DOI: 10.21564/2414–990X.161.278117

Класифікація електронних (цифрових) слідів кримінального правопорушення

Артем Володимирович Коваленко*
Луганський навчально-науковий інститут імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, Івано-Франківськ, Україна
**e-mail: new4or@gmail.com*

Анотація
Із розвитком науки і техніки змінюються й способи використання правопорушниками електронно-обчислювальних приладів під час учинення кримінально караних діянь. Кожні новий спосіб, прояв протиправної технології лишають по собі специфічні сліди, які у більшості випадків є новими і для теоретиків, і для практиків. Виявлення, вилучення та дослідження кожного виду таких слідів потребує своєрідних підходів. Тому завданням учених-криміналістів є розподіл згаданих слідів на різновиди, виходячи з їх сутнісних та криміналістично значущих ознак задля подальшого розроблення практико-орієнтованих рекомендацій щодо роботи з ними. Метою цієї статті є формування криміналістичної класифікації електронних (цифрових) слідів кримінального правопорушення. Для досягнення поставленої мети використано методи узагальнення, лінгвістичного аналізу, формально-юридичний, формально-логічний, порівняння, прогнозування прийоми аналізу та синтезу, а також діяльнісний та праксеологічний підходи у криміналістиці. Виокремлено криміналістично значущі ознаки електронних (цифрових) слідів кримінального правопорушення та обрано три групи критеріїв для їх класифікації: за ознаками слідоутворюючого об'єкта, за ознаками комп'ютерних даних як сліду та за ознаками носія таких даних (слідосприймаючого об'єкта). Відповідно до першої групи критеріїв електронні (цифрові) сліди кримінального правопорушення поділено на різновиди за слідоутворюючим об'єктом; другої групи – за форматуванням даних, за змістом даних, за способом сприйняття інформації, за автентичністю та за можливістю доступу; третьої групи – за місцем розташування носія комп'ютерних даних, за призначенням і типом встановлення носія та за енергозалежністю запам'ятовувального пристрою носія даних. На думку автора, перспективними є наукові дослідження щодо подальшого розподілу електронних (цифрових) слідів кримінальних правопорушень на підвиди та формулювання практико-орієнтованих рекомендацій щодо їх виявлення, збирання, дослідження й використання у кримінальному провадженні.

Ключові слова: кримінальне правопорушення; доказування; електронні (цифрові) сліди; комп'ютерні дані; електронно-обчислювальний пристрій; носій комп'ютерних даних.

Classification of Electronic (Digital) Traces of Criminal Offenses

Artem V. Kovalenko*
Luhansk Educational & Scientific Institute named after E. Didorenko of the Donetsk State University of Internal Affairs, Ivano-Frankivsk, Ukraine
**e-mail: new4or@gmail.com*

Abstract
With the further development of science and technology, the ways in which offenders use electronic computing devices while committing criminal acts are also changing. Each new method, each manifestation of illegal technology leaves behind specific traces, which in most cases are new for both theorists and practitioners. Identification, extraction and examination of each type of such traces requires unique approaches. Therefore, the task of forensic scientists is to divide the mentioned traces into varieties based on their essential and forensically significant features in order to further develop practical recommendations for working with them. Therefore, the purpose of this article is the formation of a forensic classification of electronic (digital) traces of a criminal offense. To achieve the goal, the methods of generalization, linguistic analysis, formal-legal, formal-logical, comparison, forecasting, analysis and synthesis methods, as well as activity and praxeological approaches in forensic science were used. The author singled out forensically significant features of electronic (digital) traces of a criminal offense and selected three groups of criteria for their classification: according to the features of the trace-forming object, according to the features of computer data as a trace, and according to the features of the carrier (media) of such data (trace-receiving object). Based on the first group of criteria electronic (digital) traces of a criminal offense are divided into varieties according to the trace-forming object; based on the second group of criteria – according to data formatting, according to data content, according to the method of information perception, according to data authenticity, according to the possibility of access; based on the third group – according to the location of the computer data carrier (media), according to the purpose and type of installation of the carrier and by the energy dependence of the storage device of the data carrier. In the author's opinion, scientific research on the further distribution of electronic (digital) traces of criminal offenses into subtypes and the formulation of practically oriented recommendations regarding their detection, collection, examination and use in criminal proceedings are promising.

