- Possibility of conducting automatic fire (in turns);
- Arrangement of weapons according to the "bul pap" or pistol type scheme;
- the presence in the design of the weapon of a device for reducing the sound level of the shot, the possibility of installing such devices is provided by the manufacturer (developer); the use of cartridges with mechanical locking of powder gases in the cartridge sleeve or special purpose cartridges with subsonic bullet flight speed in weapons as standard ammunition.

It is substantiated that today two main methods of the problem of reducing the sound level of a shot have been formed:

1) Direct use of DRLSS ("silencers" in the form of various barrel nozzles) with special weapons;

2) the use of a closed-type DRLSS in the form of special complexes, with the expansion and locking of powder gases in the variable closed volume of the barrel, barrel nozzle or a special weakened subsonic cartridge.

It is noted that due to the wide variety of design schemes, special purpose firearms do not always have any of the already mentioned features. Other design solutions also improve the ballistic and tactical performance of weapons. Moreover, some of them can be used in the design of both combat and hunting weapons, as well as special purpose weapons.

It is noted that in some models of special purpose weapons, ordinary cartridges are used as standard ones. The conclusion was formulated that the use of special cartridges for firing from special-purpose weapons is an additional qualifying feature.

The systematized regularities of the formation of marks on bullets and casings fired from special-purpose firearms aimed at improving the scientific and methodological support of expert research on weapons create the prerequisites for establishing the facts of the use of such weapons during the commission of crimes.

Keywords: special purpose military firearms, subsonic bullet flight speed, shot sound reduction device, forensic ballistics, and special cartridge.

DOI: 10.33766/2524-0323.100.226-236
УДК: 343.98

Коваленко А. В., *кандидат юридичних наук, доцент, доцент кафедри кримінально-правових дисциплін Луганського державного університету внутрішніх справ імені Е.О. Дідоренка (м. Івано-Франківськ, Україна)*
e-mail: new4or@gmail.com
ORCID iD: http.//orcid.org/0000-0003-3665-0147

ПОНЯТТЯ ТА СУТНІСТЬ ЕЛЕКТРОННИХ (ЦИФРОВИХ) СЛІДІВ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ

Стаття присвячена з'ясуванню сутності та формулюванню поняття електронних (цифрових) слідів кримінального правопорушення. Акцентовано, що розкриття й розслідування кримінальних правопорушень, учинених з використанням комп'ютерної техніки, потребує встановлення та фіксування дій, здійснених правопорушником та іншими особами з подібними приладами. Операції правопорушника з

комп'ютерною технікою можливо відслідкувати за змінами комп'ютерних даних, що утворюються в пам'яті електронно-обчислювальних машин, котрі, своєю чергою, можна вважати специфічними електронними (цифровими) слідами кримінального правопорушення.

Встановлено, що механізм утворення таких слідів пов'язаний зі зміною магнітно-електричних властивостей речовин у запам'ятовуючому пристрої електронно-обчислювального приладу внаслідок виконання заздалегідь закладених алгоритмів та введених користувачем команд. Електронні (цифрові) сліди кримінального правопорушення визначено як комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення.

На думку автора, названі сліди несуть інформацію про стан та результати роботи певної комп'ютерної системи; не можуть бути безпосередньо сприйняті органами відчуття людини та завжди потребують інтерпретації (перетворення у прийнятну для людини форму) з використанням комп'ютерної техніки; супроводжуються метаданими, тобто додатковою інформацією, що характеризує основні комп'ютерні дані; відповідають загальним ознакам документа в його криміналістичному розумінні; містять інформацію, структуровану й закодовану відповідно до певного формату; інформація, яку несуть такі сліди, у більшості випадків може бути повністю відтворена шляхом відображення (копіювання) відповідних комп'ютерних даних; електронні (цифрові) сліди не мають жорсткої прив'язки до носія комп'ютерних даних.

Ключові слова: кримінальне правопорушення, комп'ютерні дані, сліди, електронні (цифрові) сліди, електронні (цифрові) докази.

