УДК 343.983.2:004.353.24 doi: https://doi.org/10.33270/01191134.15

Орлов Ю. Ю. – доктор юридичних наук, старший науковий співробітник, головний науковий співробітник відділу організації наукової роботи та захисту прав інтелектуальної власності Національної академії внутрішніх справ, м. Київ
ORCID: https://orcid.org/0000-0001-7696-4744

Електронне відображення як криміналістичний об'єкт

Метою *статті є дослідження електронного відображення як криміналістичного об'єкта, з'ясування сутності електронних слідів, механізмів слідоутворення, особливостей виявлення, фіксації та ідентифікації електронних слідів.* ***Методологія.*** *Для досягнення мети статті, наукової обґрунтованості й об'єктивності її результатів було застосовано загальні та спеціальні методи, серед яких: аналіз, синтез, пояснення, порівняння, дедукція, індукція тощо. Досліджено сутність поняття матеріальних слідів в інформаційно-телекомунікаційній системі як комбінації станів упорядкованої низки елементарних носіїв інформації в пристрої пам'яті цієї системи. Запропоновано визначати ці сліди як двійкові коди інформації в «чистому вигляді», не прив'язаної до конкретного матеріального носія. Акцентовано на інтегральній (комбінаторній) сутності цих слідів, що надає їм унікальності. Зазначено, що матеріальний слід в елементарному носієві інформації не має індивідуальних криміналістичних ознак.* ***Наукова новизна.*** *Запропоновано визначити поняття електронного сліду як відображення на моніторі обчислювального пристрою матеріального сліду в інформаційно-телекомунікаційній системі. Рекомендовано розглядати електронне відображення як форму вияву електронних слідів. Обґрунтовано думку щодо ідеальної природи електронних слідів. Доведено помилковість тлумачення електронних слідів як слідів віртуальних. Аргументовано, що інтегральна (комбінаторна) природа матеріальних слідів в інформаційно-телекомунікаційній системі дає підстави вважати їх та створювані ними електронні сліди такими, що набувають індивідуальних криміналістичних ознак через неповторність двійкових кодів, завдяки чому можуть бути придатними для криміналістичної ідентифікації. Досліджено особливості виявлення та фіксації електронних слідів. Встановлено, що їх виявлення та фіксацію проводять за спеціальними методиками шляхом застосування програмного забезпечення загального і спеціального призначення.* ***Висновки.*** *Узагальнено, що сліди в елементарних носіях інформації не мають індивідуальних криміналістичних ознак. Проте їхня інтегральна (комбінаторна) природа дає підстави стверджувати, що матеріальні сліди в інформаційно-телекомунікаційній системі та створювані ними електронні сліди набувають цих ознак і можуть бути придатними для криміналістичної ідентифікації. Виявлення та фіксацію електронних слідів здійснюють за спеціальними методиками шляхом застосування програмного забезпечення загального та спеціального призначення. Наявні проблеми щодо виявлення та фіксації електронних слідів потребують законодавчого врегулювання. Електронні відображення мають загальні й окремі ідентифікуючі ознаки. Ідентичні електронні сліди можуть мати відмінності за окремими ознаками через їхню динамічну природу.*

Ключові слова: електронне відображення; криміналістика; криміналістичний об'єкт; криміналістична ідентифікація; двійковий код; доказ.

Вступ

Електронне відображення має унікальну сукупність властивостей, що дає підстави вважати його самостійним джерелом доказів у кримінальному провадженні. Така наукова позиція уможливлює внесення відповідних змін у ч. 2 ст. 84 КПК України, про що автор зазначає в статті, присвяченій дослідженню процесуального змісту електронних відображень (Orlov, & Cherniavskyi, 2017).

Електронне відображення хоча й отримало наукову інтерпретацію в теорії кримінального процесу, однак не було системно вивчено як криміналістичний об'єкт.

Мета і завдання дослідження

Необхідність кваліфікованого розслідування кіберзлочинів та інших кримінальних правопорушень, учинених із використанням інформаційно-телекомунікаційних технологій, актуалізує дослідження важливих питань теоретичного та прикладного спрямування, зокрема:

– як необхідно тлумачити поняття «електронний слід»;

– яким є механізм слідоутворення;

– як можна виявляти та фіксувати електронні сліди;

– які ідентифікуючі ознаки можна виокремити в цих слідах;

– які особливості ідентифікації електронних відображень.