Keywords: criminal offense; proving; electronic (digital) traces; computer data; electronic computing device; computer data carrier.

Вступ

Із розвитком науки і техніки електронно-обчислювальні пристрої дедалі частіше стають об'єктами, предметами й знаряддями вчинення різноманітних кримінальних правопорушень. Через це проблеми виявлення, збирання, дослідження та використання у кримінальному провадженні електронних (цифрових) слідів, що утворюються внаслідок використання таких пристроїв, привертають усе більше уваги в наукових колах. Зокрема, вітчизняні та зарубіжні вчені досліджують поняття, сутність та види електронних (цифрових) слідів (Avdieieva & Storozhenko, 2017; Naidon, 2019) [1–2], проблеми розслідування кримінальних правопорушень, учинених з використанням електронно-обчислювальної техніки (Horsman & Errickson, 2019; Samoilenko, 2020) [3–4], та перспективи розвитку цифрової криміналістики (Kolodina & Fedorova, 2022; Stepaniuk & Perlin, 2022) [5–6] тощо.

Так, із розвитком науки і техніки змінюються й способи використання правопорушниками електронно-обчислювальних приладів під час учинення кримінально караних діянь. Кожен новий спосіб, кожен прояв протиправної технології лишає по собі специфічні сліди, які в більшості випадків є новими і для теоретиків, і для практиків. Виявлення, вилучення та дослідження кожного виду подібних слідів потребує своєрідних підходів. У цьому контексті маємо погодитися з П. Ріді, що у випадках, коли процес інтерпретації цифрових слідів є помилковим та призводить до оцінки неточних даних, все подальше розслідування може стати помилковим, про що слідчий може навіть не здогадуватися [7, с. 498]. Тому завданням учених-криміналістів є розподіл згаданих слідів на різновиди з огляду на їх сутнісні та криміналістично значущі ознаки задля подальшої розробки практико-орієнтованих рекомендацій щодо роботи з ними.

Отже, метою пропонованого дослідження є формування криміналістичної класифікації електронних (цифрових) слідів кримінального правопорушення. Досягнення мети дослідження передбачає вирішення таких завдань: з'ясувати криміналістично значущі ознаки електронних (цифрових) слідів, що можуть стати підставами для класифікації; сформулювати критерії класифікації; поділити та згрупувати електронні (цифрові) сліди за критеріями, що характеризують слідоутворюючий об'єкт, власне, комп'ютерні дані як слід та слідосприймаючий об'єкт.

Огляд літератури

Питання сутності, визначення електронних (цифрових) слідів кримінального правопорушення, можливостей їх виявлення, збирання, дослідження та використання у кримінальному провадженні лишається недостатньо розробленим

та дискусійним у вітчизняній науковій літературі. Попри це, проблеми класифікації таких слідів неодноразово привертали увагу учених-криміналістів. Так, Г. К. Авдєєва та С. В. Стороженко поділяють електронні сліди за об'єктом, що їх утворює, за способом учинення кіберзлочину, за способом доступу до комп'ютерної системи, за правомірністю доступу до неї [1, с. 171–172]. Я. Найдьон пропонує такі підстави класифікації віртуальних слідів кіберзлочинів: за походженням, за формою подання, за місцем зберігання та за формою [2, с. 305–306]. Л. П. Гринько пропонує виокремлювати віртуальні сліди, які залишаються на електронних носіях, та ті, що містяться в мережі «Інтернет» [8, с. 23]. А. С. Колодіна та Т. С. Федорова виокремлюють активні та пасивні «цифрові відбитки», а також контент і метадані як різновиди цифрових слідів [5, с. 178]. Утім, попри увагу окремих науковців до поділу електронних (цифрових) слідів кримінальних правопорушень на різновиди, у спеціальній літературі до сьогодні не сформовано комплексної криміналістичної класифікації таких слідів, що підкреслює актуальність цього дослідження.

