УДК 343.98:343.23:681.142.35

Теплицький Б. Б. – директор Державного науково-дослідного експертно-криміналістичного центру МВС України – керівник Експертної служби МВС України, м. Київ
ORCID: https://orcid.org/0000-0002-4820-5684

Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи

Мета *статті полягає у спробі розв'язати теоретичні та практичні проблеми, пов'язані із застосуванням інформаційних технологій безпосередньо в судово-експертній діяльності під час проведення комп'ютерно-технічних судових експертиз.* ***Методологія.*** *Для досягнення поставленої мети використано загальнонаукові та спеціальні методи, які є засобами наукового пошуку. Зокрема, метод системного аналізу, а також системно-структурний, формально-логічний і статистичний методи надали можливість проаналізувати генезис становлення та розвитку комп'ютерно-технічної судової експертизи, висвітлити сутність її завдань та особливості дослідження відповідних об'єктів як окремо, так і в комплексі.* ***Наукова новизна*** *обумовлена формуванням нового інструментарію в протидії злочинності. Виокремлено основні завдання комп'ютерно-технічної судової експертизи: діагностування апаратних засобів комп'ютерної системи; визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану системного й прикладного програмного забезпечення; пошук, виявлення, аналіз й оцінювання кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі. Класифіковано об'єкти комп'ютерно-технічної судової експертизи.* ***Висновки.*** *Узагальнено основні вимоги до запитань, які ставлять на вирішення експерта у відповідному виді експертиз. Проаналізовано помилки, яких найчастіше припускаються в кримінальних провадженнях слідчі й оперативні працівники під час підготовки об'єктів для дослідження, а також суди (слідчі судді), коли призначають комп'ютерно-технічні судові експертизи. Сформульовано перелік типових запитань, що можуть бути поставлені на вирішення експерта, а також загальні вимоги до об'єктів, які надсилають для проведення комп'ютерно-технічної судової експертизи.*

Ключові слова: судова експертиза; комп'ютерно-технічна судова експертиза; програмне забезпечення; апаратний об'єкт; програмний об'єкт; інформаційний об'єкт; помилка слідчого.

Вступ

Аналіз сучасної криміногенної ситуації та практики розслідування злочинів засвідчує сталу тенденцію до збільшення питомої ваги злочинів, що пов'язані з обігом комп'ютерної інформації, а також у яких комп'ютерні інформаційні системи є засобами та знаряддям учинення злочину або використовуються злочинцями для приховування факту й слідів злочинної діяльності, спрямування зусиль працівників правоохоронних органів на хибні об'єкти. Водночас слід констатувати, що зазначена тенденція цілком природна, оскільки процеси інформатизації суспільства позначаються й на такій сфері, як злочинна діяльність: з'являються нові види та способи злочинних посягань, пов'язаних із використанням комп'ютерних технологій, злочинність освоює інформаційний простір, середовище комп'ютерних мереж (Butuzov, 2010, p. 7).

Вирізняє злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку здебільшого латентний характер, вони не залишають видимої слідової картини на місці вчинення, є складними для виявлення й розкриття, що зумовлено, зокрема, як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним, у традиційному криміналістичному значенні, місцем учинення злочину – кібернетичним простором. Поділяючи думку науковців (Kopan, & Skulysh, 2012), кібернетичним простором ми вважаємо штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене внаслідок функціонування кібернетичних комп'ютерних систем управління й обробки інформації, що забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (Kopan, & Skulysh, 2012, p. 87-88).

Така злочинна діяльність має системний характер, набуває організованих форм, тому постає необхідність розроблення комплексу спеціальних сучасних знань і практичних навичок у різнорідних науково-технічних сферах, таких як електроніка, електротехніка, програмування, зв'язок тощо.

Ні слідчий, ні оперативний працівник з об'єктивних причин не можуть бути носіями таких спеціальних знань і навичок, а отже, не можуть ефективно провадити свою діяльність із виявлення та розкриття злочинів відповідної категорії без участі фахівця – носія таких

спеціальних знань і навичок. На практиці будь-які непрофесійні слідчі (розшукові), негласні слідчі (розшукові) дії та оперативно-розшукові заходи, що пов'язані з інформаційними мережами, комп'ютерними системами, носіями цифрової інформації, можуть призвести до їх руйнування, незворотної втрати, знищення або зміни цінної для органів розслідування розшукової інформації, втрати джерел доказів.

Безперечно, найважливішою процесуальною формою використання спеціальних знань у виявленні та розслідуванні злочинів, на думку Є. Г. Коваленка (Kovalenko, 2006), є судова експертиза – найбільш значуща та кваліфікована форма під час провадження доказування обставин злочину (p. 481).