Постановка проблеми. Кінець XX і початок XXI століття характеризуються суцільною комп'ютеризацією всіх сфер суспільного життя. Електронно-обчислювальні машини різних типів і розмірів допомагають людині комфортно існувати, а іноді навіть успішно замінюють її при виконанні певних завдань. Утім, ватро зазначити, що такі прилади, як й інші новітні технології, беруться на озброєння зловмисниками. Під час учинення протиправних діянь порушники використовують комп'ютерну техніку як об'єкти та знаряддя посягань, засоби спілкування й координації дій, джерела інформації тощо. Сьогодні правопорушники здатні обернути на свою користь практично будь-який електронно-обчислювальний пристрій: персональні комп'ютери та ноутбуки, мобільні телефони, смартфони, планшети, ігрові приставки, сервери, маршрутизатори й роутери, принтери та копіювальну техніку, розумні пральні машини та холодильники, спеціалізоване обладнання, що має електронно-обчислювальні функції (промислові й виробничі станки, інженерне, медичне обладнання й таке інше).

Розкриття й розслідування кримінальних правопорушень, учинених з використанням комп'ютерної техніки, потребує з'ясування та фіксування операцій, здійснених правопорушником з подібними приладами. Будь-які дії користувача призводять до утворення в пам'яті електронно-обчислювального пристрою нових чи зміни існуючих комп'ютерних даних. Тому операції правопорушника з комп'ютерною технікою можливо відслідкувати за змінами комп'ютерних даних, що утворюються в пам'яті пристроїв. Згадані зміни, своєю чергою,

можна вважати специфічними електронними (цифровими) слідами кримінального правопорушення. Подібні сліди вимагають новітніх підходів до їх виявлення, вилучення та дослідження, а сформовані на основі їх опрацювання докази – своєрідного порядку використання у кримінальному провадженні.

Аналіз останніх досліджень і публікацій. Проблеми збирання, дослідження та використання комп'ютерних даних під час досудового розслідування кримінальних правопорушень у своїх працях досліджували Г. К. Авдєєва, А. В. Гутник, О. Дегтярьова, А. В. Коваленко, В. Г. Колесник, О. І. Крицька, П. М. Маланчук, Т. П. Матюшкова, О. П. Метелев, А. В. Ратнова, Є. Ращенко, О. А. Самойленко, Р. Л. Степанюк, С. В. Стороженко, І. А. Тітко, А. Я. Хитра, М. В. Шепітько, В. Ю. Шепітько, Р. М. Шехавцов та інші вчені. Попри це, у наукових колах відсутнє єдине розуміння комп'ютерних даних як слідів кримінального правопорушення й досі не напрацьовано спільного підходу до найменування подібних слідів і сформованих на основі їх дослідження доказів. Тому з'ясування сутності електронних (цифрових) слідів кримінального правопорушення та формулювання доктринальної дефініції подібних слідів набуває суттєвого наукового й практичного значення.

Формулювання цілей. Метою пропонованого дослідження є з'ясування сутності й формулювання поняття електронних (цифрових) слідів кримінального правопорушення, а також встановлення криміналістично значущих ознак відповідних слідів.

Виклад основного матеріалу. У межах кримінального провадження процес пізнання події кримінального правопорушення уповноваженими особами практично завжди є ретроспективним, тобто спрямованим на минуле. Суб'єкти доказування (сторони обвинувачення й захисту, потерпілий, слідчий суддя й суд) у більшості випадків сприймають результати минулої кримінально-протиправної діяльності, зміни, що відбулися в навколишньому середовищі внаслідок та у зв'язку із вчиненням таких діянь. У теорії криміналістики подібні зміни прийнято називати слідами кримінального правопорушення. На основі аналізу відповідних слідів можливо висунути обґрунтовані припущення (версії) про механізм їх виникнення, а їх виявлення, закріплення та дослідження є основою доказування у кримінальному судочинстві.