Матеріали та методи

Задля здійснення класифікації електронних (цифрових) слідів кримінальних правопорушень автор статті з огляду на предмет та сформульовану мету дослідження використав низку загальних та спеціальних методів наукового пошуку. Основою методології пропонованого дослідження є діалектичний метод наукового пізнання, що дозволило всебічно опрацювати проблеми класифікації електронних (цифрових) слідів. Методи узагальнення та лінгвістичного аналізу використано для вивчення позицій вітчизняних і зарубіжних науковців щодо підходів до класифікації електронних (цифрових) слідів. Формально-юридичний метод застосовано для опрацювання положень чинного кримінального процесуального законодавства щодо збирання, дослідження й використання доказів у кримінальному провадженні. Логічні прийоми аналізу та синтезу допомогли виокремити сутнісні ознаки електронних (цифрових) слідів та осягнути механізм їх утворення. Метод порівняння використано для зіставлення ознак електронних (цифрових), матеріально-фіксованих та ідеальних слідів кримінального правопорушення, а також алгоритмів поводження уповноважених осіб із такими слідами. Діяльнісний та праксеологічний підходи у криміналістиці дозволили зважити криміналістичну значущість виокремлених ознак та з'ясувати їх вплив на процедури виявлення, збирання, дослідження й використання досліджуваних слідів. Формально-логічний метод та метод моделювання застосовано для визначення критеріїв класифікації таких слідів та їх розподілу на різновиди. Метод прогнозування дозволив визначити подальші перспективи дослідження проблем виявлення, збирання, дослідження та використання

електронних (цифрових) слідів кримінальних правопорушень у кримінальному провадженні.

Пропоноване дослідження є структурованим та послідовним. На його першому етапі опрацьовано позиції вітчизняних і зарубіжних науковців щодо підходів до класифікації електронних (цифрових) слідів кримінального правопорушення. У межах другого етапу дослідження проаналізовано сутність електронних (цифрових) слідів та з'ясовано їх основні характерні ознаки. На третьому етапі дослідження оцінено криміналістичну значущість сутнісних ознак таких слідів та визначено критерії (підстави) їх класифікації. На завершальному, четвертому, етапі дослідження здійснено розподіл електронних (цифрових) слідів кримінального правопорушення на різновиди та сформульовано коротку характеристику кожного з них.

Теоретичною основою дослідження виступили положення загальної теорії криміналістики, вчення про сліди кримінального правопорушення й процес слідоутворення, вчення про збирання, дослідження й використання доказів у кримінальному провадженні. Нормативну основу дослідження становлять положення чинного кримінального процесуального законодавства України.

Під час виконання цього дослідження автор виходив із раніше обґрунтованого ним розуміння електронних (цифрових) слідів кримінального правопорушення як комп'ютерних даних, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення [9, с. 230]. Критерії для класифікації були обрані, виходячи з ознак, що характеризують електронні (цифрові) сліди як комп'ютерні дані, а також із особливостей механізму слідоутворення. Серед згаданих ознак виокремлено й застосовано ті, що мають криміналістичну значущість і, зокрема, впливають на процес збирання, дослідження та використання електронних (цифрових) доказів у кримінальному провадженні. Запропоновано три класифікаційні ряди електронних (цифрових) слідів кримінального правопорушення: за критеріями, що характеризують слідоутворюючий об'єкт; за критеріями, що характеризують, власне, комп'ютерні дані як слід; за критеріями, що характеризують носій таких даних (слідосприймаючий об'єкт) на момент їх виявлення.

Результати та обговорення

Класифікація електронних (цифрових) слідів за критеріями, що характеризують слідоутворюючий об'єкт

За слідоутворюючим об'єктом такі сліди можна поділити на утворені внаслідок отримання ввідних даних і команд від користувача та утворені внаслідок