Судова експертиза, відповідно до Закону України «Про судову експертизу» ("Zakon Ukrainy", 1994), – це дослідження на підставі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду (st. 1). Комп'ютерно-технічна судова експертиза (далі – КТЕ), акцентує В. Я. Колдін (Koldin, 2002), становить самостійний вид судових експертиз, що належить до класу інженерно-технічних, її проводять з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення й вивчення його слідової картини в розслідуваному злочині, а також одержання доступу до інформації на носіях даних з подальшим усебічним її дослідженням (Koldin, 2002, p. 161). Тільки КТЕ спроможна, забезпечивши отримання органами досудового розслідування унікальної розшукової інформації, створити відповідно до норм КПК України ("Kryminalnyi protsesualnyi kodeks", 2012) процесуальне джерело доказів – висновок експерта (ch. 2, st. 84). За таких умов невідкладними й найважливішими завданнями слідчих та оперативних працівників є пошук, фіксація, вилучення й надання експерту в непошкодженому вигляді матеріальних об'єктів – носіїв комп'ютерної інформації, що набувають статусу об'єктів експертного дослідження, і правильне визначення завдань КТЕ.

Отже, необхідність з'ясування завдань та об'єктів КТЕ актуалізується в контексті стрімкого розвитку та модернізації високих інформаційних технологій, які дедалі ширше застосовують представники кримінального середовища для вчинення злочинів, відповідає потребам як криміналістичної науки, так і правозастосовної практики правоохоронних органів.

Проблемні аспекти, пов'язані з протидією, виявленням і розслідуванням злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вивчали такі провідні вітчизняні науковці, як В. М. Бутузов, М. В. Гуцалюк, О. В. Копан, С. А. Кузьмін, В. І. Осадчий, М. А. Погорецький, Є. Д. Скулиш, О. А. Федотов, В. Г. Хахановський, Д. М. Цехан, В. П. Шеломенцев, О. М. Юрченко та ін.

Дослідники порушували різні питання, зокрема обробки ("Systemy obrobky", 2018) і захисту інформації, інформаційних ресурсів (Skulysh et al., 2011; Zybin, 2007), забезпечення інформаційної безпеки (Martynova, & Baranov, 2010), розглядали інформаційні технології (Stefanchuk, 2018), комп'ютерні системи (Shoroshev, & Khoroshko, 2007; Salnyk, Storchak, & Kramskyi, 2019), різні аспекти кіберзлочинності (Kharin, & Plotnikova, 2018; Huey, Nhan, & Broll, 2013), захисту інформації (Degtyareva, Miroshnykova, & Voloshko, 2019), висвітлювали проблеми цифрового криміналістичного аналізу (Carvey, 2015), експертизи комп'ютерних документів (Flynn, 2006) тощо.

Проте слід констатувати, що бракує ґрунтовних досліджень теоретичних і практичних питань, пов'язаних із застосуванням сучасних інформаційних технологій безпосередньо в судово-експертній діяльності під час проведення КТЕ, визначенням завдань та об'єктів КТЕ, що й актуалізує порушену проблематику.

Мета і завдання дослідження

Мета публікації полягає в окресленні в контексті діяльності судового експерта, з огляду на практику розслідування злочинів, пов'язаних з обігом комп'ютерної інформації, а також злочинів, у яких комп'ютерні інформаційні системи є засобами та знаряддями вчинення злочину, проблемних питань, пов'язаних з особливостями визначення завдань та об'єктів КТЕ, і в розробленні певних рекомендацій. Для досягнення поставленої мети необхідно: виокремити основні завдання, класифікувати об'єкти КТЕ відповідно до потреб практики, сформулювати перелік типових запитань, що можуть бути поставлені на вирішення КТЕ.

Виклад основного матеріалу

З огляду на сучасні потреби слідчої та оперативно-розшукової практики, досвід роботи відповідних підрозділів Експертної служби МВС, до основних завдань КТЕ, на нашу думку, слід віднести лише такі:

– діагностування апаратних засобів комп'ютерної системи;

– визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану пред-

ставленого програмного системного та прикладного забезпечення;

– пошук, виявлення, аналіз й оцінювання кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі.

У контексті застосування норм закону про кримінальну відповідальність доцільно зауважити, що поняття комп'ютерної (кібернетичної) інформації можна ототожнити з поняттям комп'ютерних даних, які, вважають В. М. Бутузов, С. А. Кузьмін і В. П. Шеломенцев (Butuzov, Kuzmin, & Shelomentsev, 2010), слід тлумачити як сукупність усіх даних, які обробляють в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, передають мережами електрозв'язку незалежно від засобу їх фізичного та логічного представлення, а також зберігають на електронних носіях інформації (Butuzov, Kuzmin, & Shelomentsev, 2010, p. 22).

Крім діагностичних, коли виконують КТЕ, традиційно можуть вирішувати й ідентифікаційні завдання (наприклад, ототожнення файлів з різних носіїв інформації).