Сліди кримінального правопорушення в науковій літературі розглядають у вузькому та широкому розумінні. Сліди у вузькому значенні – це матеріальні утворення, що відбивають зовнішню будову взаємодіючих об'єктів, тобто сліди-копії, які можуть бути об'ємними або площинними. Сліди в широкому значенні – це будь-які зміни в навколишньому середовищі, причинно пов'язані з подією злочину. Водночас слідами в широкому значенні є ідеальні відображення – сліди пам'яті (уявні образи) [1, с. 112]. Утім із розповсюдженням комп'ютерної техніки, її активним використанням під час учинення практично всіх різновидів кримінальних деліктів, правопорушники почали лишати по собі нові сліди, котрі повною мірою не підпадають під вищенаведену «класичну» класифікацію. Такі відображення є докази, сформовані на основі їх дослідження, називають

комп'ютерними [2, с. 122], електронними [3; 4; 5], цифровими [6, с. 124; 7; 8], інформаційними [9; 10, с. 74], електронними (цифровими) [11; 12] тощо слідами (доказами).

Чи не найпопулярніші терміни «електронний слід» та «електронний доказ» походять від назви негативно зарядженої елементарної частинки – електрона, рух якої покладено в основу роботи всіх електричних приладів. Більшість сучасних обчислювальних пристроїв (процесорів, логічних схем) та флеш-накопичувачів даних (SSD-диски, USB-диски, вбудована пам'ять мобільних пристроїв) побудовані на базі транзисторів, а пристрої динамічної оперативної пам'яті (DRAM) працюють на базі конденсаторів. Дані кодуються, обробляються та передаються шляхом регулювання руху електронів через транзистори, а також накопичення певного електричного заряду конденсаторами. Відтак, комп'ютерні дані (інформація), що мають значення для кримінального провадження, часто безпосередньо пов'язані з рухом електронів у логічних елементах електронно-обчислювальної техніки.

Зі свого боку популярні терміни «цифровий слід» та «цифровий доказ» походять від англійського слова digital – «цифровий» (digit – «цифра») та були запозичені в зарубіжних процесуалістів і криміналістів. Застосування категорії «цифровий» 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 й передавання будь-якої інформації. Цифрову форму кодування прийнято протиставляти більш старій та менш розповсюдженій аналоговій, за якої дані передаються через коливання фізичних показників струму, світлового потоку, радіохвиль тощо. Таким чином, у більшості випадків комп'ютерні дані (інформація), що мають значення для кримінального провадження, закодовані в цифровій формі та потребують інтерпретації (перетворення, декодування) для сприйняття людиною.

Зауважимо, що жоден з наведених підходів не є оптимальним з технічної точки зору: уже сьогодні існують системи кодування, що не побудовані на використанні цифр, обчислювальні пристрої й сучасні засоби передавання інформації, котрі не покладаються на рух електронів й не підпадають під загальну категорію «комп'ютер». У сучасних умовах, на нашу думку, категорії «електронний» та «цифровий» по відношенню до слідів і доказів є рівнозначними та несуть однакове смислове навантаження. Тому до закріплення в чинному кримінальному процесуальному законодавстві легальних визначень досліджуваних понять, вважаємо за доцільне використовувати термін «електронні (цифрові) сліди (докази)».

Г. К. Авдєєва та С. В. Стороженко слушно зазначають, що основою механізму утворення електронних слідів слугують електромагнітні взаємодії двох і більше матеріальних об'єктів, кожен із яких є сукупністю електронного цифрового пристрою (комплексу пристроїв) і системи управління ним (набору програмних продуктів) [3, с. 170]. У дещо спрощеній формі механізм утворення електронних (цифрових) слідів можна описати так. Унаслідок виконання елект-

ронно-обчислювальною технікою заздалегідь закладених алгоритмів та введених користувачем команд змінюються магнітно-електричні властивості речовин у запам'ятовуючому пристрої цієї техніки. Наприклад, два стани транзистора у флеш-диску можуть позначати 0 та 1. Комбінації мільйонів подібних транзисторів зі змінними станами дозволяють зберігати та обробляти значні об'єми інформації. Властивості подібних речовин у запам'ятовуючих пристроях відслідковуються процесорами та інтерпретуються (перекладаються) у форму, що може бути сприйнята людиною. Конкретний механізм запису, зберігання та зміни інформації залежить від типу носія (магнітні та оптичні носії, флеш-пам'ять, динамічна пам'ять тощо працюють по-різному).

