Розділ 15

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ ЦИФРОВИХ СЛІДІВ

15.1. Поняття, завдання та значення криміналістичного дослідження цифрових слідів

Виявлення, розкриття та розслідування деяких кримінальних правопорушень потребує з'ясування і фіксування операцій, здійснених із використанням електронно-обчислювальних пристроїв, зокрема мобільних телефонів, персональних комп'ютерів і ноутбуків, смартфонів, планшетів, ігрових приставок, серверів, роутерів, принтерів і копіювальної техніки, спеціалізованого обладнання, що має електронно-обчислювальні функції (промислові й виробничі станки, інженерне, медичне обладнання тощо). При цьому дії користувача можливо відслідкувати за змінами комп'ютерних даних, що утворюються в пам'яті електронно-обчислювальних пристроїв, які, зі свого боку, виступають специфічними цифровими слідами кримінального правопорушення.

Цифрові сліди – це будь-які криміналістично значущі дані, що залишаються в електронному середовищі внаслідок діяльності користувачів або систем (програм), а також у результаті взаємодії з цифровими пристроями, призначеними для отримання та оброблення інформації в цифровій формі. До таких даних можна віднести логи системи, дані з соціальних мереж, файли на комп'ютерах і мобільних пристроях, електронні листи тощо. У цьому плані цифрові сліди являють собою сліди вчинення будь-яких дій в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем і мереж, які можуть бути використані в кримінальному провадженні й судочинстві.

У науковому обігу й на практиці сьогодні використовують, крім поняття «цифрові сліди», також поняття «електронні сліди», «електронні (цифрові) сліди», «віртуальні сліди», «комп'ютерні сліди», «інфор-

маційні сліди», «комп'ютерно-технічні сліди». Убачається, що доцільним є використання терміна «цифрові сліди» як найбільш адаптованого до швидкого розвитку сучасних інформаційних і цифрових технологій, що дає змогу охопити різноманітні прояви (властивості) цього поняття. Такий підхід відображає його реальну технічну (цифрову) природу утворення і охоплює нові формати та джерела інформації, які можуть стати значущими в досудовому розслідуванні й судовому провадженні.

Дослідження цифрових слідів слідчим, прокурором, слідчим суддею і судом при здійсненні відповідно розслідування або судового провадження дає змогу встановити обставини вчиненого кримінального правопорушення та конкретно осіб, які його вчинили. Робота суб'єктів кримінального провадження із цими слідами вимагає новітніх підходів до їх виявлення, вилучення та дослідження, а сформовані на основі їх опрацювання цифрові докази – своєрідного порядку використання в кримінальному процесі й вирішенні завдань судочинства. Тому з накопиченням досвіду виявлення, вилучення та дослідження комп'ютерних (цифрових) даних почалося формування відповідної окремої галузі криміналістичної техніки – криміналістичного дослідження цифрових слідів.

Криміналістичне дослідження цифрових слідів **– це галузь криміналістичної техніки, яка досліджує закономірності й механізм утворення цифрових слідів і розробляє методи, прийоми, технології та техніко-криміналістичні засоби їх виявлення, вилучення і дослідження під час розкриття, розслідування, профілактики кримінальних правопорушень і судового розгляду.**

Будучи самостійною галуззю криміналістичної техніки, криміналістичне дослідження цифрових слідів має власний *предмет дослідження* – це закономірності утворення та відображення цифрових слідів кримінального правопорушення, а також методи, прийоми, технології та техніко-криміналістичні засоби виявлення, вилучення, дослідження та використання таких слідів. Криміналістичне дослідження цифрових слідів охоплює процеси виявлення, збирання, аналізу й оцінювання електронних (цифрових) даних, що залишаються в цифровому просторі в результаті використання цифрових пристроїв, технологій та інформаційних мереж, які можуть бути використані в досудовому розслідуванні й судовому провадженні.

Специфічними *об'єктами дослідження* цієї галузі криміналістичної техніки є цифрові сліди як результат слідоутворення і відображення процесу взаємодії користувача з комп'ютерною технікою, електронно-обчислювальні прилади (комп'ютерна техніка в широкому розумінні як невід'ємний елемент механізму утворення таких слідів), а також дії користувача (оператора) електронно-обчислювального приладу.

Криміналістичне дослідження цифрових слідів має тісні зв'язки з іншими галузями криміналістичної техніки, положеннями криміналістичної тактики, методики розслідування та судовими й іншими науками. Ця галузь криміналістичної техніки має міцні зв'язки з трасологією та криміналістичним дослідженням документів, оскільки цифрові сліди за своєю суттю поєднують ознаки матеріально фіксованих слідів і документів (у їх криміналістичному розумінні). Взаємовплив і зв'язок із криміналістичною тактикою простежується в тім, що криміналістичне дослідження цифрових слідів розробляє методи, прийоми, технології та техніко-криміналістичні засоби, що використовують під час проведення слідчих (розшукових) дій, спрямованих на виявлення, збирання, вилучення, дослідження та використання електронних (цифрових) даних, що залишаються в цифровому просторі як результат застосування цифрових пристроїв, технологій та інформаційних мереж під час учинення злочинної діяльності, яка виступає об'єктом дослідження криміналістики. Водночас ця новітня галузь криміналістичної техніки розробляє для криміналістичної методики прийоми, методи й засоби збирання доказів і доказування під час розслідування кримінальних правопорушень, учинених із використанням електронно-обчислювальної техніки[1].