Під час експертних досліджень комп'ютерних програм і компіляцій даних, зазначають Л. М. Головченко, А. І. Лозовий, Е. Б. Сімакова-Єфремян (Holovchenko, Lozovyi, & Simakova-Yefremian, 2016), використовують формально-логічні методи пізнання, а також набір програмно-технічних засобів для встановлення працездатності та функціональності комп'ютерних програм (Holovchenko, Lozovyi, & Simakova-Yefremian, 2016, p. 422).

Також варто зауважити, що погляд деяких учених (Koldin, 2002) щодо завдань КТЕ (Koldin, 2002, p. 163) досить дискусійний, оскільки занадто розширений через фактичну підміну завдань КТЕ конкретними прикладними питаннями, зумовленими окремими кримінальними провадженнями.

Систему об'єктів КТЕ становлять класи (які поділяють на види й підвиди), а саме:

апаратних об'єктів:

– персональні комп'ютери (у будь-яких варіантах виконання);

– периферійні пристрої до персональних комп'ютерів;

– мережеві апаратні засоби (сервери, робочі станції, комутатори, модеми, роутери й інше серверне обладнання);

– інтегровані системи (мобільні телефони тощо);

– будь-які комплектувальні всіх зазначених вище компонентів (апаратні блоки, блоки живлення, плати розширення тощо).

Ці види можуть поєднуватися. Безпосередньо в контексті криміналістики найважливіший підвид запам'ятовувальних пристроїв та інших носіїв інформації (електронних даних) – усі відомі на момент призначення експертного дослідження носії інформації (електронних даних): жорсткі диски, флеш-накопичувачі, диски для лазерних систем зчитування, карти пам'яті тощо. До апаратних об'єктів належать: системний блок; жорсткий диск; інші накопичувачі даних – гнучкі диски (5.25" і 3,5"), CD-ROM, магнітооптичні диски; сервер (на платформі Intel-процесорів або сумісних із ними); RAID-масиви; принтери (під час виконання комплексної експертизи разом із технічною експертизою документів);

програмних об'єктів:

– системне програмне забезпечення – комплекс програм, призначених для управління роботою обчислювальної системи, розподілу її ресурсів, підтримання діалогу з користувачами, надання їм допомоги в обслуговуванні комп'ютера, а також для часткової автоматизації розроблення нових програм. Системне програмне забезпечення поділяють на три основні складові: операційні системи, системи програмування, сервісні програми;

– прикладне програмне забезпечення – комплекс програм, призначених для виконання прикладних завдань фахової діяльності людини (виробничі, наукові, навчальні, розважальні тощо);

інформаційних об'єктів (електронних даних):

– текстові й графічні файли, створені з використанням комп'ютерів або мобільних пристроїв;

– аудіовізуальні (мультимедійні) дані;

– інформація у форматах баз даних та іншого прикладного програмного забезпечення.

До інформаційних об'єктів (даних) належать файли, підготовлені з використанням зазначених вище й інших програмних засобів – з розширеннями текстових форматів (.txt, .doc), графічних форматів (.bmp, .jpg, .tif, .cdr), форматів баз даних (.dbf, .mdb), електронних таблиць (.xls, .cal) тощо.

Складнощі в слідчій і судовій практиці виникають тоді, коли перед судовим експертом некоректно поставлено запитання. Тому, формулюючи їх, обов'язково дотримуються певних правил і рекомендацій, які ґрунтуються на класичних принципах криміналістики. Від того, наскільки компетентно формулюватимуть такі запитання, залежить і результат (повнота й об'єктивність) експертного дослідження.

Зокрема, поставлені перед судовим експертом запитання мають бути максимально конкретизовані, лаконічні, а також ґрунтуватися на попередньо встановлених слідчим процесуальним шляхом фактичних обставинах у кримінальному провадженні й не виходити за межі

спеціальних знань експертної спеціальності судових експертів, які здійснюють конкретну КТЕ. Їх слід розміщувати в логічній послідовності – спочатку ті, від вирішення яких залежатиме можливість вирішення інших.

Максимально повний і завершений перелік поставлених на вирішення експерта запитань становить передумову для забезпечення вичерпності висновку. Проте недопустимим є механічне відтворення в ухвалі про призначення експертизи загального списку запитань, які можуть вирішуватися КТЕ.

Крім того, перед судовим експертом не ставлять запитання, які, зважаючи на сучасний стан судово-експертної та криміналістичної науки, вирішити взагалі неможливо.

Отже, окреслимо основні вимоги, яких слід дотримуватися, формулюючи запитання для вирішення КТЕ.

Насамперед необхідно використовувати усталений понятійний апарат, не послуговуватися жаргонними й напівпрофесійними термінами (наприклад, «вінт», «логи» тощо). Потрібно застосовувати термінологію, визначену законами України, державними стандартами й іншими нормативно-правовими актами, а за браком такої – використовувати терміни, які використовують розробники технічних засобів, програмних продуктів у супровідній документації.

