцем знаходження такої інформації стають машинні носії, ЕОМ (комп'ютери), системи ЕОМ та комп'ютерні мережі, до того ж, у режимі безперервного функціонування. Питання належності конкретного електронного пристрою чи носія цифрової інформації до певного виду комп'ютерних об'єктів не є простим, як це могло б здаватися на перший погляд.

Щодо будь-яких об'єктів, що виявляються і вилучаються в процесі досудового розслідування та визнаються речовими доказами, мають бути враховані особливості їх збирання та дослідження, що пов'язані з їхнім агрегатним або структурним станом, їхніми розмірами та походженням. Комп'ютерні об'єкти можна розглядати лише як один із різновидів окремої групи речових доказів, специфіка яких зумовлена сферою використання з метою створення, обробки, накопичення чи передачі інформації в її електронному вигляді. Комп'ютерні об'єкти можуть бути речовими доказами у справі завдяки їхнім індивідуальним або системним властивостям лише в разі, якщо ці об'єкти були знаряддям злочину або зберегли на собі сліди злочину, а також, якщо вони можуть виступати засобами виявлення злочину або встановлення обставин вчинення й приховування злочину.

Всі речові докази мають бути оглянуті. Усі учасники огляду повинні сприйняти їхні характерні й індивідуальні властивості, а слідчий на підставі оцінки доказових властивостей кожного з об'єктів приймає рішення про визнання їх саме такими, про що складається постанова. Під час проведення процесуальних дій

можуть бути виявлені різні комп'ютерні об'єкти, фізичні властивості яких сприймаються зором, тактильно, але, на відміну від інших предметів матеріального світу, таким способом установити значущість предмета для доказування у кримінальному провадженні не можна. Для сприйняття інформації, що зберігається в комп'ютерних об'єктах, або для визначення їхньої здатності до створення чи оперування інформацією потрібне проведення специфічних досліджень та використання спеціального обладнання. Тобто, у разі вирішення питання щодо визнання комп'ютерного об'єкта речовим доказом потрібне застосування спеціальних апаратно-програмних комп'ютерних засобів і відповідних комп'ютерних методик. Лише їх застосування дасть можливість правильно сприйняти й оцінити сутність, значущість, належність до конкретного кримінального провадження таких об'єктів.

На практиці для встановлення змісту й сутності комп'ютерних об'єктів завжди звертаються до спеціаліста в галузі інформаційних технологій, за допомогою якого та з використанням відповідного комп'ютерного обладнання слідчий установлює властивості цих об'єктів або ж призначає відповідну комп'ютерно-технічну експертизу. Наприклад, магнітний носій, що містить шкідливу програму з комп'ютерним вірусом, зовні нічим не відрізняється від будь-якого іншого, що містить якусь нейтральну інформацію або навіть без будь-якої інформації. Виявити конкретні шкідливі властивості програми, що записана на звичайному магнітному носієві, простим зовнішнім оглядом навіть і за участю фахівця не можна. Для цього потрібні не тільки спеціальні знання, а й спеціальне комп'ютерне обладнання, а іноді – спеціальна методика розкриття й дослідження такої інформації. Велику кількість комп'ютерних об'єктів вивчає та досліджує сам слідчий, а для їх поглибленого дослідження призначаються судові експертизи. Речовими доказами стають лише ті з них, які відповідають загальновизнаним критеріям речового доказу. Але, беручи до уваги специфіку таких об'єктів, пов'язану з природою їхнього походження та потребою застосування засобів комп'ютерної техніки для оцінювання їхніх властивостей, у разі розслідування злочинів у сфері інформаційних технологій слід розглядати комп'ютерні об'єкти як різновид предметів матеріального світу, що можуть бути речовими доказами, знаряддями вчинення злочину або ж предметами злочинного посягання.

Поняття віртуальних об'єктів як предметів власності відоме вітчизняній і світовій цивілістиці, яка сьогодні вже вирішує питання правового регулювання відносин, пов'язаних із віртуальним майном, де право віртуальної власності відрізняють від права інтелектуальної власності за специфічним об'єктом, яким є віртуальне майно [7, с. 42; 8, с. 59–60].