Особливої значимості набувають зв'язки цієї галузі криміналістичної техніки з судовою експертологією, зокрема в контексті залучення спеціалістів і проведення судових експертиз. Для дослідження цифрових слідів призначають судову комп'ютерно-технічну експертизу, у якій виокремлюють такі види: експертиза комп'ютерної техніки (апаратно-комп'ютерна), експертиза програмних продуктів (програмно-

[1] Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. С. 111–116.

комп'ютерна), інформаційно-комп'ютерна експертиза, комп'ютерно-мережева експертиза[1].

Криміналістичне дослідження цифрових слідів також має тісні наукові зв'язки з іншими науками, зокрема комп'ютерно-технічними, інженерними, оскільки ця галузь криміналістичної техніки у свої дослідженнях ґрунтується на загальнотеоретичних положеннях цих наук, використовує та запозичує методи, прийоми й технології роботи із цифровими даними і їх носіями.

Перед криміналістичним дослідженням цифрових слідів постає низка завдань, які не можуть бути вирішені іншими галузями криміналістичної техніки. Такими ***завданнями*** є:

– вивчення та дослідження закономірностей і механізму утворення цифрових слідів, появу нових їх різновидів, зумовлених активним розвитком комп'ютерних, цифрових та інформаційних технологій, сучасних досягнень науки й техніки;

– розроблення і впровадження методів, прийомів, технологій та техніко-криміналістичних засобів виявлення, вилучення і дослідження цифрових слідів (доказів) під час розкриття, розслідування, профілактики кримінальних правопорушень і судового розгляду;

– удосконалення існуючих, розроблення та впровадження в практику інноваційних прийомів, методів, технологій і техніко-криміналістичних засобів, спрямованих для виявлення, фіксацію, вилучення та дослідження цифрових слідів, які можуть мати значення для ефективного вирішення завдань розслідування і забезпечення досягнення цілей судочинства;

– розроблення і пропонування методів, прийомів, технологій і техніко-криміналістичних засобів виявлення, вилучення і попереднього дослідження цифрових слідів кримінальних правопорушень;

– розроблення, формулювання і впровадження практичних рекомендацій щодо процесуального закріплення цифрових слідів кримінальних правопорушень і надання їм доказового значення;

– удосконалення наукових основ використання спеціальних знань у дослідженні цифрових слідів, особливостей призначення і проведен-

[1] Климчук М. П., Коміссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2022. С. 34–45.

ня судової комп'ютерно-технічної експертизи, оцінки її результатів і застосування їх у судовій практиці;

– вивчення, аналіз і дослідження причин та умов, що сприяли вчиненню злочинної діяльності з використанням цифрових технологій, розроблення на їх основі рекомендацій щодо ефективного використання методів, прийомів та техніко-криміналістичних і профілактичних засобів виявлення, фіксації та дослідження цифрових слідів (доказів);

– використання міжнародного досвіду щодо застосування методів, прийомів, технологій і техніко-криміналістичних засобів із метою ефективного виявлення, фіксації та дослідження цифрових слідів і цифрових доказів тощо.

Криміналістичне дослідження цифрових слідів передбачає виявлення цих даних, їх збереження в первісному вигляді, а також проведення аналізу для встановлення фактів, що мають значення для розслідування та судового розгляду.

Значення криміналістичного дослідження цифрових слідів полягає в такому:

1) **доказова база**: цифрові сліди можуть слугувати важливими доказами в кримінальних справах, даючи змогу встановити обставини вчинення кримінального правопорушення, ідентифікувати особу, яка його вчинила, та підтвердити показання;

2) **відстеження злочинної діяльності**: аналіз цифрових слідів може допомогти виявити злочинні схеми, фінансові потоки та зв'язки між особами;

3) **запобігання злочинності**: виявлення та аналіз цифрових слідів можуть бути використані для запобігання кримінальним правопорушенням завдяки моніторингу підозрілої активності.

15.2. Механізм утворення цифрових слідів і їх класифікація

Основою механізму утворення цифрових слідів є електромагнітні взаємодії між цифровими фізичними об'єктами й системами програмного управління ними, які взаємодіють у процесі оброблення та передачі інформації. Цей процес охоплює фіксацію взаємодії між цифровими пристроями та виявлення криміналістично значущої інформації.

Утворення цифрових слідів пов'язане в першу чергу не з фізичною присутністю певного об'єкта в конкретному місці, що, наприклад, є характерним для матеріально фіксованих слідів (слідів ніг, транспортних засобів), і контактуванням поверхонь, а з його взаємодією з цифровими засобами й технологіями. Так, навіть одноразове відвідування певного вебсайту або застосунку залишить інформацію щодо часу й тривалості відвідування, IP-адреси користувача, типу браузера й операційної системи, а також подробиці здійснених операцій (кліки по лінках, пошукові запити чи введення даних у форми, реєстраційна інформація) тощо. Також залежно від налаштувань відповідного пристрою та застосунків можуть залишатися дані щодо місцезнаходження користувача навіть у режимі реального часу. Така інформація може бути використана для встановлення та аналізу місць перебування, проживання, роботи, відвідуваних місць і шляхів переміщення. Тобто будь-яка діяльність особи в мережі Інтернет або із застосуванням цифрових технологій і пристроїв, незалежно від фактичного її місця перебування, залишає дані, які можуть бути використані для ідентифікації особи, установлення місцезнаходження, відстеження її поведінки, соціальних зав'язків, виявлення звичок, послідовності певних подій і діяльності, моніторингу фінансових та інших видів операцій тощо. При цьому такі сліди залишаються не на якійсь поверхні, а в цифровому просторі, який охоплює не лише мережу Інтернет, а й інші джерела цифрової інформації (комп'ютери, планшети, ноутбуки, смартфони тощо)[1].