Запитання формулюють максимально чітко, щоб судовий експерт мав можливість надати однозначну відповідь. Вони не повинні стосуватися етапів дослідження інформації (опис характеристик носіїв інформації та особливостей розміщення інформації на них, відновлення й дослідження інформації серед знищених файлів є обов'язковим етапом дослідження інформації), мати довідкове, правове спрямування та виходити за межі компетенції судового експерта певної експертної спеціальності (спеціальних знань). Вони мають відповідати чинній методичній і технічній базі, доступній судовому експерту, бути спрямованими на встановлення конкретних обставин події, що належить до предмета доказування, формулюватися так, щоб витрати (фінансові, технічні, часові тощо) на проведення дослідження, коли виконують конкретні завдання розслідування, були мінімальні.

За результатами аналізу судово-експертної практики, слідчі судді, призначаючи, відповідно до змісту клопотань слідчих, КТЕ, припускаються типових помилок, унаслідок чого подовжуються терміни експертизи й ускладнюється або унеможливлюється її проведення. Зокрема:

– на експертизу надають об'єкти, які не містять і не можуть містити інформації, що має значення для доказування;

– однією ухвалою слідчого судді призначають судові експертизи за надмірною кількістю об'єктів, що фактично унеможливлює своєчасне та належне їх дослідження;

– однією ухвалою призначають експертизи за різними видами об'єктів (сервери та персональні комп'ютери або мобільні телефони й «планшетні» комп'ютери), для дослідження яких потрібно залучати відповідних спеціалістів;

– судовому експерту надають об'єкти, які з об'єктивних причин неможливо належно дослідити (через відсутність відповідних програмних й апаратних засобів і пристроїв).

Крім того, на вирішення судовому експерту не слід виносити запитання, які не мають змістовного навантаження, а також такі, що виходять за межі КТЕ, як-от:

– яка інформація міститься на носії;

– які файли та папки містяться на носії;

– який зміст інформації, що міститься на носії;

– яке цільове призначення інформації, що міститься на носії;

– чи міститься на конкретному електронному носії інформація про фінансово-господарську діяльність підприємств (суб'єктів господарської діяльності тощо);

– хто є користувачем комп'ютера;

– чи містить носій інформації програмне забезпечення з ознаками контрафактності (питання вирішують під час експертизи у сфері інтелектуальної власності);

– чи містить носій інформації відомості про втручання до автоматизованої системи.

Також необхідно зауважити, що перед судовим експертом, коли призначають КТЕ, не ставлять запитання про: правомірність дій користувачів; ліцензійність програмних продуктів; вартість комп'ютерної техніки та програмних продуктів, оскільки такі запитання належать або до компетенції виключно правозастосовного органу, або судових експертів з іншого виду експертиз. Експертна практика доводить, що об'єднання КТЕ з іншими видами експертиз у комплексну експертизу є недоцільним через її специфічність.

Для оптимізації навантаження на експертів за напрямом КТЕ, скорочення строків їх виконання й підвищення якісної значущості висновку експерта як джерела доказів у кримінальному провадженні пропонується запровадити такий алгоритм підготовчих заходів під час призначення КТЕ та розподілу навантаження на фахівців, зокрема Експертної служби МВС України.

Перед призначенням КТЕ (поданням клопотання слідчому судді) слідчому необхідно:

1. Провести попередній огляд об'єктів із залученням фахівців (зокрема Експертної служби

МВС України) для встановлення наявності даних, що можуть мати доказове значення в кримінальному провадженні, і вирішення питання про доцільність подальшого призначення експертизи.

2. Узгодити з фахівцями (судовими експертами) перелік запитань за конкретними об'єктами й оптимізувати їх кількість. Ставити такі запитання, які стосуються безпосередньо об'єктів дослідження в конкретному кримінальному провадженні, виключаючи запитання юридичного змісту й такі, вирішення яких не потребує спеціальних знань.

3. Визначати першочерговість і пріоритети дослідження наданих на експертизу об'єктів.

4. У разі об'єктивної необхідності дослідження значного обсягу різноманітної комп'ютерної техніки (понад 10 одиниць) варто призначати експертизи, поділяючи об'єкти дослідження на групи, або проводити окремі експертизи за кожним об'єктом дослідження.

З огляду на сучасні потреби органів досудового розслідування, можна сформулювати й *перелік типових запитань, що можуть бути поставлені на вирішення КТЕ:*

1. Чи в робочому стані системний блок, якщо ні, то які несправності він має?

2. Чи міститься на цьому носії інформація стосовно… (зазначити, яка інформація становить інтерес)?

3. Чи міститься на наданому на дослідження носії інформація з такими ключовими словами та словосполученнями: … (надати перелік ключових слів, словосполучень)? (До переліку ключових слів не включають так звані стоп-слова, що є послідовністю символів, які не мають змістового навантаження. Послуговуються такими словами, зокрема, в усіх найвідоміших документах, проте пошук за ними не дасть певних результатів (приклади стоп-слів: договір, угода, справа тощо).