У випадку якщо комп'ютерні дані, що зберігаються в пам'яті електронно-обчислювальної техніки, були створені або змінені правопорушником чи іншими особами у зв'язку із вчиненням кримінального правопорушення, вони матимуть значення для розслідування та можуть бути вилучені й досліджені як електронні (цифрові) сліди правопорушення. З огляду на наведене, пропонуємо розуміти електронні (цифрові) сліди кримінального правопорушення як комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення.

Електронні (цифрові) сліди, як комп'ютерні дані, мають певні криміналістично значущі властивості, що є суттєвими для їх розуміння та використання під час розслідування кримінальних правопорушень.

Зокрема, названі сліди *несуть інформацію про стан та результати роботи певної комп'ютерної системи* (електронно-обчислювального пристрою, системи чи мережі пристроїв). Такі комп'ютерні дані можуть містити інформацію, отриману комп'ютером від користувача (input) через пристрої введення інформації (клавіатуру, маніпулятори, сенсорі екрани, мікрофони, камери тощо) та пристрої й інтерфейси передавання інформації (завантаження файлів через інтернет-з'єднання, копіювання даних із зовнішніх запам'ятовувальних пристроїв тощо); результати обробки даних від користувача; а також дані, що створюються операційною системою та іншим програмним забезпеченням в автоматичному режимі відповідно до заздалегідь закладених (запрограмованих) алгоритмів та зберігають дані про стан і роботу системи, її користувачів, виконані алгоритми, помилки, що виникли під час їх виконання та інше (log-файли, звіти про помилки, тимчасові фали, транзакційні бінарні файли, дампи даних тощо).

Досліджувані в статті сліди не можуть бути безпосередньо сприйняті органами відчуття людини та *завжди потребують інтерпретації (перетворення у прийнятну для людини форму)* з використанням комп'ютерної техніки. Інформацію, що несе подібний слід, може бути відображено на екрані комп'ютера чи роздруковано в оригінальній, закодованій формі (байт-код, бінарний код, синтаксичний запис тощо). Комп'ютерні дані, що містять текст, зображення, звуки та інші аудіовізуальні форми інформації можуть бути декодовані та відтворені через пристрої виведення даних, а код, що містить алгоритми дій, – виконано (запу-

щено програму). Аудіовізуальна форма відображення даних, як правило, доступна через використання спеціального (асоційованого) програмного забезпечення.

Електронні (цифрові) сліди в більшості випадків *супроводжуються метаданими* [13, с. 22] (від давньогрецького μετά – «після», «за межами» та англійського data – «дані»), тобто додатковою інформацією, що характеризує основні комп'ютерні дані. Метадані характеризують файл («контейнер» для даних) або папку-каталог їх індексації і можуть зберігатися як разом із основними даними, так й 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 й дослідження електронних (цифрових) слідів. 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.

Оскільки комп'ютерні дані спеціально створюються для збереження, обробки й передавання інформації у специфічній закодованій формі, вони *відповідають загальним ознакам документа* у його криміналістичному розумінні. Через те в межах криміналістичного документознавства виокремлюють такий різновид документів, як електронні. Поняття електронного документу закріплено в чинному законодавстві (хоч й у формі, що відрізняється від криміналістичного розуміння електронних документів). Відповідно до ст. 5 Закону України «Про електронні документи та електронний документообіг», електронний документ – документ, інформація, у якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [14]. Дещо відрізняється кримінальне процесуальне розуміння електронного документу. Відповідно до змісту ст. 99 КПК України, електронні документи є різновидом документів, як процесуальних джерел доказів [15]. Комп'ютерні дані набувають процесуального значення електронного документу після їх огляду (чч. 1, 2 ст. 237 КПК України), за умови, що зміст таких даних відповідає вимогам ч. 1 ст. 99 КПК України (тобто такі дані спеціально створені з метою збереження інформації, містять зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження).