Механізм утворення цифрових слідів можна пояснити тим, що практично всі сучасні комп'ютери використовують математичні алгоритми й комбінації цифр (найчастіше – бінарний код, поєднання 0 та 1) як універсальний засіб кодування, збереження і передавання будь-якої інформації. Цифрову форму кодування прийнято протиставляти більш старій і менш поширеній аналоговій, за якої дані передаються через коливання фізичних показників струму, світлового потоку, радіохвиль тощо. Крім того, використання терміна «цифровий слід» дає змогу максимально охопити різноманітні прояви цього явища й відображає його реальну технічну природу утворення. Тобто цифровий формат таких даних підкреслює не лише форму існування, а й сутність таких

[1] Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 85, ч. 4. С. 74.

слідів, що обґрунтовує доцільність використання терміна «цифрові сліди»[1].

Цифрові сліди можна знайти під час аналізу комп'ютерного обладнання, операційних систем, програм, антивірусів і програмного коду. Коли цифрові пристрої (наприклад, комп'ютери, смартфони) обмінюються даними через мережу, вони створюють цифрові сліди, які можуть фіксуватись у вигляді логів, записів або інших цифрових форм.

При виконанні різних дій на пристроях, таких як збереження файлів, відправлення повідомлень або перегляд вебсторінок, генеруються дані, які також залишають сліди в системах. Взаємодія апаратного забезпечення (мікросхеми, електронні елементи) з програмним забезпеченням (операційні системи, додатки) дає змогу обробляти, зберігати й передавати інформацію, створюючи цифрові сліди.

Об'єкти, які генерують і сприймають цифрові сліди, мають реальну матеріальну природу. Це означає, що вони існують у фізичному світі й можуть бути представлені у вигляді апаратних засобів, таких як комп'ютери, смартфони, обладнання телекомунікаційних мереж, сервери, цифрові фото- й відеокамери та інші цифрові пристрої. Ці об'єкти взаємодіють між собою через електромагнітні сигнали, що дає їм змогу обмінюватися даними та створювати цифрові сліди внаслідок своєї діяльності. Важливо, що такі об'єкти не лише створюють інформацію, а й сприймають її, зберігаючи й обробляючи у формі, яка може бути використана для подальшого аналізу або розслідування.

Цифрові сліди виникають унаслідок зовнішнього втручання в комп'ютерні системи, яке має на меті знищення, копіювання або модифікацію інформації, а також блокування їхньої роботи. Це може проявлятися у видаленні файлів із каталогів, що ускладнює їх відновлення, або в модифікації записів у базах даних, що призводить до спотворення інформації. Фізичне пошкодження носіїв даних, наприклад їх руйнація або розмагнічування, перешкоджає доступу до інформації і може призвести до її безповоротної втрати. Зміна імен каталогів і файлів може викликати плутанину в структурі даних, ускладнюючи

[1] Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. С. 113.

їх пошук, тоді як зміна вмісту файлів, зокрема їх розміру, також ускладнює ідентифікацію.

Крім того, зміна атрибутів файлів, наприклад прав доступу, впливає на їх використання, а поява нових каталогів і файлів може бути наслідком несанкціонованих дій. Зміна інформації про час останнього доступу до даних ускладнює дослідження і відстеження дій у системі. Також важливими є сліди, що залишають антивірусні або тестові програми, оскільки вони можуть надати цінну інформацію під час розслідувань. Усі ці цифрові сліди є важливими для криміналістичного аналізу, оскільки допомагають відновити події, що призвели до втручання в систему, і виявити причетних.

Цифрові сліди в більшості випадків супроводжуються ***метаданими*** (від давньогрец. *μετά* – після, за межами та англ. *data* – дані), тобто додатковою інформацією, що характеризує основні комп'ютерні дані. Метадані характеризують файл («контейнер» для даних) або папку-каталог їх індексації і можуть зберігатись як разом з основними даними, так і окремо від них. Перелік і зміст метаданих залежить від операційної системи, типу файлу та програмного забезпечення, з яким файл асоційовано. Такі дані мають обов'язково фіксуватися під час вилучення та дослідження цифрових слідів. В операційних системах «Microsoft Windows» метадані файлу можна відобразити на екрані за кліком по ньому правою кнопкою миші й вибором опції «Властивості». Основними метаданими є розмір файлу (міра кількості даних, базовою одиницею є байт), назва, розширення назви (наприклад *.doc,*.exe), назва асоційованого програмного забезпечення, каталог розташування, час створення, час останнього редагування, час останнього відкриття, кількість редакцій, найменування користувача, який створив чи останнім редагував файл тощо[1].

Отже, цифрові сліди формуються в результаті складного процесу взаємодії апаратних і програмних компонентів цифрових пристроїв, що відбувається під час їхньої роботи.

Цифрові сліди, що утворюються під час учинення кіберзлочинів – це інформація, яка зафіксована в цифровому форматі, міститься в різ-

[1] Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. С. 115.

ного роду цифрових пристроях зі створення, оброблення, збереження та передачі цієї інформації, причинно пов'язана з подією кіберзлочину та дає змогу встановити як обставини вчиненого правопорушення, так і особу кіберзлочинця. Тому під ***цифровим слідом*** варто розуміти дані, що залишаються в цифровому просторі внаслідок використання цифрових пристроїв, технологій та інформаційних мереж, які можуть бути використані в кримінальному провадженні й судочинстві.