4. Чи містить носій досліджуваного комп'ютера інформацію про дії користувача (зазначити, які саме)?

5. Чи могла бути створена ця інформація на наданому на дослідження комп'ютері, чи її перенесено на цей комп'ютер з носія цифрової інформації?

6. У який спосіб інформацію (зазначити, яку саме) перенесено на наданий на експертизу комп'ютер або носій цифрової інформації?

7. Якою є хронологія створення електронного документа, які інформаційні технології для цього використовували?

8. Якими є атрибути (дата, час створення, редагування, друкування, видалення тощо) файлів, що містять інформацію (зазначити, яку саме)?

9. Чи міститься на носіях інформації наданого на дослідження комп'ютера програмне забезпечення (зазначити, яке саме)?

10. Які саме функціональні несправності має надана на дослідження комп'ютерна система або її окремі складові, як ці несправності (у разі їх виявлення) впливають на роботу комп'ютерної системи загалом?

11. Чи наявне на носієві цифрової інформації електронне й поштове листування?

12. Встановити зміст журналу дзвінків, телефонної книги, смс-повідомлень наданого на дослідження стільникового (мобільного) телефона.

13. Встановити історію відвідування Інтернету за певний період.

14. Чи міститься на жорсткому диску, наданому на дослідження, інформація про відвідування інтернет-сайту (зазначити, якого саме)?

15. Чи міститься на наданих на дослідження об'єктах серед наявних і видалених файлів інформація про ключові слова (зазначити, які саме)? Якщо так, то які атрибути (дата й час створення, редагування, друкування, видалення тощо) файлів, що містять цю інформацію?

16. Чи містяться на наданих на дослідження об'єктах наявні та видалені файли документів формату «doc», «docx», «pdf» та електронних таблиць формату «xls», «xlsx»?

17. Чи містяться на наданих на дослідження об'єктах серед наявної та видаленої інформації графічні або відеофайли з ознаками порнографічної продукції? (Виключно в разі призначення комплексної комп'ютерно-технічної та мистецтвознавчої судової експертизи).

18. Чи містяться на наданих на дослідження об'єктах файли листів електронної пошти? У разі наявності скопіювати зазначену інформацію на окремий носій.

19. До яких веб-адрес Інтернету та коли здійснювали доступ з наданих на дослідження об'єктів?

20. Чи містяться на наданих на дослідження об'єктах облікові дані (логіни та паролі) для доступу до інтернет-ресурсів?

21. Чи встановлені на наданих на дослідження об'єктах програми, призначені для спілкування в Інтернеті (Viber, Skype, Telegram, WhatsApp тощо)? Якщо так, чи містять вони інформацію про історію повідомлень і дзвінків?

22. Чи міститься на наданих на дослідження об'єктах програмне забезпечення, призначене для віддаленого керування комп'ютером (TeamViewer, Ammyy Admin, Radmin, UltraVNC тощо)? Якщо так, чи містяться на наданих на дослідження об'єктах лог-файли використання виявлених програм?

23. Чи наявні на наданих на дослідження об'єктах програми (клієнти) для дистанційного банківського обслуговування на зразок «Клієнт-

Банк», «Інтернет-Банкінг»? Якщо так, чи містять вони лог-файли використання зазначених програм?

24. Чи міститься на наданих на дослідження об'єктах програмне забезпечення (зазначити назву або функціональне призначення, а також вид – встановлене чи невстановлене)? (Щодо грального бізнесу – iConnect, iChampion, G-slot, Gaminator, Superomatic, iGaming Casino, Megasuperomatic).

25. Чи можна виконати певні дії (зазначити, які саме) за допомогою цього програмного продукту?

26. Чи можна виконати завдання (зазначити, яке саме) за допомогою цього програмного продукту?

27. Чи реалізовано в цьому програмному продукті функції, передбачені технічним завданням на його розроблення?

28. Чи містяться на наданому на дослідження відеореєстраторі відеозаписи, створені в період (зазначити дату й час необхідних відеозаписів)? Якщо так, то виявлені відеозаписи скопіювати на окремий носій.

29. Чи міститься в пам'яті наданих на дослідження стільникових (мобільних) телефонів інформація про список контактів, журнал дзвінків, текстові та мультимедійні повідомлення, веб-історії, повідомлення в Інтернеті, а також текстові, графічні, відеофайли користувача? За наявності цієї інформації скопіювати її на окремий носій інформації.

Запропонований перелік запитань не є вичерпним. Він може розширюватися залежно від тих експертних завдань, що виникатимуть за певних обставин учинення злочину в конкретному кримінальному провадженні.