Вважаємо, що запровадження такої категорії об'єктів у криміналістику й теорію кримінального процесу є своєчасним і відповідає реаліям сьогодення, що зумовлені впровадженням високих технологій у різні сфери суспільного життя, виробництва,

побуту. Виокремлення таких об'єктів з-поміж інших матеріальних предметів відбиває потребу застосування специфічних знарядь, прийомів і методів для їх сприйняття, дослідження й оцінювання. Це поняття можна вважати узагальнювальним і визначити поняття комп'ютерного об'єкта як певну категорію предметів, що є компонентами електронно-обчислювальних машин (комп'ютерів), автоматизованих інформаційних систем та інформаційних технологій, котрі використовуються для вирішення завдань машинної обробки інформації та мають значення для виявлення, розкриття, досудового розслідування, судового розгляду кримінальних справ і запобігання вчиненню злочинів у сфері інформаційних технологій.

Такі комп'ютерні об'єкти за їхніми властивостями та змістом, а також за зв'язками зі злочином можуть бути поділені на: електронні речові докази, електронні документи та апаратуру й обладнання. Ураховуючи криміналістичне значення таких об'єктів та їхній вплив на організацію й методику розслідування злочинів, усі комп'ютерні об'єкти на підставі їх криміналістичного аналізу можна класифікувати на окремі групи, взявши за основу такої класифікації криміналістичне значення інформації, носіями якої вони є. За цим критерієм комп'ютерні об'єкти можна виокремити в самостійні групи: інформаційні об'єкти; програмні об'єкти; комп'ютерно-апаратні об'єкти. В останній групі найважливіші в криміналістичному розумінні ті об'єкти, котрі є носіями інформації.

Висновки. Питання кібербезпеки та протидії кіберзлочинності з урахуванням постійного розширення сфери застосування сучасних інформаційних технологій набуває все більшого значення. Указом Президента України від 15.03.2016 № 96/2016 введено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», метою розробки якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Однією із загроз на цьому шляху є вчинення злочинів у сфері використання інформаційних технологій. У забезпеченні протидії такій загрозі важливу роль відіграє криміналістика, зокрема її розробки, спрямовані на своєчасне виявлення, розкриття та досудове розслідування злочинів, що вчинені з використанням засобів комп'ютерної техніки. Пропонуючи криміналістичні рекомендації з досудового розслідування злочинів, що вчинені з використанням комп'ютерних технологій, слід ураховувати розроблені на підставі криміналістичного аналізу спеціальні методики їх розслідування. Стосовно криміналістичного аналізу злочинів доцільно вести мову про аналіз складових злочинної діяльності та її наслідків, дослідження криміналістичних ознак яких має значення для виявлення, розкриття та проведення розслідування з використанням засобів і методів криміналістики.

У методиці розслідування комп'ютерних злочинів важливе значення має криміналістичний аналіз їхніх об'єктів, специфіка яких зумовлює й

особливості методики розслідування. Для сприйняття інформації, що зберігається в комп'ютерних об'єктах, потрібні проведення специфічних досліджень і використання спеціального обладнання, а в разі визнання комп'ютерного об'єкта речовим доказом необхідне застосування спеціальних апаратно-програмних комп'ютерних засобів і відповідних комп'ютерних методик. Беручи до уваги специфіку таких об'єктів, пов'язану з природою їхнього походження та потребою застосування засобів комп'ютерної техніки для оцінювання їхніх властивостей, слід розглядати комп'ютерні об'єкти як різновид предметів матеріального світу, що можуть бути речовими доказами, знаряддями вчинення злочину або ж предметами злочинного посягання. Запровадження такої категорії об'єктів у криміналістику й теорію кримінального процесу як окремих джерел доказів є своєчасним і відповідає реаліям сьогодення, що зумовлені впровадженням високих технологій у різні сфери суспільного життя, виробництва, побуту, а їх виокремлення з-поміж інших матеріальних предметів відбиває потребу застосування специфічних знарядь, прийомів і методів для їх сприйняття, дослідження та правильного оцінювання.

Список використаних джерел

1. International critical information infrastructure protection handbook 2008–2009 / Edited by A. Wenger, V. Mauer & M. Cavelty. Zurich : Center for Security Studies, 2009. 650 p.