Основними властивостями цифрових слідів є:

а) технологічність (така властивість формування цифрових слідів зумовлена передусім цифровою формою існування, відсутністю традиційної матеріальної форми, а також специфікою реалізації інформаційно-телекомунікаційних технологій, оскільки для перетворення цифрових слідів у доступну для сприйняття форму також використовують зазначені технології);

б) висока швидкість трансформації (за певних умов цифрові сліди легко знищуються чи модифікуються, саме тому навіть незначне зволікання з фіксацією виявлених цифрових слідів може спричинити їх утрату);

в) здатність до відтворення та поширення (цифрові сліди можуть бути представлені практично нескінченною кількістю ідентичних копій, легко можуть бути передані через комп'ютерні мережі й бути доступними в будь-якій точці, де є підключення до мережі Інтернет);

г) неможливість безпосереднього сприйняття органами чуття, тобто підлягають виявленню та дослідженню тільки за допомогою використання певного обладнання та/або спеціалізованого програмного забезпечення;

ґ) багатокомпонентність і складність інформаційної структури цифрових слідів (така властивість зумовлена тим, що цифрові сліди не мають фізично цілісної структури, адже вони можуть складатися з великої кількості окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох фізичних носіях цифрової інформації). Крім цього, поряд зі значущою кримінально релевантною інформацією міститься значний обсяг допоміжних даних, що відповідають за цілісність і доступність цифрової інформації, що й зумовлює складність інформаційної структури цифрого сліду;

д) можливість підтвердження контрольними числами (хеш-сумами) або іншими даними, що свідчать про їх цілісність, оскільки для пере-

вірки цілісності даних використовують механізм розрахунку контрольної суми або хеш-суми. Перелік таких властивостей може змінюватися та розширюватися залежно від виду цифрового сліду й джерела його походження.

Класифікація цифрових слідів може здійснюватися за різними критеріями, ураховуючи їх походження, характер, мету використання та інші класифікаційні ознаки.

1. За походженням:

– цифрові сліди, що утворюються в процесі нормальної роботи систем (лог-файли, записи сеансів);

– сліди, що виникають унаслідок несанкціонованого втручання (видалення, модифікації даних).

2. За характером:

– технічні – містять дані, що стосуються роботи системи (зміни в конфігураціях, операційних системах);

– контентні – містять інформацію, що стосується самих даних (уміст файлів, повідомлень).

3. За формою:

– фізичні сліди, що залишаються на фізичних носіях інформації (пошкодження, знищення носіїв);

– логічні сліди, що фіксуються в програмному забезпеченні (зміни в базах даних).

4. За доступом:

– публічні сліди, доступні для загального перегляду (пости в соціальних мережах);

– приватні сліди, що зберігаються в закритих системах (внутрішні бази даних, зашифровані файли).

5. За місцем розташування носія цифрових данних:

– сліди, що містяться на локальних носіях;

– сліди, що містяться на віддалених носіях.

15.3. Виявлення, вилучення та дослідження цифрових слідів

Цифрові сліди відображаються в кіберпросторі й не мають традиційної матеріально фіксованої форми, чим ускладнені їх виявлення,

фіксація та дослідження. Вони містять метадані, тобто фактично є інформацією про інформацію про її автора, дату, час створення, зміни, переміщення та її видалення. Дослідження цифрових слідів потребує не лише додаткових експертних знань, а й спеціального програмного забезпечення.

Необхідно враховувати специфічні властивості цифрової інформації та з урахуванням цього залучати експертів-криміналістів і спеціалістів до проведення слідчих (розшукових) дій, під час яких можуть бути виявлені цифрові сліди, оскільки через неправильне їх виявлення та вилучення вони можуть бути пошкоджені (знищені). Також слід ураховувати, що деякі цифрові сліди можуть бути недоступними для дослідження під час судового розгляду, тому вони потребують розшифрування та відтворення у звичній графічній, текстовій або звуковій формі у висновку експерта.

Процес виявлення, вилучення та дослідження цифрових слідів має істотне значення, оскільки на кожному із цих етапів можуть бути внесені зміни в цифрові сліди, а також сліди можуть зникнути. Період зберігання цифрових слідів може бути нетривалим, тому необхідно вживати оперативних заходів для їх фіксації. При цьому важливим є те, щоб такі дії були завчасно спланованими й кваліфікованими із обов'язковим знанням усіх властивостей цифрових доказів, оскільки при некоректному збиранні, зберіганні та поводженні цифрові сліди можуть утратити свою доказову цінність. Залежно від носія інформації вилучення може здійснюватися через безпосереднє вилучення, а в інших – лише через копіювання інформації.

Особливої уваги вимагає процес виявлення. Можна виокремити чотири слідчі ситуації залежно від того, чи був увімкнений носій цифрових слідів самим володільцем та необхідності долати логічний доступ[1] до даних: 1) носій цифрових слідів був у розпорядженні володільця та слідчий, не здійснюючи повторного входу, почав їх фіксувати; 2) носій цифрових слідів був вимкнений та для подальшого збирання інформації був увімкнений; 3) доступ до носія вимагає подолання логічного доступу; 4) відсутня необхідність розблокування носія для отримання доступу до інформації на носії. Це є важливим з огляду на те, що ідентифікаційні дані, за якими надалі будуть уста-

[1] Логічний доступ стосується програмних засобів, які контролюють або обмежують доступ до даних (паролі, інші засоби автентифікації, шифрування тощо).