Виклад основного матеріалу

Передусім слід визначити базове поняття «електронний слід».

Видатний учений-криміналіст І. М. Якимов розглядав слід як «відтиск на будь-чому предмета, що надає можливість робити висновок про його форму або призначення» (Iakimov, 1935, p. 44), трактуючи його як слід-відображення. Аналогічну позицію обстоював і Б. І. Шевченко, розуміючи слід як «відображення зовнішньої будови матеріальних об'єктів» (Shevchenko, 1947, p. 5-6). Цей підхід було

обрано за основу сучасної класифікації слідів в українській криміналістиці[1].

За часів формування наукового визначення сліду як криміналістичного поняття не існувало інформаційно-телекомунікаційних мереж, тому сучасні спроби науковців відобразити процес та особливості слідоутворення в таких мережах з позицій класичної трасології спричиняють складнощі. Вони пов'язані з тим, що слід, який злочинець залишає в інформаційно-телекомунікаційній системі, має низку унікальних особливостей, які необхідно встановити й описати на науковому рівні.

По-перше, слід в інформаційно-телекомунікаційній системі фізично існує у вигляді певних змін на магнітному або електронному носієві[2], який знаходиться в складі мережевого сервера, окремого комп'ютера, термінала мобільного зв'язку або ж є автономним. Цей слід становить комбінацію індивідуальних стандартних станів низки так званих елементарних носіїв інформації.

Слідоутворення на магнітному й електронному носієві відбувається за схожим зразком. Так, на магнітному носієві (на жорсткому диску комп'ютера, в автономному вінчестері тощо) елементарним носієм інформації є домени (дискретні області) у пласті феромагнетика, яким покрито диск. Намагнічування кожного із цих доменів здійснює магнітна головка накопичувача в одному з двох протилежних напрямів. Залежно від напряму намагніченості інформаційна система сприймає домен як логічний «0» або логічну «1».

В електронному носієві (флеш-накопичувачах, картах пам'яті тощо) елементарним носієм інформації є спеціалізований мікроскопічний пристрій у складі мікросхеми пам'яті – транзистор з плаваючим затвором. Кожен із цих транзисторів може знаходитися в одному з двох сталих станів, що визначають наявність або відсутність від'ємного електричного заряду на плаваючому затворі; інформаційна система сприймає їх як логічний «0» або логічну «1». Запис інформації на електронний носій відбувається шляхом подання електричної напруги на транзисторні переходи «витік (стік) – підкладка», що зумовлює так званий лавинний пробій цих переходів.

З огляду на природу цих слідів, умовимося називати їх *матеріальними слідами в інформаційно-телекомунікаційній системі*.

Зауважимо, що лінійні розміри елементарних магнітних носіїв інформації нині сягають 5×10^{-8} м, електронних – 10^{-8} м. У зв'язку з мікроскопічними розмірами цих носіїв, матеріальні сліди в інформаційно-телекомунікаційній системі формально можна розглядати як мікросліди.

По-друге, особливості «хмарних» технологій, які використовують в інформаційно-телекомунікаційних мережах, передбачають, зокрема, автоматичний (не контрольований людиною) перезапис інформації з одного носія на інший під час обчислювального процесу з метою його оптимізації. Таким чином, слід в інформаційно-телекомунікаційній мережі в загальному випадку не прив'язаний до конкретного матеріального носія. Отже, на відміну від класичного об'єкта трасології, матеріальний слід в елементарному носієві інформації позбавлений будь-яких індивідуальних криміналістичних ознак, які традиційно визначені саме носієм. Такий слід є інформацією в «чистому вигляді».

По-третє, стан окремого елементарного носія інформації не можна вважати слідом у загальноприйнятому значенні, оскільки він сам по собі не містить криміналістичної інформації. Про матеріальний слід в інформаційно-телекомунікаційній системі в контексті криміналістики можна говорити лише як про комбінацію станів упорядкованої низки елементарних носіїв інформації, яка утворює певний цифровий код. Тобто природа матеріальних слідів в інформаційно-телекомунікаційній системі є *інтегральною*.