2. Нашинець-Наумова А. Ю. Кібершпіонаж – загроза сучасному інформаційному суспільству. *Кібербезпека в Україні: правові та організаційні питання* : матеріали міжнар. наук.-практ. конф., (Одеса, 22 листоп. 2019 р.). Одеса : ОУВС, 2019. С. 11–13.

3. Духов В. Е. Экономическая разведка и безопасность бизнеса. Киев : ИМСО МО Украины ; НВФ «Студцентр», 1997. 176 с.

4. Колесник В. А., Гора І. В., Костін М. І. Розслідування комп'ютерних злочинів : наук.-метод. посіб. Київ : Вид-во НА СБ України, 2003. 124 с.

5. Обнорський В. І. Комп'ютерні злочини – способи та види. *Інформаційний бюлетень*. 2000. № 2. С. 14–20.

6. Про захист інформації в інформаційних телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286 (у редакції Закону № 2594-IV від 31.05.2005 із наступними змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 02.05.2021).

7. Некіт К. Г. Віртуальна власність: поняття та сутність. *Право і суспільство*. 2019. № 2. С. 37–42.

8. Майданик Л. Р. Віртуальний об'єкт як виклик для класичних підходів у речовому праві. *Теорія і практика інтелектуальної власності*. 2019. № 2. С. 59–64.

Аннотация. В статье рассмотрены вопросы криминалистического обеспечения противодействия совершению преступлений в сфере информационных технологий. Обращается внимание на то, что внедрение современных информационных процессов в разные сферы государственной деятельности, производства и общественные отношения кроме положительных результатов привело к увеличению фактов совершения преступлений с использованием цифровых технологий. Компьютерные преступления – это новое явление в общей преступности, поэтому требуется разработка современных мер по борьбе с ними. В этом процессе важна роль криминалистики, и прежде всего в подготовке рекомендаций по методике расследования компьютерных преступлений.

Криминалистический анализ преступлений в сфере информационных технологий, которые называют «компьютерными преступлениями», показывает, что их расследование отличается от расследования других преступлений. Во многом это связано с особенностью компьютерных объектов, которые могут быть и средствами совершения таких преступлений, и предметами преступного посягательства. Информация, которая хранится на компьютерных носителях, может быть воспринята и оценена исключительно с использованием компьютерного оборудования и цифровых технологий. Без этого невозможно установить лиц, причастных к преступлению, и получить нужные для раскрытия преступления доказательства. Для их изучения и оценки как источников доказательств нужно использовать помощь специалистов, средства компьютерной техники и сложное программное обеспечение. Это отличает их от других материальных объектов и дает основание вести речь о необходимости выделения компьютерных объектов в криминалистике и уголовном процессе в отдельную категорию источников доказательств.

Ключевые слова: информационные технологии, киберпреступность, криминалистика, досудебное расследование, компьютерные объекты, доказательства.

Abstract. The article deals with the issues of forensic support for preventing commission of crimes in the field of information technology. It is called to attention that although introduction of modern information processes in various spheres of government activities, production and public relations has brought positive results, it has also led to an increase in the cases of committing cyber crimes. Cyber crimes are a new phenomenon in general crime, therefore, the development of advanced techniques to combat them is required. In this process, the forensic science plays an important role, first of all, for the preparation of recommendations on methods for investigating cyber crimes. Forensic analysis of information technology crimes which are called cyber crimes indicates that their investigation is different from the investigation of other crimes. This is largely due to the fact that computer objects can be both means of committing such crimes and objects of criminal encroachment. Information stored on computer media can be perceived and evaluated solely by using computer equipment and digital technology. Without this, it is impossible to identify persons involved in committing a crime and obtain the evidence necessary to solve the crime. To study and evaluate them as sources of evidence, one needs to resort to the help of specialists, computer equipment and sophisticated software. It distinguishes computer objects from other material objects that is why it is necessary to put computer objects into a separate category of sources of evidence in forensic science and criminal procedure.

Key words: information technologies, cybercrimes, forensic science, pre-trial investigation, computer objects, proofs.