новлювати ідентичність, можуть змінюватися після кожного входу до системи. Ознаки несанкціонованого доступу зазвичай зберігаються в журналах операційних систем і спеціальних програм, які фіксують виконані дії, зберігають резервні копії файлів і створюють звіти. Слід звертати увагу на розбіжності між обсягом попередніх даних і даних з урахуванням появи стороннього програмного забезпечення, а також співвідношення часу появи попередніх даних і стороннього програмного забезпечення. Ці журнали містять інформацію про останні дії на комп'ютері, яка може стати важливою для розслідування.

Тому важливо розглядати можливість фіксації не лише цифрових слідів, але й традиційних, таких як відбитки пальців, фізичні електронні носії (флешнакопичувачі, жорсткі магнітні диски).

Аналіз цифрових слідів, зокрема інформації про конфігурацію браузера зловмисника, може допомогти в ідентифікації цифрового пристрою, з якого здійснювалося несанкціоноване втручання. Ця інформація може містити IP-адреси, версії програмного забезпечення та інші метадані, що надають цінні підказки для слідства. Дослідження цих слідів не лише сприяє виявленню злочинців, але й дає змогу відновити послідовність подій, що призвели до кримінального правопорушення. Тому детальний аналіз журналів і резервних копій є важливим етапом.

Перед пошуком цифрових слідів спеціалісту рекомендовано створити криміналістичну копію (образ e.01) носія (наприклад, жорсткого диска), з яким він працюватиме. Це дасть змогу забезпечити збереження та незмінність цифрових слідів на основному носії. Після цього фахівець може відновити резервні копії системи, лог-файли, дампи оперативної пам'яті, дампи мережевих трафіків, інші файли або їх частини (у разі пошкодження) як наявні, так і видалені, а також службову інформацію про ці файли тощо. Потім спеціаліст аналізує сукупність знайдених цифрових слідів і вибудовує з прив'язкою до часу архітектуру діяльності користувача ЕОМ щодо операцій, які здійснювалися з певними файлами і програмами (установлення, видалення, зміна), про роботу в локальній мережі або мережі Інтернет.

За відсутності доступу до фізичного носія (наприклад, у випадку фіксації даних з інтернету) рекомендовано: 1) фіксацію даних через огляд інформації в порядку ст. 237 КПК України з дотриманням вимог ч. 4 ст. 99 КПК України; 2) термінове зберігання даних згідно з про-

цедурою Будапештської конвенції з подальшим скеруванням запиту в порядку ст. 548 КПК України.

Усі дії, пов'язані з пошуком, виявленням, фіксацією та вилученням цифрових слідів кримінальних правопорушень, повинні відповідати міжнародним стандартам щодо ідентифікації, збирання, отримання та збереження цифрових доказів (зокрема ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»).

Це має суттєве значення під час аналізу цифрових слідів у мережі Інтернет, експерт може не мати змоги охопити та зберегти весь необхідний трафік. Також цифрові сліди можуть бути розпорошені між різними фізичними або віртуальними місцями, такими як онлайнові соціальні мережі, криптовалютні гаманці, механізм CaaS, хмарні ресурси й певний електронно-обчислювальний пристрій, підключений до персональної мережі. Тому ефективність пошуку, виявлення, фіксації та вилучення цифрових слідів кримінальних правопорушень потребує досконалого знання та практичних навичок роботи з комп'ютерним і телекомунікаційним обладнанням, а також спеціалізованим програмним забезпеченням, що забезпечить найбільш ефективне його застосування під час пошуку, фіксації, вилучення та подальшого дослідження і зберігання цифрових слідів.

Способи фіксації цифрових слідів: 1) опис у протоколі (основний спосіб); 2) фотографування, відеозапис, скріншоти; 3) копіювання. Скріншоти забезпечують статичну копію виявлених цифрових слідів, які згодом можуть бути змінені або видалені з інтернету, що гарантує слідчим наявність надійного посилання на оригінальний матеріал. Це особливо важливо у випадках, коли вміст є чутливим або схильним до змін.

З метою виявлення та фіксації відомостей щодо обставин учинення кримінального правопорушення слідчий, прокурор проводять огляд речей, документів і комп'ютерних даних. Огляд комп'ютерних даних проводить слідчий, прокурор, відображаючи в протоколі огляду інформацію, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або в паперовій формі).

Згідно з Конвенцією про кіберзлочинність до комп'ютерних даних віднесено будь-яке представлення фактів, інформації або концепцій

у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою (ст. 1)[1].

Визнання скопійованих слідчим, прокурором цифрових слідів, у тому числі комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, судом як оригіналу потребує залучення спеціаліста під час проведення огляду (ч. 4 ст. 99 КПК України). Це дає змогу використовувати такі копії під час судового розгляду нарівні з оригіналами.

Фізичне вилучення цифрової інформації не завжди є процедурно чи технічно можливим, тому копіювання вважають ефективним способом отримання доказів із відповідних електронних носіїв або з інтернету.

До спеціалізованих засобів для виявлення та аналізу цифрових слідів у кримінальних правопорушеннях належать такі інструменти: 1) програмне забезпечення для криміналістичної експертизи комп'ютерних носіїв інформації, наприклад «X-Ways Forensics», «EnCase Forensic», «Belkasoft Evidence Center», «Forensic Toolkit»; 2) мобільні комплекси для вилучення, декодування та аналізу даних із мобільних пристроїв, як-от «MSAB XRY Field», «MOBILedit Forensic Express Pro», «Cellebrite UFED Touch 2»; 3) програмне забезпечення для відновлення комп'ютерних даних, зокрема «UFS Explorer», «RStudio» та інші[2].