У більшості випадків електронні (цифрові) сліди, як комп'ютерні дані, *містять інформацію, структуровану й закодовану відповідно до певного формату*. Як правило, форматовані дані запаковані в контейнери (файли), мають розширення назви, що відповідає їх формату, та супроводжуються специфічними метаданими. Кожен формат файлу асоційований із певним програмним забезпеченням. Наприклад, файли, що містять зображення формату *.png, можуть бути відтворені чи редаговані більшістю графічних редакторів, а зображення фор-

мату *.psd є специфічними для програмного забезпечення Adobe Photoshop. Неформатовані дані найчастіше утворюються внаслідок виникнення програмних або апаратних помилок, неповного копіювання чи передавання даних тощо. Такі дані не можуть бути інтерпретовані (перетворені в прийнятну для людини форму) та мають досліджуватися в оригінальному закодованому вигляді.

Окрім того, основна інформація, яку несуть електронні (цифрові) сліди, у більшості випадків *може бути повністю відтворена шляхом відображення (копіювання) відповідних комп'ютерних даних*. На відміну від матеріально фіксованих слідів, котрі не можливо повністю скопіювати чи відтворити в натурі, комп'ютерні дані за дотримання правил поводження з ними можуть бути скопійовані необмежену кількість разів без зміни їх змісту. За загальним правилом, копії комп'ютерних даних відрізняються від оригіналів лише окремими метаданими (змінюються каталог розміщення, дата створення, найменування користувача, що створив файл, тощо). Описана властивість комп'ютерних даних знайшла відображення й у кримінальному процесуальному законодавстві: відповідно до чч. 3, 4 ст. 99 КПК України, відображення електронного документу, а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

З огляду на наведену ознаку, варто зробити висновок про те, що електронні (цифрові) сліди *не мають жорсткої прив'язки до носія комп'ютерних даних*. Зокрема, на це звертають увагу Г. К. Авдєєва та С. В. Стороженко. Цитовані науковці зазначають, що електронні сліди не мають нерозривного зв'язку з матеріальним носієм та можуть бути миттєво перенесені між пристроями, у тому числі з однієї частини земної кулі в іншу [3, с. 171]. Додамо також, що комп'ютерні дані постійно переміщуються між носіями під час нормальної роботи електронно-обчислювального пристрою, наприклад, із приладу постійної пам'яті до приладу оперативної пам'яті чи кеш-пам'яті процесора й у зворотному напрямку; операційна система може переміщувати дані між блоками й секторами одного чи декількох носіїв задля оптимізації роботи тощо. Через це, вважаємо, що електронні (цифрові) сліди кримінального правопорушення мають розглядатися у відриві від фізичного носія комп'ютерних даних. Водночас суттєве значення для встановлення обставин кримінального правопорушення має носій, на якому виявлено такі сліди, носії, що містять копії відповідних комп'ютерних даних, тип і технологія роботи цих носіїв, час та спосіб перенесення на них даних тощо.

Висновки. Підсумовуючи викладене, зазначимо, що із розповсюдженням комп'ютерної техніки, її активним використанням під час учинення практично всіх різновидів кримінальних деліктів, правопорушники лишають по собі в навколишньому середовищі новий тип змін, котрий цілком не вкладається в «класичну» класифікацію слідів кримінальних правопорушень. Такі відображення й докази, сформовані на основі їх дослідження, у спеціальній літературі назива-

ють комп'ютерними, електронними, цифровими, інформаційними, електронними (цифровими) тощо слідами (доказами). На нашу думку, жоден із наведених підходів не є оптимальним з технічної точки зору. До закріплення в чинному кримінальному процесуальному законодавстві легальних визначень досліджуваних понять вважаємо за доцільне використовувати термін «електронні (цифрові) сліди (докази)».

Механізм утворення таких слідів пов'язаний зі зміною магнітно-електричних властивостей речовин у запам'ятовуючому пристрої електронно-обчислювального приладу внаслідок виконання заздалегідь закладених алгоритмів та введених користувачем команд. Електронні (цифрові) сліди кримінального правопорушення визначено як комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення. Подібні сліди, як комп'ютерні дані, мають певні криміналістично значущі властивості, що є суттєвими для їх розуміння та використання під час розслідування кримінальних правопорушень.