По-четверте, у магнітному накопичувачі сучасного побутового комп'ютера знаходиться близько 10^{12} елементарних носіїв інформації, на флеш-накопичувачі – до 10^{11}, у терміналі мобільного зв'язку – до 10^{10}, а в Інтернет-мережі загалом кількість цих носіїв сягає астрономічної величини – 10^{21}. Відповідно, кількість унікальних комбінацій індивідуальних стандартних станів елементарних носіїв інформації (які корелюються з кількістю різних за інформаційним змістом слідів, що можуть бути сформовані) лише в одному побутовому комп'ютері сягає $\sim 2^{1000000000000}$, що становить величезне число, яке має близько 100 млрд цифр[3]. Отже, кожен матеріальний слід в інформаційно-

[1] Є й інші погляди на тлумачення поняття «сліди». Так, Д. А. Турчин, виокремлює не лише сліди відображення, а й сліди у вигляді якісних і кількісних змін, сліди у вигляді відношень між об'єктами, просторово-часові сліди, сліди у вигляді наявності чи відсутності предметів, явища, що виконують роль слідів, а також мікросліди (Turchin, 1983, p. 91); О. О. Волобуєва поділяє сліди на сліди-відображення, сліди-предмети та сліди-речовини (Volobuiev, 2011, p. 81).

[2] У сучасних інформаційних системах застосовують магнітні й електронні носії інформації, оскільки вони забезпечують сучасні вимоги щодо ємності, швидкодії та надійності. З розвитком технологій можливою є поява носіїв інформації, що використовуватимуть інші фізичні принципи.

[3] Для точнішого обчислення загальної кількості потенційно можливих матеріальних слідів у пам'яті комп'ютера необхідно враховувати не лише різні комбінації станів елементарних носіїв інформації, а й можливі варіанти їх розміщення на носієві. Тому насправді загальна кількість слідів виявляється суттєво більшою і становить $\sum_{k=0}^{n} A_n^k = \sum_{k=0}^{n} \frac{n!}{(n-k)!}$, де $n = 10^{12}$. Це число неможливо відобразити в явному вигляді, оскільки лише кількість цифр у ньому сягає астрономічного числа довжиною понад трильйон знаків.

телекомунікаційній системі, не маючи індивідуальних криміналістичних ознак у класичному їх розумінні, *є унікальним через свою інтегральну (комбінаторну) природу*. З математичної позиції це двійковий код, який зазвичай має довжину від кількох тисяч до кількох мільярдів розрядів. Так, для файлу довжиною 1 кілобайт (близько півсторінки тексту без урахування формату) імовірність повного збігу двійкового коду (що відповідає детальній підробці файлу) становить надзвичайно малу величину 10^{-2466}.

Це дає підстави стверджувати, що матеріальні сліди в інформаційно-телекомунікаційній системі принципово можуть бути використані для виконання завдань з криміналістичної ідентифікації після розроблення відповідних методик.

Водночас ці сліди мають унікальні особливості, яких позбавлені класичні сліди-відображення, що не дає змогу безпосередньо застосувати для їх дослідження класичні підходи, напрацьовані криміналістичною практикою.

По-перше, на відміну від класичних слідів-відображень, матеріальний слід в інформаційно-телекомунікаційній системі *неможливо спостерігати безпосередньо*. Людина може сприймати його лише у вигляді віртуальної моделі на екрані комп'ютерного монітора чи монітора термінала мобільного зв'язку. Саме таку модель автор пропонує називати *електронним слідом*.

Питання моделювання в трасології досліджував Г. Л. Грановський. Учений визначав криміналістичну модель як «предмет або математичний опис, що є засобом фіксації речових доказів, зразків та інших об'єктів криміналістичного дослідження, який здатний замінити їх у процесі такого дослідження» (Granovskiy, 1974, p. 17). Розвиток технологій надає можливість розширити класичний перелік трасологічних моделей, до яких, окрім предметів і математичних описів, слід віднести також електронні відображення.