Після виявлення цифрових слідів їх необхідно сфотографувати, а потім описати в протоколі огляду. У протоколі зазначають: де саме виявлено цифрові сліди і їх місцезнаходження; розташування цифрових слідів в об'єкті; метадані та хеш-код; вид сліду; розміри й інші властивості кожного із цифрових слідів; які способи виявлення і фіксації використовувалися; як саме скопійовано та збережено цифрові сліди.

Збереження метаданих надає важливу інформацію про файл, наприклад, дату створення, програмне забезпечення, за допомогою яко-

[1] Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575.

[2] Омельян О. С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза.* 2020. Вип. 65. С. 457–466.

го його було створено, і будь-які внесені зміни. Аналіз метаданих за допомогою програм, таких як «MediaInfo», дає змогу слідчим підтвердити походження, наприклад, відео, та виявити можливі спроби фальсифікації.

Розрахунок і збереження хеш-коду дає змогу створити контрольну точку для перевірки цілісності файлу в майбутньому. Якщо файл буде змінено, хеш-код зміниться, що вкаже на можливу маніпуляцію. Цей крок є ключовим для забезпечення того, щоб докази залишалися незмінними з моменту їх збирання.

Збереження файлів і пов'язаних із ними метаданих на оптичному диску або флешносії як додаток до протоколу забезпечує збереження даних у стабільному й незмінному форматі. Цей метод зберігання додає рівень безпеки й гарантує збереження доказів у форматі, що є надійним і доступним у довгостроковій перспективі.

Окремо слід зазначити з приводу копіювання (завантаження) та збереження **відео з YouTube** та інших подібних платформ. Збереження таких динамічних цифрових слідів, як відео в його початковій формі, дає змогу уникнути ризику видалення або модифікації з боку автора чи платформи. Також **архівування вебсторінок** дає змогу зберегти знімок вебсторінки в конкретний момент часу. Це особливо важливо для фіксації цифрових слідів, оскільки вміст вебсторінок може бути легко змінений або видалений. Архівування вебсторінок гарантує доступ до незміненої версії сторінки навіть після того, як оригінал був змінений або видалений.

Отже, на сьогодні виявлення, розслідування та розкриття значної кількості кримінальних правопорушень потребує виявлення, збирання, дослідження та використання цифрових слідів. Якщо здійснюється опрацювання зібраних цифрових слідів у певних програмах і системах, то постає питання захисту даних.

15.4. Підготовка та призначення судових експертиз для дослідження цифрових слідів

Підготовка до проведення різних видів експертиз має кілька ключових етапів, які забезпечують точність і достовірність результатів

дослідження. Важливим є формулювання питань, які необхідно вирішити за допомогою експертизи, а також надання вилучених цифрових слідів і забезпечення їх належного зберігання та транспортування для уникнення пошкодження або фальсифікації, а також визначення компетентної судово-експертної організації, якій буде доручено її проведення. Для проведення комп'ютерно-технічної експертизи слід підготувати належні об'єкти на дослідження та процесуальні документи: 1) сам комп'ютерний носій, а за потреби комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій), технічна документація до них, наявні захисні механізми (паролі, шифрування тощо); 2) постанову слідчого чи прокурора про доручення проведення експертизи або ухвалу слідчого судді; 3) протокол огляду (інші матеріали кримінального провадження).

Необхідно забезпечити збереження носіїв інформації в робочому стані за допомогою їх пакування в окремі пакети. При цьому системні блоки персональних комп'ютерів пакують таким чином, щоб унеможливити доступ до носіїв інформації або підключення до мережі живлення. При підготовці програмних продуктів необхідно надати носій із копією досліджуваного програмного продукту або програмного коду.

З метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки.

Сутність комп'ютерно-технічної експертизи. Комп'ютерно-технічна експертиза є різновидом інженерно-технічної, яка спрямована на дослідження комп'ютерної техніки, серверів, інших електронних пристроїв, програмного забезпечення, інформаційних систем і аналізу логів системи, історії браузера та інших даних користувача з метою встановлення істотних фактів і обставин, що підлягають доказуванню в межах кримінального провадження.

Основними завданнями комп'ютерно-технічної експертизи є:

– установлення робочого стану комп'ютерно-технічних засобів (перевірка працездатності комп'ютерних систем і їх компонентів; виявлення можливих несправностей та оцінка їх впливу на функціональність системи);

– установлення обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечен-

ня (аналіз дій користувачів щодо використання комп'ютерів і програмного забезпечення; дослідження історії використання системи і її компонентів);

– виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях (відновлення видалених або зашифрованих даних; аналіз структури та змісту даних на носіях інформації);

– установлення відповідності програмних продуктів певним версіям чи вимогам на його розроблення (перевірка відповідності програмного забезпечення технічним завданням; оцінка відповідності версії програмного продукту встановленим вимогам).

За допомогою цього виду експертизи можна дослідити вміст носія на предмет наявності конкретної інформації та/або конкретного програмного забезпечення на комп'ютері, проаналізувати журнали подій та історії дій користувача на комп'ютері, виявити сліди видалення даних або форматування носія, установити джерела походження даних, проаналізувати шляхи передачі даних, установити технологічні процеси та час створення документа, його метаданих файлів для встановлення їх історії, а також оцінити технічний стан обладнання та вплив несправностей на його роботу, проаналізувати функціональні можливості програмного забезпечення, оцінити відповідність програмного продукту для виконання конкретних завдань, перевірити відповідність функціональних можливостей програмного забезпечення технічному завданню.