Подальші наукові розробки в даній сфері мають бути пов'язані з класифікацією електронних (цифрових) слідів кримінального правопорушення, формулюванням практично-орієнтованих рекомендацій щодо виявлення, вилучення та фіксації таких слідів, а також щодо дослідження й використання електронних (цифрових) доказів у кримінальному провадженні.

Використані джерела:

1. Салтевський М. В. Криміналістика. Підручник: У 2-х ч. Ч. 1. Харків, 1999. 416 с.

2. Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи: дис.… д-ра юрид. наук: 12.00.09. Одеса, 2018. 626 с.

3. Авдєєва Г. К., Стороженко С. В. Електронні сліди : поняття та види. *Вісник Луганського державного університету внутрішніх справ*. 2017. № 1 (77). С. 169-176.

4. Коваленко А. В. Електронні докази у кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ*. 2018. № 4 (84). С. 237-245.

5. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Юридичний вісник*. 2021. № 6. С. 273-278.

6. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія ; за заг. ред. А. Ф. Волобуєва. Одеса :ТЕС, 2020. 372 с.

7. Колесников І. В. Цифрова криміналістика: доказування з використанням ифрових доказів. *Протидія кіберзагрозам у сучасному безпековому середовищі: актуальні питання теорії та практики* : збірник матеріалів Міжнародної науково-практичної конференції, 29 жовтня 2021 року. Київ : ІСТЕ СБУ, 2021. С. 94-98.

8. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ*. 2022. № 3 (99). С. 283-294. URL : https://doi.org/10.33766/2524-0323.99.283-284.

9. Самойленко О., Паляничко Д., Баланюк О., Ващенко І. Інформаційні сліди в контексті механізму вчинення злочинів із використанням обстановки кіберпростору.

Криміналістика та судова експертологія: наука, навчання, практика : матеріали XIV міжнар. Конгресу (м. Одеса, 13-15 верес.): у 2-х т. Т. 2. Одеса : Гельветика, 2018. С. 216-221.

10. Ращенко Є. Комп'ютерні дані як носій криміналістичної інформації про злочин у сфері комп'ютерних технологій. *Правова інформатика*. 2007. № 1 (13). С. 76-80.

11. Матюшкова Т. П. Електронна (цифрова) інформація: сучасний стан і перспективи розвитку криміналістики. *Актуальні проблеми кримінального процесу та криміналістики*: тези доп. Міжнар. наук.-практ. конф.(м. Харків, 29 жовт. 2021 р.). Харків : ХНУВС, 2021. С. 248-250.

12. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238.

13. Renu Gopal Mani, Rahul Parthasarathy, Sivaraman Eswaran and Prasad Honnavalli. A Survey on Digital Image Forensics: Metadata and Image forgeries. *Workshop on Applied Computing*, January 27 – 28, 2022, Chennai, India. P. 22-55. URL : https://ceur-ws.org/Vol-3142/PAPER_03.pdf.

14. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV / *Законодавство України*. URL : https://zakon.rada.gov.ua/laws/show/851-15.

15. Кримінальний процесуальний кодекс України. Кодекс України; Закон, Кодекс від 13.04.2012 № 4651-VI. / *Законодавство України.* URL : https://zakon.rada.gov.ua/laws/show/4651-17.

References:

1. Saltevskyi, M. V. (1999). Kryminalistyka. Pidruchnyk (Part. 1-2; Part. 1). Kharkiv : Konsum, Osnova. [in Ukrainian].

2. Kovalchuk, S. O. (2018). Vchennia pro rechovi dokazy u kryminalnomu protsesi: teoretyko-pravovi ta praktychni osnovy. [in Ukrainian].

3. Avdieieva, H. K., Storozhenko, S. V. (2017). Elektronni slidy : poniattia ta vydy. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav – Bulletin of Luhansk State University of Internal Affairs named after E. Didorenko, 1 (77), 169-176.* [in Ukrainian].

4. Kovalenko, A. V. (2018). Elektronni dokazy u kryminalnomu provadzhenni: suchasnyi stan ta perspektyvy vykorystannia. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav – Bulletin of Luhansk State University of Internal Affairs named after E. Didorenko, 4 (84), 237-245.* [in Ukrainian].