Коли йдеться про електронний слід, ми здебільшого маємо на увазі не власне слід на матеріальному носієві інформації, а його ідеальне відображення, сформоване електронною схемою комп'ютера. Тобто *електронний слід існує у формі електронного відображення*. З позицій теорії кримінального процесу слід в інформаційно-телекомунікаційній мережі, який стає доступним для безпосереднього спостереження, автор запропонував називати саме електронним відображенням і, з огляду на його специфічність, вважати самостійним видом доказів у кримінальному провадженні (Orlov, & Cherniavskyi, 2017).

По-друге, в інформаційно-телекомунікаційній системі є такі матеріальні сліди, які формують електронні відображення шляхом визначення алгоритмів функціонування відповідних комп'ютерів і мереж або ж позначаються на цих алгоритмах (це, зокрема, операційні системи, різноманітні прикладні комп'ютерні програми, комп'ютерні віруси тощо). Особливість їх полягає в тому, що вони можуть безпосередньо не відображатися на екрані монітора. Таким чином, електронний слід (тобто електронне відображення матеріального сліду в інформаційно-телекомунікаційній системі) необхідно розглядати в широкому значенні слова – не просто як «картинку» на моніторі, а як динамічний, змінюваний у часі процес. Цей процес може відображатися на екрані монітора як послідовність змінюваних зображень або ж узагалі не відображатися на екрані, допускати або не допускати участь оператора в цьому процесі. Зазначене ускладнює роботу з електронними слідами, потребує розроблення нетрадиційних методик щодо їх виявлення, фіксації та дослідження.

По-третє, електронні сліди існують виключно в так званому кіберпросторі, який визначено на рівні законодавства як «середовище (віртуальний простір), що надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» ("Zakon Ukrainy", 2017). Тому електронні сліди іноді називають «віртуальними слідами» (від лат. *virtualis* – можливий). На нашу думку, ця назва з наукової позиції є некоректною, оскільки електронний слід не є можливим (тобто таким, що не існує або ж спонтанно зникає). По-перше, він реально існує, як, наприклад, і показання свідка. По-друге, він придатний для відтворення в інформаційно-телекомунікаційній системі в будь-який момент часу. По-третє, його можна зафіксувати (наприклад, у вигляді скриншотів, роздруківок або окремих файлів).

Нематеріальний характер електронних слідів, їхня похідна природа (вони визначаються матеріальними слідами в інформаційно-телекомунікаційній системі), а також незалежність від матеріального носія (здатність до необмеженого копіювання без спотворення змісту) дають підстави віднести їх до категорії *ідеальних слідів*. Єдиними відомими нині в криміналістиці ідеальними слідами є сліди пам'яті людини. Вони також є нематеріальними, мають похідну природу (визначаються матеріальними змінами в нейронній структурі мозку) і в загальному випадку не залежать від матеріального носія (вони можуть необмежено передаватися від однієї людини до іншої під час спілкування) (Matijević, 2018).

Електронні сліди, як і показання свідка, виконують роль посередника між матеріальними слідами в інформаційно-телекомунікаційній системі

(слідами пам'яті людини в її мозку) й експертом або слідчим, який на підставі дослідження електронних відображень (відповідно – допиту особи) встановлює обставини, які підлягають доказуванню в кримінальному провадженні.

На підставі аналізу криміналістичної практики можна стверджувати, що під час передавання інформації від однієї особи до іншої ця інформація може зменшуватися в обсязі, а також зазнавати спотворень (Shapovalova, & Shapovalov, 2016). Це зумовлено суб'єктивізмом у сприйнятті й оцінюванні інформації людиною та особливостями передавання відомостей мовними засобами. Так, показання свідка, який був безпосереднім очевидцем події, є достовірнішими, повнішими й детальнішими, ніж показання особи, яка отримала інформацію про подію від такого очевидця. Саме тому похідні докази потребують додаткової перевірки.

Закономірним є питання про можливість спотворення інформації: 1) під час її автоматичного перезапису з одного носія на інший у процесі функціонування інформаційної мережі; 2) під час формування електронного відображення на екрані монітора. Від відповіді на ці питання буде залежати висновок стосовно достовірності електронних відображень як доказів у кримінальному провадженні.