виконання електронно-обчислювальною технікою заздалегідь закладених алгоритмів. Перші містять інформацію, отриману комп'ютером від користувача (input) через пристрої введення інформації (клавіатуру, маніпулятори (миша, джойстик, геймпад), сенсорні екрани, мікрофони, камери тощо), та пристрої й інтерфейси передавання інформації (завантаження файлів через інтернет-з'єднання, копіювання даних із зовнішніх запам'ятовувальних пристроїв тощо). Другі створюються операційною системою та іншим програмним забезпеченням в автоматичному режимі відповідно до заздалегідь закладених (запрограмованих) алгоритмів та зберігають дані про стан та роботу системи, її користувачів, виконані алгоритми, помилки, що виникли під час їх виконання та інше (log-файли, звіти про помилки, тимчасові файли, транзакційні бінарні файли, дампи даних тощо). За Г. Хорсманом, практично будь-яка взаємодія користувача з цифровою операційною системою, пристроєм чи програмним забезпеченням призводить до автоматичного створення та/чи зміни файлів, що містять відомості про налаштування та журнали використання. Цитований автор називає такі файли цифровими артефактами й наголошує, що їх дослідження є основою пошуку потенційно доказової інформації в пам'яті цифрових пристроїв [10, с. 1]. Також варто наголосити, що електронні (цифрові) сліди можуть утворюватися внаслідок автоматизованої взаємодії двох чи більше електронно-обчислювальних пристроїв, з'єднаних однією мережею. Південно-корейські дослідники зазначають, що комп'ютерні пристрої, здатні комунікувати з іншими пристроями, генерують сліди на локальних пристроях, у мережах та на хмарних сервісах [11, с. 1]. Як приклад описаного механізму слідоутворення М. В. Корбець та Р. М. Корбець наводять автоматичне збереження у пам'яті WI-FI роутера MAC-адреси пристрою, що під'єднувався до нього [12, с. 37].

Класифікація електронних (цифрових) слідів за критеріями, що характеризують, власне, комп'ютерні дані як слід

За форматуванням даних електронні (цифрові) сліди варто поділити на форматовані та неформатовані. Практично всі комп'ютерні дані, за визначенням, мають вважатися форматованими, адже вони спеціально створюються для збереження, обробки й передавання інформації у закодованому вигляді та структуровані відповідно до вимог певного формату. Отже, комп'ютерні дані можуть бути поділені на різновиди за критерієм формату, до якого вони належать. 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 формату *.psd є специфічними для програмного забезпечення Adobe Photoshop. У свою чергу, неформатовані дані найчастіше утворюються внаслідок виникнення програмних або апаратних помилок, неповного копіювання чи передавання даних тощо. Такі дані не можуть бути інтерпретовані (перетворені у прийнятну для людини форму) та мають досліджуватися в оригінальному закодованому вигляді.

За змістом даних досліджувані сліди пропонується поділяти на основні дані (А. С. Колодіна та Т. С. Федорова пропонують називати їх контентом [5, с. 178]) та метадані. Основні дані несуть інформацію щодо роботи електронно-обчислювального приладу та операцій користувачів, структуровані відповідно до вимог певного формату й містяться у «контейнері» – файлі. Метадані (від давньогрец. μετά – після, за межами та з англ. data – дані) – додаткова інформація, що характеризує основні дані (файл «контейнер» даних, каталог індексації даних) та можуть зберігатися разом з основними даними чи окремо від них. Перелік та зміст метаданих залежать від формату основних даних, операційної системи, типу файлу та програмного забезпечення, з яким файл асоційовано, тощо. Прикладами метаданих є розмір файлу, назва, розширення назви, асоційоване програмне забезпечення, каталог розташування, час створення й останнього редагування тощо.

За способом сприйняття інформації можна виокремити дані, що несуть інформацію в аудіовізуальній формі та дані без аудіовізуальної форми. Комп'ютерні дані за визначенням є зашифрованими та призначеними для оброблення обчислювальними пристроями засобів комп'ютерної техніки. Для їх сприйняття завжди необхідно здійснити інтерпретацію (перетворення) даних у прийнятну для людини форму. При цьому певні дані після інтерпретації можуть мати аудіовізуальну форму: зображення, відео, аудіо, тексти, таблиці, інтерфейси тощо. З іншого боку, виконуваний код, що не має користувацького інтерфейсу (user interface, UI/UX) й виконується у фоновому режимі, як правило, не має аудіовізуальної форми, окрім, власне, закодованого запису даних.