Для вирішення цих завдань можуть бути поставлені такі запитання.

1. Чи міститься на даному носії інформація стосовно [указати, яка інформація цікавить] і в якому вигляді?

2. Чи містить носій досліджуваного комп'ютера інформацію про певні [указати, які саме] дії користувача?

3. Чи піддавався досліджуваний накопичувач певним процедурам із метою знищення інформації?

4. Чи могла бути створена зазначена інформація на цьому комп'ютері, чи вона перенесена з іншого носія?

5. Яким чином інформація [указати, яка саме] перенесена до досліджуваного комп'ютера (носія)?

6. Яка технологія та хронологія створення електронного документа [указати електронний документ і певний зміст]?

7. Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно [указати зміст]?

8. Чи містить накопичувач інформації досліджуваного комп'ютера певне [указати, яке саме – установлене, не встановлене] програмне забезпечення?

9. Які функціональні несправності має дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

10. Чи можливо виконання певних дій за допомогою даного програмного продукту?

11. Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

12. Чи реалізовані в даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розроблення?

Експертиза електронних комунікацій є важливою складовою досліджень цифрових слідів, що охоплює аналіз мереж електронних комунікацій, їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв та інформації, яку вони передають, приймають та обробляють.

Основні завдання експертизи електронних комунікацій:

1) визначення характеристик та параметрів мереж електронних комунікацій і їх складових, радіообладнання, радіоелектронних засобів та випромінювальних пристроїв: вивчення технічних характеристик і параметрів роботи мереж і пристроїв; оцінка якості сигналів і відповідності стандартам;

2) установлення фактів і способів передачі (отримання) інформації з використанням мереж електронних комунікацій і їх складових: аналіз протоколів передачі даних і маршрутів передачі інформації; виявлення методів комунікації та використаних технологій;

3) установлення фактів і способів доступу до мереж, ресурсів та інформації у сфері електронних комунікацій: дослідження методів доступу до мережевих ресурсів; аналіз прав доступу й логів авторизації;

4) визначення технічних чинників якості надання електронних комунікаційних послуг на рівні їх споживання: оцінка параметрів якості обслуговування (QoS) та користувацького досвіду (QoE); виявлення факторів, що впливають на якість послуг;

5) установлення конфігурації та робочого стану мереж електронних комунікацій і їх складових: аналіз налаштувань і технічного стану мережевих пристроїв; перевірка справності та працездатності обладнання;

6) установлення типу, марки, моделі й інших класифікаційних категорій мереж електронних комунікацій і їх складових: ідентифікація та класифікація мережевих пристроїв; установлення версій програмного забезпечення та апаратних модифікацій;

7) дослідження алгоритмів оброблення інформації та її захисту в мережах електронних комунікацій: аналіз методів шифрування та інших механізмів захисту даних; оцінка безпеки інформаційних систем.

За допомогою цього виду експертизи можна ідентифікувати характеристику обладнання, параметри підключення та налаштувань, оцінити справність і функціональність мережевих елементів, параметрів підключення окремих компонентів, виявити зміни в конфігурації та часових відміток, установити використане програмне забезпечення для підключення, структуру й розміщення мережевих пристроїв, перевірити відповідність роботи мережі до технічних вимог, зробити детальний аналіз технічних параметрів обладнання, виявити сліди доступу й методи авторизації, установити факти передачі та прийому даних, проаналізувати маршрути й методи передачі даних через радіообладнання, виявити сліди несанкціонованого втручання, оцінити можливості використання мережі для конкретних завдань, а також перевірити відповідність радіообладнання для виконання завдань.

Для вирішення цих завдань можуть бути поставлені такі запитання.

1. Які тип, марка, модель мережі електронних комунікацій і її складових?

2. Чи в робочому стані знаходиться мережа електронних комунікацій і її складові?

3. Які характеристики підключень до мережі має елемент мережі електронних комунікацій?

4. Чи змінювалися користувачем налаштування мережі електронних комунікацій, у який час, які їх значення?

5. Які параметри підключень мають складові мережі електронних комунікацій?

6. За допомогою яких програмних засобів здійснювалося підключення до мережі електронних комунікацій?

7. Яка топологія технічних пристроїв, об'єднаних у мережу електронних комунікацій?

8. Чи відповідає функціонування мережі електронних комунікацій технічній документації?

9. Які технічні характеристики має мережа електронних комунікацій та її складові?

10. Чи мав місце факт доступу до мережі електронних комунікацій та в який спосіб?

11. Чи мало місце використання ресурсів та інформації в мережі електронних комунікацій та в який спосіб?

12. Чи мав місце факт передачі (отримання) інформації в мережі електронних комунікацій та її складових?

13. Чи мав місце факт передачі (отримання) інформації з використанням радіообладнання та в який спосіб?

14. Чи є ознаки втручання в роботу мережі електронних комунікацій?

15. Які шляхи маршрутизації даних у мережі електронних комунікацій?

16. Чи можливо використання мережі електронних комунікацій та її складових для вказаних цілей?

17. Чи можливо використання радіообладнання для вказаних цілей?

Для підготовки експертизи електронних комунікацій слід дотримуватися таких етапів, які є дотичними до описаних вище.