5. Dehtiarova, O. (2021). Dokazuvannia u kryminalnomu provadzhenni na pidstavi elektronnykh dokaziv. *Yurydychnyi visnyk – Law Herald, 6, 273-278*. [in Ukrainian].

6. Samoilenko, O. A. (2020). Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori : monohrafiia ; A. F Volobuiev (Ed.). Odesa :TES. [in Ukrainian].

7. Kolesnykov, I. V. (2021) Tsyfrova kryminalistyka: dokazuvannia z vykorystanniam yfrovykh dokaziv. *Protydiia kiberzahrozam u suchasnomu bezpekovomu seredovyshchi: aktualni pytannia teorii ta praktyky : zbirnyk materialiv Mizhnarodnoi naukovo-praktychnoi konferentsii, 29 zhovtnia 2021 roku - Protydiia cyberzahrozam u suchasnomu bezpekovomu seredovyshchi: aktualni pytannia teorii ta praktyky : zbirnyk materialiv Mizhnarodnoi naukovo-praktychnoi konferentsii, 29 zhovtnia 2021 roku, 94-98*. Kyiv : ISTE SBU. [in Ukrainian].

8. Stepaniuk, R. L., Perlin, S. I. (2022). Tsyfrova kryminalistyka y udoskonalennia systemy kryminalistychnoi tekhniky v Ukraini. *Visnyk Luhanskoho derzhavnoho universytetu*

vnutrishnikh sprav – Bulletin of Luhansk State University of Internal Affairs named after E. Didorenko, 3 (99), 283-294. [in Ukrainian].

9. Samoilenko, O., Palianychko, D., Balaniuk, O. & Vashchenko, I. (2018). Informatsiini slidy v konteksti mekhanizmu vchynennia zlochyniv iz vykorystanniam obstanovky kiberprostoru. *Kryminalistyka ta sudova ekspertolohiia: nauka, navchannia, praktyka : materialy XIV mizhnar. Konhresu* (m. *Odesa, 13-15 veres.): (u 2 h t.: T. 2.*) - *Forensics and forensic expertise: science, training, practice: materials of the International Congress (Odesa, September 13-15): (Vol.1-2: Vol. 2.), 216-221.* Odesa : Helvetyka. [in Ukrainian].

10. Rashchenko, Ye. (2007). Kompiuterni dani yak nosii kryminalistychnoi informatsii pro zlochyn u sferi kompiuternykh tekhnolohii. *Pravova informatyka – Legal informatics, 1 (13), 76-80.* [in Ukrainian].

11. Matiushkova, T. P. (2021) Elektronna (tsyfrova) informatsiia: suchasnyi stan i perspektyvy rozvytku kryminalistyky. *Aktualni problemy kryminalnoho protsesu ta kryminalistyky: tezy dop. Mizhnar. nauk.-prakt. konf.*(m. Kharkiv, 29 zhovt. 2021 r.) - *Actual problems of the criminal process and criminology: theses add. International science and practice conference (Kharkov, October 29, 2021), 248-250.* Kharkiv: KhNUVS. [in Ukrainian].

12. Metelev, O. P. (2019). Problemy vyznachennia dopustymosti i nalezhnosti tsyfrovykh (elektronnykh) dokaziv u kryminalnomu protsesi. *Visnyk kryminalnoho sudochynstva – Herald of Criminal Justice, 3, 224-238*. [in Ukrainian].

13. Renu Gopal Mani, Rahul Parthasarathy, Sivaraman Eswaran & Prasad Honnavalli (2022). A Survey on Digital Image Forensics: Metadata and Image forgeries. *Workshop on Applied Computing*, *January 27-28, 22-55*. Chennai, India. 22-55. URL : https://ceur-ws.org/Vol-3142/PAPER_03.pdf. [in English].

14. Pro elektronni dokumenty ta elektronnyi dokumentoobih. Zakon Ukrainy vid 22.05.2003 № 851-IV. (2003) / *Zakonodavstvo Ukrainy.* N. p. URL : https://zakon.rada.gov.ua/laws/show/851-15. [in Ukrainian].