За автентичністю електронні (цифрові) сліди варто поділити на незмінні (оригінальні, автентичні) й такі, що зазнали впливу (зміни) з метою приховування ознак кримінального правопорушення. Британські науковці радять ураховувати можливості осіб, які вчиняють кібератаки, протидіяти розслідуванню (в оригіналі «use anti-forensic techniques», у перекладі з англійської – застосовувати протикриміналістичні техніки). На думку цитованих авторів, застосування певних технік дозволяє зловмисникам приховувати, видаляти чи частково змінювати сліди своєї діяльності, що може призвести до хибних

висновків під час дослідження доказів [13, с. 14]. Г. Хорсман та Д. Ерріксон наводять шість популярних протикриміналістичних технік кіберзлочинців: приховування, видалення, розмиття, маскування та доповнення даних, а також фізичне знищення їх носія [3, с. 569]. Кожна з наведених форм впливу на електронні (цифрові) сліди змінює їх характерним чином, що дає змогу в подальшому встановити факт і форму такого впливу та спробувати відновити оригінальні дані.

За можливістю доступу електронні (цифрові) сліди доцільно поділити на незахищені та захищені. Доступ до перших із них не обмежується системою, тоді як операції з другими можуть бути обмежені засобами логічного захисту: паролем доступу, додатковим шифруванням, обмеженнями на зміну, видалення чи копіювання тощо. Подолання логічного захисту для дослідження й вилучення таких слідів потребує залучення спеціаліста чи направлення носія даних для проведення судової експертизи комп'ютерної техніки і програмних продуктів.

Класифікація електронних (цифрових) слідів за критеріями, що характеризують носій даних (слідосприймаючий об'єкт)

За місцем розташування носія комп'ютерних даних варто виокремити електронні (цифрові) сліди, що містяться на локальних носіях, та сліди, що містяться на віддалених носіях. У першому випадку носій даних чи комп'ютер, частиною якого є носій, перебуває у межах фізичного доступу уповноважених осіб та може бути безпосередньо досліджений, скопійований чи вилучений у натурі. У другому випадку електронні (цифрові) сліди містяться на носії, що розміщений поза межами фізичної досяжності уповноважених осіб, але доступ до якого може бути отримано віддалено (наприклад, сервери поштових служб, месенджерів, хмарних сховищ, що розміщені на території інших держав; носії, місце розміщення яких невідоме, тощо). Досить часто унаслідок роботи одного приладу можуть утворюватись електронні (цифрові) сліди одночасно на локальних та віддалених носіях. Зокрема, як зазначають Ф. Сервіда та Е. Кейсі, пристрої інтернету речей (розумні сенсори, камери, датчики й трекери тощо) можуть утворювати сліди у власній пам'яті, у пам'яті смартфона, до якого вони під'єднані, та на віддалених серверах [14, с. 23]. Якщо сліди, що містяться на віддалених носіях, публічно доступні через мережу «Інтернет», вони мають бути оглянуті з використанням службового комп'ютера й програми інтернет-браузера та зафіксовані у протоколі огляду комп'ютерних даних у формі, придатній для сприйняття їх змісту. В інших випадках уповноважені особи мають отримувати фізичний доступ до відповідного обладнання.

У свою чергу, сліди, що містяться на віддалених носіях, доцільно поділити на розміщені на носіях у межах національної юрисдикції органу досудового розслідування та розміщені на носіях поза її межами (на території інших держав). Дослідники зазначають, що кіберзлочини дуже часто є міжнародними, не підпадають під єдину національну юрисдикцію, а комп'ютери правопорушника та потерпілого можуть знаходитися на територіях різних держав [15, с. 268]. Процедури отримання фізичного доступу до таких носів можуть суттєво відрізнятися та вимагати проведення часозатратних процесуальних заходів у межах міжнародної взаємодії.