1. Оформлення процесуальних документів: складання постанови слідчого чи прокурора про доручення проведення експертизи або ухвали слідчого судді; долучення протоколів огляду місця події та інших матеріалів кримінального провадження.

2. Забезпечення надання об'єктів дослідження: надання мережевих пристроїв, радіообладнання та інших компонентів для дослідження; забезпечення належного пакування та транспортування об'єктів.

3. Підготовка програмного забезпечення та технічної документації: надання експертам необхідного програмного забезпечення та технічної документації до обладнання.

4. Консультація з експертом: отримання консультацій від спеціалістів для визначення об'єктів дослідження та методів їх аналізу.

Цей порядок підготовки забезпечує всебічне дослідження та аналіз мереж електронних комунікацій, що сприяє отриманню точних і достовірних результатів експертизи.

Отже, залежно від об'єктів і мети судово-експертних досліджень можна виділити такі класифікації.

Комп'ютерно-технічна експертиза:

– дослідження комп'ютерів, серверів й інших електронних пристроїв;

– відновлення видалених файлів;

– аналіз логів системи, історії браузера й інших даних користувача.

Експертиза мобільних пристроїв:

– аналіз даних, що зберігаються на мобільних телефонах, планшетах та інших портативних пристроях;

– відновлення видалених повідомлень, дзвінків, фотографій та інших даних.

Експертиза мережевих технологій:

– аналіз мережевого трафіку та протоколів передачі даних;

– відстеження дій користувачів у мережі Інтернет;

– установлення джерела атак і виявлення шкідливого програмного забезпечення.

Експертиза електронної пошти:

– дослідження електронних листів для виявлення ознак фальсифікації;

– аналіз метаданих електронних листів;

– установлення відправника й отримувача повідомлень.

Експертиза зображень і відео:

– аналіз цифрових фотографій і відеофайлів для виявлення маніпуляцій;

– відновлення видалених зображень і відео.

Експертиза шкідливого програмного забезпечення:

– аналіз підозрілих файлів для виявлення шкідливих програм;

– установлення джерела шкідливого програмного забезпечення.

Експертиза даних із хмарних сервісів:

– дослідження даних, збережених у хмарних сервісах, таких як Google Drive, Dropbox тощо;

– аналіз синхронізації даних між хмарними сервісами й локальними пристроями.

Експертиза інформаційної безпеки:

– оцінка рівня захищеності інформаційних систем;

– аналіз інцидентів інформаційної безпеки;

– виявлення та усунення вразливостей у системах.

Криптографічна експертиза:

– аналіз зашифрованих даних і їх розшифрування;

– дослідження криптографічних протоколів та алгоритмів;

– установлення стійкості шифрувальних систем.

Експертиза програмного забезпечення:

– аналіз програмного коду для виявлення вразливостей та шкідливого функціоналу;

– дослідження легітимності програмного забезпечення та відповідності його функцій заявленим.

Експертиза цифрових аудіо та відео:

– встановлення автентичності аудіо- та відеозаписів;

– відновлення пошкоджених або частково видалених записів;

– виявлення маніпуляцій та монтажу в цифрових медіафайлах.

Експертиза даних із систем GPS і навігаційних пристроїв:

– аналіз даних про переміщення об'єктів;

– установлення маршрутів пересування та часових відміток.

Експертиза інтернет-трафіку:

– аналіз даних про відвідувані вебсайти;

– установлення факту завантаження або передачі файлів через інтернет;

– дослідження дій користувачів у соціальних мережах та інших онлайн-сервісах.

Експертиза електронних підписів і документів:

– перевірка автентичності електронних підписів;

– аналіз електронних документів на предмет фальсифікації;

– установлення відповідності електронних підписів законодавчим вимогам.

Експертиза даних із «розумних» пристроїв (IoT):

– аналіз даних, що збираються «розумними» пристроями, такими як датчики, камери, «розумні» годинники тощо;

– установлення фактів використання таких пристроїв для збору або передачі інформації.

Ці експертизи можуть проводитися окремо або в комплексі, залежно від обставин справи й наявних цифрових слідів.

Запитання для самоконтролю

1. У чому сутність криміналістичного дослідження цифрових слідів як галузі криміналістичної техніки?
2. Що є предметом та об'єктами криміналістичного дослідження цифрових слідів?
3. Які завдання вирішує криміналістичне дослідження цифрових слідів?
4. Що являють собою цифрові сліди і які властивості притаманні такому різновиду слідів?
5. У чому полягає особливість механізму утворення цифрових слідів і вибір критеріїв для їх поділу на певні види?
6. У яких формах може бути відображена інформація, яку несуть цифрові сліди?
7. Які різновиди цифрових слідів ви знаєте? Охарактеризуйте їх.
8. Що таке метадані і які відомості зберігаються в метаданих?
9. Які ви знаєте загальні правила поводження із цифровими слідами?
10. Які існують методи й прийоми збирання, фіксації та дослідження цифрових слідів?
11. Які судові експертизи призначають при криміналістичному дослідженні цифрових слідів кримінального правопорушення?
12. Які завдання можуть бути вирішенні експертизою комп'ютерної техніки і програмних продуктів?
13. Які об'єкти можуть направлятися на дослідження для проведення експертизи комп'ютерної техніки і програмних продуктів?
14. У чому полягають особливості залучення експертів і призначення судових експертиз при криміналістичному дослідженні цифрових слідів кримінального правопорушення?
15. Яка специфіка й форми використання спеціальних знань при криміналістичному дослідженні цифрових слідів?