Щоб уникнути складнощів під час експертизи, сформулюємо загальні вимоги, яких мають дотримуватися сторони кримінального процесу, надсилаючи об'єкти дослідження на КТЕ. Зокрема, для дослідження інформації, що міститься на носіях цифрової інформації, експерту надають носій цифрової інформації, за необхідності – разом із системним блоком. Сторони кримінального провадження вживають заходів щодо забезпечення збереження носіїв цифрової інформації в робочому стані та їх відповідного пакування. Системні блоки персональних комп'ютерів пакують під час вилучення та надсилання для проведення експертизи так, щоб унеможливити потенційний доступ до носіїв цифрової інформації та підключення системного блока комп'ютера до електромережі.

У разі потреби встановити, застосовуючи КТЕ, факт робочого стану комп'ютерно-технічних засобів, судовому експерту в обов'язковому порядку мають надавати не тільки досліджувані засоби, а й відповідну технічну документацію виробника.

Наукова новизна

Наукова новизна цієї статті полягає в аналізі теоретичних і практичних проблем, пов'язаних із застосуванням інформаційних технологій у судово-експертній діяльності під час КТЕ. Реалізуючи поставлені завдання, слід зважати на такі чинники:

– сутність й основні завдання КТЕ;

– особливості дослідження відповідних об'єктів як окремо, так і в комплексі;

– діагностування апаратних засобів комп'ютерної системи, що має забезпечувати відповідна методика;

– визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану наданого системного та прикладного програмного забезпечення;

– пошук, виявлення, аналіз й оцінювання кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі;

– особливості класифікації об'єктів КТЕ;

– вимоги до запитань, що ставлять на вирішення експерта у відповідному виді експертиз;

– аналіз помилок, яких найчастіше припускаються в кримінальних провадженнях слідчі й оперативні працівники під час підготовки об'єктів для дослідження, а також суди (слідчі судді), коли призначають КТЕ;

– перелік типових запитань, що можуть бути поставлені на вирішення експерта, а також загальні вимоги до об'єктів, які надсилають для проведення КТЕ.

Висновки

Виокремлено основні завдання КТЕ, до яких належать: діагностування апаратних засобів комп'ютерної системи; визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану наданого програмного системного та прикладного забезпечення; пошук, виявлення, аналіз й оцінювання кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі.

З огляду на сучасні потреби органів досудового розслідування сформульовано перелік типових запитань, що можуть бути поставлені на вирішення КТЕ, а також загальні вимоги до об'єктів, які надсилають на КТЕ.

Підрозділи експертної служби МВС України у сфері КТЕ потребують оснащення сучасним апаратним і ліцензійним програмним забезпеченням. Слід розробляти та впроваджувати

автоматизовані робочі місця, які сприятимуть підвищенню ефективності досліджень як комп'ютерної техніки, виконаної на різних платформах, так й інших новітніх гаджетів. Водночас необхідно поширювати позитивний іноземний досвід у цій сфері.

КТЕ – порівняно новий вид експертизи, який потребує вдосконалення та впровадження відповідного науково-методичного забезпечення. Доцільно активізувати підготовку наукових публікацій із цієї тематики, у яких має бути висвітлено актуальні для практики питання розроблення усталеної термінології та, безперечно, результати ґрунтовних наукових досліджень, зокрема на дисертаційному рівні.

Застосування зазначених положень під час проведення слідчих (розшукових) і негласних слідчих (розшукових) дій, призначення КТЕ забезпечать належний рівень судово-експертної діяльності в кримінальних провадженнях щодо злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також розслідування споріднених видів злочинів.

REFERENCES

Butuzov, V.M. (2010). *Protydiia kompiuternii zlochynnosti v Ukraini (systemno-strukturnyi analiz) [Computer Crime in Ukraine (Structural Analysis)].* Kyiv: KYT [in Ukrainian].

Butuzov, V.M., Kuzmin, S.A., & Shelomentsev, V.P. (2010). *Naukovo-praktychnyi komentar do Kryminalnoho kodeksu Ukrainy. Osoblyva chastyna. Rozdil XVI. Zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku [Scientific and Practical Commentary to the Criminal Code of Ukraine. The special part. Section XVI. Crimes in the use of electronic computers (computers), systems and computer networks and telecommunication networks].* Kyiv: Palyvoda A.V. [in Ukrainian].

Carvey, H. (2015*). Windows Registry Forensics. Advanced Digital Forensic Analysis of the Windows Registry* (2nd ed.). doi: https://doi.org/10.1016/C2014-0-03973-1.

Degtyareva, L., Miroshnykova, M., & Voloshko, S. (2019). Analiz struktury systemy zakhystu informatsii [Analysis of the structure of the information security system]. *Systemy upravlinnia, navihatsii ta zviazku, Management, navigation and communication systems, 2(54),* 78-82. doi: https://doi.org/10.26906/sunz.2019.2.078 [in Ukrainian]

Flynn, W. (2006). The Examination of Computer-Generated Documents. *Forensic and Police Science Series,* 191-216. doi: https://doi.org/10.1201/9781420003765.ch16.