За призначенням та типом встановлення носія електронні (цифрові) сліди розподіляють на такі, що містяться на внутрішніх та зовнішніх носіях. Зовнішні носії призначені для зберігання даних поза межами електронно-обчислювального приладу та використовуються для переміщення інформації між такими приладами (CD, DVD-диски, USB флеш-диски, флеш-карти пам'яті, зовнішні жорсткі диски тощо). Внутрішні носії призначені для зберігання даних у межах електронно-обчислювального приладу й забезпечення його роботи, розміщуються всередині корпуса комп'ютера та, у свою чергу, поділяються на від'єднувані та невід'єднувані. Від'єднувані внутрішні носії обладнані необхідними інтерфейсами підключення та можуть бути вилучені з корпуса одного комп'ютерного пристрою й підключені до іншого (внутрішні жорсткі диски, модулі оперативної пам'яті). Сліди, що містяться на зовнішніх та деяких від'єднуваних внутрішніх носіях, можуть вилучатися разом із носієм та досліджуватися з використанням службових комп'ютерів уповноважених осіб. Невід'єднувані внутрішні носії являють собою чіпи пам'яті, розпаяні на платах усередині електронно-обчислювального пристрою (флеш-пам'ять мобільних пристроїв, роутерів, побутової техніки, кеш-пам'ять процесорів та ін.). За загальним правилом дані, що містяться на подібних чипах, копіюються або досліджуються з використанням приладу, частиною якого вони є.

За енергозалежністю запам'ятовувального пристрою носія даних можна виокремити електронні (цифрові) сліди, що містяться на енергозалежних та на енергонезалежних носіях. Деякі запам'ятовувальні пристрої для роботи потребують постійного електричного живлення, тобто є енергозалежними (наприклад, оперативна пам'ять DRAM та SRAM, кеш-пам'ять процесорів тощо). Описані носії здатні забезпечити більш високі швидкості читання та запису даних, проте не придатні для їх довгострокового зберігання. Після від'єднання живлення від такого пристрою вся інформація у його пам'яті втрачається. Через це дані, що містяться на енергозалежних носіях, потребують специфічного поводження: їх потрібно скопіювати, поки пристрій

увімкнено, або вилучити сам пристрій, забезпечуючи його живлення (наприклад, вилучення ноутбуків, смартфонів, іншої техніки, що має вбудовані акумулятори, включеними задля збереження даних у оперативній пам'яті). О. В. Манжай наголошує, що в енергозалежних запам'ятовувальних пристроях часто містяться чи не найважливіші для розслідування дані: ключі до різних криптоконтейнерів, останні повідомлення в мережі, відкриті документи тощо [16, с. 116]. У свою чергу, енергонезалежні носії не потребують постійного живлення, а дані, що вони містять, не втрачаються із від'єднанням від живлення. Прикладами таких носіїв є HDD та SSD диски, флеш-пам'ять, лазерні (оптичні) CD, DVD, Blue-Ray диски тощо.

Висновки

Підсумовуючи викладене, зазначимо, що електронні (цифрові) сліди кримінального правопорушення доцільно поділити на різновиди за трьома основними групами критеріїв: за ознаками, що характеризують слідоутворюючий об'єкт; за ознаками, що характеризують, власне, комп'ютерні дані як слід; та за ознаками, що характеризують носій таких даних (слідосприймаючий об'єкт) на момент їх виявлення.

За слідоутворюючим об'єктом такі сліди можна поділити на утворені внаслідок отримання ввідних даних і команд від користувача та утворені внаслідок виконання електронно-обчислювальною технікою заздалегідь закладених алгоритмів.

За критеріями, що характеризують, власне, комп'ютерні дані як слід, запропоновано такі підстави класифікації. За форматуванням даних електронні (цифрові) сліди варто поділити на форматовані та неформатовані. За змістом даних досліджувані сліди пропонується поділяти на основні дані та метадані. За способом сприйняття інформації можна виокремити електронні (цифрові) сліди, що несуть інформацію в аудіовізуальній формі, та дані без аудіовізуальної форми. За автентичністю досліджувані сліди варто поділити на незмінні (оригінальні, автентичні) й такі, що зазнали впливу (зміни) з метою приховування ознак кримінального правопорушення. За можливістю доступу електронні (цифрові) сліди доцільно поділити на незахищені та захищені.