15. Kryminalnyi protsesualnyi kodeks Ukrainy. Kodeks Ukrainy; Zakon, Kodeks vid 13.04.2012 № 4651-VI. (2012) / *Zakonodavstvo Ukrainy.* N. p. URL : https://zakon.rada.gov.ua/laws/show/4651-17. [in Ukrainian].

Стаття надійшла до редколегії 04.12.2022

Kovalenko A., *Ph.D in Law Associate professor, Associate professor of Department of Criminal-Law disciplines, Luhansk State University of Internal Affairs named after E. O. Didorenko (Ivano-Frankivsk, Ukraine)*

CONCEPT AND ESSENCE OF ELECTRONIC (DIGITAL) TRACES OF CRIMINAL OFFENSES

The proposed article is devoted to clarifying the essence and formulating the concept of electronic (digital) traces of a criminal offense. It is emphasized that the disclosure and investigation of criminal offenses committed with the use of computer technology requires finding out and recording the actions performed by the offender and other persons with such devices. The offender's operations with computer equipment can be monitored by changes in computer data generated in the memory of electronic computing machines, which, in turn, can be considered specific electronic (digital) traces of a criminal offense.

It was established that the mechanism of formation of such traces is related to the change in the magnetic-electric properties of substances in the memory device of the electronic computing device as a result of the execution of pre-set algorithms and commands entered by the user. Electronic (digital) traces of a criminal offense are defined as computer data that were created or changed in the memory devices of electronic computing equipment as a result of user actions related to the commission of a criminal offense.

It is emphasized that electronic (digital) traces, as computer data, have certain forensically significant properties, which are essential for their understanding and use during the investigation of criminal offenses. According to the author, the named traces: carry information about the state and results of a certain computer system; cannot be directly perceived by human senses and always require interpretation (transformation into a form acceptable to humans) using computer technology; are accompanied by metadata, that is, additional information characterizing the basic computer data; correspond to the general features of the document in its forensic sense; contain information structured and encoded according to a certain format; the information carried by such traces can, in most cases, be completely reproduced by displaying (copying) the relevant computer data; electronic (digital) traces are not rigidly linked to the computer data carrier.

Keywords: criminal offense, computer data, traces, electronic (digital) traces, electronic (digital) evidence.

DOI: 10.33766/2524-0323.100.236-246
УДК: 343.98:343.71:343.137.5(477)

Коваленко В. В., *кандидат юридичних наук, професор, професор кафедри кримінально-правових дисциплін Луганського державного університету внутрішніх справ імені Е. О. Дідоренка (м. Івано-Франківськ, Україна)*
e-mail: kvvkrimluvd@ukr.net
ORCID iD: https://orcid.org/0000-0001-5310-2092

ТИПОВІ СЛІДЧІ СИТУАЦІЇ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ ГРАБЕЖІВ, ВЧИНЕНИХ НЕПОВНОЛІТНІМИ

Стаття присвячена розгляду типових слідчих ситуацій початкового етапу розслідування грабежів, вчинених неповнолітніми.

Наголошено, що на сьогодні, як серед науковців, так і серед практиків, найпопулярнішим підходом до організації досудового розслідування кримінальних правопорушень в Україні є ситуаційний підхід. Наведено джерела, що характеризуються найбільшим обсягом первинної інформації про подію, яка відбулася.

На основі положень криміналістичної тактики, думок науковців та результатів узагальнення судово-слідчої практики досудового розслідування грабежів, вчинених неповнолітніми, виокремлено найбільш типові слідчі ситуації початкового етапу розслідування вказаних злочинів. Такими ситуаціями є: Ситуація 1. Злочинця затримано на місці події або відразу після вчинення злочину (10 % досліджених кримінальних проваджень). Ситуація 2. Злочинця не затримано, його особа відома потерпілому (30 % досліджених проваджень). Ситуація 3. Злочинця не затримано, його особа не відома потерпілому (60 % досліджених кримінальних проваджень): ситуація 3.1.