Holovchenko, L.M., Lozovyi, A.I., & Simakova-Yefremian, E.B. (2016). *Osnovy sudovoi ekspertyzy [Basics of forensic examination].* Kharkiv: Pravo [in Ukrainian].

Huey, L., Nhan, J., & Broll, R. (2013). Uppity civil iansand cyber-vigilantes: The role of the general publicin policing cyber-crime. *Criminology and Criminal Justice, 1(13),* 81-97. doi: 10.1177/1748895812448086.

Kharin, V.V., & Plotnikova, T.V. (2018). Kiberprestupnost kak ugroza mezndunarodnoi bezopasnosti [Cybercrime as a threat to international security]. *Aktualnye problemy gosudarstva i prava, Actual problems of state and law, 8(2),* 96-107 [in Russian]. doi: https://doi.org/10.20310/2587-9340-2018-2-8-96-107 [in Russian].

Koldin, V.Ia. (Eds.). (2002). *Veshchestvennye dokazatelstva: Informatsionnye tekhnologii protsessualnogo dokazyvaniia [Physical evidence: information technology procedural evidence].* Moscow: Norma [in Russian].

Kopan, O.V., & Skulysh, Ye.D. (Eds.). (2012). *Slovnyk terminiv z kiberbezpeky [Dictionary of cybersecurity terms].* Kyiv: Avanpost-Prym [in Ukrainian].

Kovalenko, Ye.H. (2006). *Teoriia dokaziv u kryminalnomu protsesi Ukrainy [Evidence theory in the criminal process of Ukraine].* Kyiv: Yurinkom Inter [in Ukrainian].

Kryminalnyi protsesualnyi kodeks Ukrainy: vid 13 kvit. 2012 r. No. 4651-VI [Criminal Procedure Code of Ukraine from April 13, 2012, No. 4651-VI]. (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon.rada.gov.ua/laws/show/4651-17 [in Ukrainian].

Martynova, O.P., & Baranov, V.L. (2010). Obespechenie informatsionnoi bezopasnosti i kachestva obsluznivaniia v kompiuternoi seti [Ensuring information security and quality of service in a computer network]. *Zakhyst informatsii, Protection of information, 4(49), vols. 12.* doi: https://doi.org/10.18372/2410-7840.12.1980 [in Russian].

Salnyk, S.V., Storchak, A.S., & Kramskyi, A.Ye. (2019). Analiz vrazlyvostei ta atak na derzhavni informatsiini resursy, shcho obrobliaiutsia v informatsiino-telekomunikatsiinykh systemakh [Analysis of vulnerabilities and attacks on state information resources processed in information and telecommunication systems]. *Systemy obrobky informatsii, Information processing systems, 2(157),* 121-128. doi: https://doi.org/10.30748/soi.2019.157.17 [in Ukrainian].

Shoroshev, V.V., & Khoroshko, V.O. (2007). Systemy vyiavlennia atak na kompiuterni systemy [Systems for detecting attacks on computer systems]. *Ukrainian Information Security Research Journal, 4(36), vols. 9.* doi: https://doi.org/10.18372/2410-7840.9.4124 [in Ukrainian].

Skulysh, Ye.D., Korchenko, O.H., Horbenko, Yu.I., Pushkarov, O.I., Soloviov, O.A., & Koriakov, I.V. (2011). Suchasni systemy zakhystu derzhavnykh informatsiinykh resursiv [Modern systems of protection of state information resources]. *Zakhyst informatsii, Protection of information, 4(53), vols. 13.* doi: https://doi.org/10.18372/2410-7840.13.2041 [in Ukrainian].

Stefanchuk, R. (2018). Informatsiini tekhnolohii ta pravo: quo vadis? [Information technology and law: quo vadis?]. *Pravo Ukrainy, Law of Ukraine, 1,* 30. doi: https://doi.org/10.33498/louu-2018-01-030 [in Ukrainian].

Systemy obrobky informatsii. (2018). *Information processing systems, 4(155), vols. 23.* doi: https://doi.org/10.30748/soi [in Ukrainian].

Zakon Ukrainy "Pro sudovu ekspertyzu": vid 25 liut. 1994 r. No. 4038-XII [Law of Ukraine "On Forensics" from February 25, 1994, No. 4038-XII]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12 [in Ukrainian].

Zybin, S.V. (2007). Model obiekta zakhystu informatsii i modeli kanaliv vytokiv informatsii [Model of information security object and model of information leakage channels]. *Ukrainian Information Security Research Journal, 4(36), vols. 9.* doi: https://doi.org/10.18372/2410-7840.9.4127 [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КИТ, 2010. 408 с.

Бутузов В. М., Кузьмін С. А., Шеломенцев В. П. Науково-практичний коментар до Кримінального кодексу України. Особлива частина. Розділ XVI. *Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*. Київ : Паливода А. В., 2010. 152 с.

Carvey H. Windows Registry Forensics. Advanced Digital Forensic Analysis of the Windows Registry. 2nd ed. 2015. doi: https://doi.org/10.1016/C2014-0-03973-1.