За критеріями, що характеризують носій даних (слідосприймаючий об'єкт, запропоновано такі підстави класифікації. За місцем розташування носія комп'ютерних даних варто виокремити електронні (цифрові) сліди, що містяться на локальних носіях, та сліди, що містяться на віддалених носіях, які, у свою чергу, можна розділити на віддалені носії, розміщені в межах національної юрисдикції органу досудового розслідування, та поза її межами

(на території інших держав). За призначенням та типом встановлення носія електронні (цифрові) сліди розподіляють на такі, що містяться на внутрішніх та зовнішніх носіях. Внутрішні носії можуть бути поділені на від'єднувані та невід'єднувані. Нарешті, за енергозалежністю запам'ятовувального пристрою носія даних можна виокремити електронні (цифрові) сліди, що містяться на енергозалежних та на енергонезалежних носіях.

На нашу думку, перспективними є наукові дослідження щодо подальшого розподілу електронних (цифрових) слідів кримінальних правопорушень на підвиди та формулювання практико-орієнтованих рекомендацій щодо їх виявлення, збирання, дослідження й використання у кримінальному провадженні.

Список використаних джерел

[1] Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. № 1(77). С. 168–175.

[2] Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304–307. https://doi.org/10.32849/2663-5313/2019.5.56.

[3] Horsman G., Errickson D. When finding nothing may be evidence of something: Anti-forensics and digital tool marks. *Science & Justice*. 2019. Vol. 59, issue 5. P. 565–572. https://doi.org/10.1016/j.scijus.2019.06.004.

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

[5] Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. Вип. 1. С. 176–180. https://doi.org/10.32782/klj/2022.1.27.

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

[7] Reedy P. Interpol review of digital evidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520. https://doi.org/10.1016/j.fsisyn.2020.01.015.

[8] Гринько Л. П. «Слідова картина» шахрайств, вчинених через мережу Інтернет. *Полтавський правовий часопис*. 2022. № 3. С. 16–27.

[9] Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2022. № 4(100). С. 226–236. https://doi.org/10.33766/2524-0323.100.236-246.

[10] Horsman G. Raiders of the lost artefacts: Championing the need for digital forensics research. *Forensic Science International: Reports*. 2019. Vol. 1. November 2019, 100003. P. 1–5. https://doi.org/10.1016/j.fsir.2019.100003.

[11] Jieon Kim, Jungheum Park, Sangjin Lee. An improved IoT forensic model to identify interconnectivity between things. *Forensic Science International: Digital Investigation*.

2023. Vol. 44. March 2023, 301499. P. 1–13. https://doi.org/10.1016/j.fsidi.2022.301499.

[12] Коробець М. В., Коробець Р. М. Використання можливостей WI-FI роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник*. 2022. № 2(38). С. 36–47. https://doi.org/10.37025/1992-4437/2022-38-2-36.

[13] Antonia Nisioti, George Loukas, Alexios Mylonas, Emmanouil Panaousis. Forensics for multi-stage cyber incidents: Survey and future directions. *Forensic Science International: Digital Investigation*. 2023. Vol. 44. March 2023, 301480. P. 1–16. https://doi.org/10.1016/j.fsidi.2022.301480.

[14] Fracesco, Servida, Eoghan, Casey. IoT forensic challenges and opportunities for digital traces. *Digital Investigation*. 2019. Vol. 28, Supplement, April 2019. P. 22–29. https://doi.org/10.1016/j.diin.2019.01.012.

[15] Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investiga*. 2022. Vol. 11, issue 53. P. 259–269. https://doi.org/10.34069/AI/2022.53.05.26.

[16] Манжай О. В. Особивості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111–120.

References

[1] Avdieieva, H.K., & Storozhenko, S.V. (2017). Electronic traces: concepts and types. *Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko*, 1(77), 168-175.

[2] Naidon, Ya. (2019). Concept and classification of virtual traces of cybercrimes. *Entrepreneurship, Economy and Law*, 5, 304-307. https://doi.org/10.32849/2663-5313/2019.5.56.

[3] Horsman, G., & Errickson, D. (2019). When finding nothing may be evidence of something: Anti-forensics and digital tool marks. *Science & Justice*, 59(5), 565-572. https://doi.org/10.1016/j.scijus.2019.06.004.

[4] Samoilenko, O.A. (2020). Fundamentals of the methodology of investigation of crimes committed in cyberspace. A.F. Volobuyev (Ed.). Odesa: TES.