Дегтярьова Л. М., Мірошникова М. В., Волошко С. В. Аналіз структури системи захисту інформації. *Системи управління, навігації та зв'язку.* 2019. Т. 2 (54). С. 78–82. doi: https://doi.org/10.26906/sunz.2019.2.078.

Flynn W. The Examination of Computer-Generated Documents. *Forensic and Police Science Series.* 2006. P. 191–216. doi: https://doi.org/10.1201/9781420003765.ch16.

Головченко Л. М., Лозовий А. І., Сімакова-Єфремян Е. Б. Основи судової експертизи : навч. посіб. Харків : Право, 2016. 925 с.

Huey L., Nhan J., Broll R. Uppity civil iansand cyber-vigilantes: The role of the general publicin policing cyber-crime. *Criminology and Criminal Justice.* 2013. No. 1. Vol. 13. P. 81–97. doi: 10.1177/1748895812448086.

Харин В. В., Плотникова Т. В. Киберпреступность как угроза международной безопасности. *Актуальные проблемы государства и права.* 2018. № 8. Т. 2. С. 96–107. doi: https://doi.org/10.20310/2587-9340-2018-2-8-96-107.

Вещественные доказательства: Информационные технологии процессуального доказывания / под общ. ред. В. Я. Колдина. М. : Норма, 2002. 768 с.

Словник термінів з кібербезпеки / за заг. ред. О. В. Копана, Є. Д. Скулиша. Київ : Аванпост-Прим, 2012. 214 с.

Коваленко Є. Г. Теорія доказів у кримінальному процесі України : підручник. Київ : Юрінком Інтер, 2006. 632 с.

Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17.

Мартынова О. П., Баранов В. Л. Обеспечение информационной безопасности и качества обслуживания в компьютерной сети. *Захист інформації.* 2010. № 4 (49). Т. 12. doi: https://doi.org/10.18372/2410-7840.12.1980.

Сальник С. В., Сторчак А. С., Крамський А. Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційно-телекомунікаційних системах. *Системи обробки інформації*. 2019. № 2 (157). С. 121–128. doi: https://doi.org/10.30748/soi.2019.157.17.

Шорошев В. В., Хорошко В. О. Системи виявлення атак на комп'ютерні системи. *Ukrainian Information Security Research Journal.* 2007. № 4 (36). Т. 9. doi: https://doi.org/10.18372/2410-7840.9.4124.

Скулиш Є. Д., Корченко О. Г., Горбенко Ю. І., Пушкарьов О. І., Соловйов О. А., Коряков І. В. Сучасні системи захисту державних інформаційних ресурсів. *Захист інформації.* 2011. № 4 (53). Т. 13. doi: https://doi.org/10.18372/2410-7840.13.2041.

Стефанчук Р. Інформаційні технології та право: quo vadis? *Право України.* 2018. № 1. С. 30. doi: https://doi.org/10.33498/louu-2018-01-030.

Системи обробки інформації. 2018. № 4 (155). Т. 23. doi: https://doi.org/10.30748/soi.

Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12.

Зибін С. В. Модель об'єкта захисту інформації і моделі каналів витоків інформації. *Ukrainian Information Security Research Journal.* 2007. № 4 (36). Т. 9. doi: https://doi.org/10.18372/2410-7840.9.4127.

Стаття надійшла до редколегії 30.04.2019

Teplytskyi B. – Director of the State Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine – Head of the Expert Service of the Ministry of Internal Affairs of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4820-5684

Tasks, Objects and Computer Forensics Issues

*The **purpose** of this article is to attempt to address theoretical and practical issues related to the use of information technology directly in forensic activities when conducting computer forensics. **Methodology.** To achieve this goal, we use general scientific and special methods, which are the means of scientific search. In particular, the method of system analysis, as well as system-structural, formal-logical and statistical methods made it possible to analyze the genesis of the formation and development of computer-technical forensic examination, to reveal the essence of its tasks and the peculiarities of the study of relevant objects both individually and in complex. **Scientific novelty** is due to the formation of new tools in combating crime. The main tasks of computer-aided forensic analysis are distinguished: diagnostics of computer system hardware; determination of functional purpose, characteristics and realized requirements, algorithm and structural features, current state of the presented system and application software; search, detection, analysis and evaluation of cybernetic information (computer data) prepared by the user or created by programs for organizing information processes in the computer system. The objects of computer forensics are classified. **Conclusions.** The main requirements for the questions to be answered by the expert in the appropriate type of expertise are summarized. The mistakes most often made in criminal proceedings by investigators and operatives during the preparation of objects for investigation, as well as the courts (investigating judges) when appointing computerized forensics are analyzed. A list of common questions that can be asked by an expert is formulated, as well as general requirements for the objects that are submitted for the computer forensic examination.*

Keywords: forensic examination; computer-technical examination; software; hardware object; software object; information object; error investigator.