[5] Kolodina, A.S., & Fedorova, T.S. (2022). Digital forensics: problems of theory and practice. *Kyiv Journal of Law*, 1, 176-180. https://doi.org/10.32782/klj/2022.1.27.

[6] Stepaniuk, R.L., & Perlin, S.I. (2022). Digital forensics and improvement of the forensic technlogy system in Ukraine. *Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko*, 3(99), 283-294. https://doi.org/10.33766/2524-0323.99.283-284.

[7] Reedy, P. (2020). Interpol review of digital evidence 2016–2019. *Forensic Science International: Synergy,* 2, 489-520. https://doi.org/10.1016/j.fsisyn.2020.01.015.

[8] Hrynko, L.P. (2022). "Trace pictur" of fraud on the Internet. *Poltava Law Review*, 3, 16-27.

[9] Kovalenko, A.V. (2022). Concept and essence of electronic (digital) traces of criminal offenses *Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko*, 4(100), 226-236. https://doi.org/10.33766/2524-0323.100.236-246.

[10] Horsman, G. (November, 2019). Raiders of the lost artefacts: Championing the need for digital forensics research. *Forensic Science International: Reports*, 1, 100003, 1-5. https://doi.org/10.1016/j.fsir.2019.100003.

[11] Jieon, Kim, Jungheum, Park, & Sangjin, Lee. (March, 2023). An improved IoT forensic model to identify interconnectivity between things. *Forensic Science International: Digital Investigation,* 44, 301499, 1-13. https://doi.org/10.1016/j.fsidi.2022.301499.
[12] Korobets, M.V., & Korobets, R.M. (2022). Using WI-FI routers capabilities detection and investigation of criminal offenses. *Forensic Herald*, 2(38), 36-47. https://doi.org/10.37025/1992-4437/2022-38-2-36.
[13] Antonia Nisioti, George Loukas, Alexios Mylonas, & Emmanouil Panaousis. (March, 2023). Forensics for multi-stage cyber incidents: Survey and future directions. *Forensic Science International: Digital Investigation*, 44, 301480, 1-16. https://doi.org/10.1016/j.fsidi.2022.301480.
[14] Fracesco, Servida, & Eoghan, Casey. (April, 2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation*, Vol. 28, Supplement, 22-29. https://doi.org/10.1016/j.diin.2019.01.012.
[15] Pohoretskyi, M., Cherniak, A., Serhieieva, D., Chernysh, R., & Toporetska, Z. (2022). Detection and proof of cybercrime. *Amazonia Investiga*, 11(53), 259-269. https://doi.org/10.34069/AI/2022.53.05.26.
[16] Manzhai, O.V. (2016). Features of computer technique facilities examination. *Bulletin of Kharkiv National University of Internal Affairs*, 3(74), 111-120.

Артем Володимирович Коваленко
кандидат юридичних наук, доцент,
професор кафедри поліцейської діяльності
Луганський навчально-науковий інститут імені Е. О. Дідоренка
Донецького державного університету внутрішніх справ
76005, вул. Національної Гвардії, 3, Івано-Франківськ, Україна
e-mail: new4or@gmail.com
ORCID 0000-0003-3665-0147

Artem V. Kovalenko
Ph.D. in Law, Associate Professor,
Professor in the Department of Police Activities
Luhansk Educational & Scientific Institute named after E. Didorenko
of the Donetsk State University of Internal Affairs
76005, 3 Natsional'noi Hvardii Str., Ivano-Frankivsk, Ukraine
e-mail: new4or@gmail.com
ORCID 0000-0003-3665-0147

Рекомендоване цитування: Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. https: //doi.org/10.21564/2414-990X.161.278117.

Suggested Citation: Kovalenko, A.V. (2023). Classification of Electronic (Digital) Traces of Criminal Offenses. *Problems of Legality,* 161, 202-214. https: //doi.org/10.21564/2414-990X. 161.278117.

Статтю подано / Submitted: 01.05.2023
Доопрацьовано / Revised: 18.05.2023
Схвалено до друку / Accepted: 25.05.2023
Опубліковано / Published: 30.06.2023