Автоматичний перезапис інформації з одного матеріального носія на інший (наприклад, з одного на інший сервер) у нормальному режимі роботи інформаційної мережі здійснюється з абсолютною точністю та високим рівнем надійності. Технологія самоконтролю комп'ютерних вінчестерів S.M.A.R.T. (від англ. *self-monitoring, analysis and reporting technology* – технологія самоконтролю, аналізу й звітності), розроблена 1995 року й упроваджена в усі моделі пристроїв пам'яті, надає можливість оцінювати стан жорсткого диска безпосередньо в процесі його функціонування, відслідковувати можливі збої в роботі та в реальному масштабі часу повідомляти користувача. Аналогічні технології самоконтролю використовують у флеш-накопичувачах (тестувальна утиліта HDDScan, методи обчислення контрольних сум тощо). Автоматичний перезапис інформації з одного матеріального носія на інший під час реалізації «хмарних» мережевих технологій практично не позначається на її достовірності.

Водночас можна припустити, що спотворення інформації під час її автоматичного перезапису з одного матеріального носія на інший може відбутися внаслідок втручання людини. Проте для реалізації цього хакеру-правопорушнику доведеться «зламати» мережеву операційну систему, що є вельми ускладненим через підвищені безпекові вимоги, які висувають до таких систем (Shoroshev, & Khoroshko, 2007). Принаймні автору не відомі випадки вразливості найбільш популярної мережевої системи Windows Server унаслідок реальних хакерських атак. Розробники мережевих операційних систем постійно тестують свій продукт на вразливість і підвищують його захищеність від несанкціонованого втручання. Крім того, сумнівними видаються практична доцільність і технологічна оптимальність спотворення інформації людиною саме в процесі її автоматичного перезапису.

Отже, імовірність зловмисного спотворення електронних відображень людиною під час реалізації «хмарних» технологій є надзвичайно низькою. Очевидно, що вона є значно нижчою, ніж імовірність спотворення інформації, отриманої від свідка. Попри це, у разі виникнення підозри, що електронне відображення могло бути спотворене через несанкціоноване втручання в мережеву операційну систему, слідчий має призначити експертизу щодо встановлення факту такого втручання.

З огляду на викладене, можна стверджувати, що особливості «хмарних» технологій загалом не позначаються на достовірності електронних відображень як доказів.

Спробуємо відповісти на питання, чи може бути спотворено інформацію, записану на комп'ютерному носієві, у процесі формування відповідного електронного відображення на екрані монітора. Таке спотворення справді може відбуватися унаслідок впливу шкідливої комп'ютерної програми, яка міститься на комп'ютері, автономному носієві, сервері (якщо комп'ютер під'єднаний до інформаційної мережі) або в терміналі мобільного зв'язку.

Наявність у комп'ютері, терміналі зв'язку чи інформаційно-телекомунікаційній мережі шкідливих комп'ютерних програм (комп'ютерних вірусів) може позначатися на достовірності електронних відображень як доказів. Тому, за наявності підстав вважати отримане електронне зображення спотвореним унаслідок впливу комп'ютерних вірусів, слідчий має призначити комп'ютерно-технічну експертизу на предмет відсутності в комп'ютері (сервері, терміналі зв'язку) шкідливих програм. Водночас слід ураховувати, що кожен провайдер інтернет-послуг повсякчас здійснює профілактику своїх серверів задля запобігання можливим збоям функціонування через комп'ютерні віруси.

Процеси виявлення та фіксації електронних слідів передбачають нетрадиційні підходи, що пов'язано з унікальними особливостями цих об'єктів. Так, електронні сліди в інформаційній мережі можуть бути *виявлені* шляхом здійснення комп'ютерного пошуку в кіберпросторі. Під час пошуку в мережі необхідно враховувати, що встановити конкретний матеріальний носій електрон-

ного сліду не завжди можливо. Комп'ютерний пошук здійснюють за певними атрибутами, використовуючи можливості стандартних пошукових систем (Google, Yandex, Rambler, Yahoo!) через стандартні інтернет-браузери (Google Chrome, Mozilla Firefox, Internet Explorer, Opera тощо). Інструментарій і технології здійснення комп'ютерного пошуку проаналізовано в спеціальній літературі (Orlov, 2010; Orlov, Kukharenko, & Shkolnyi, 2011).

Пошук електронних слідів в окремому (автономному) комп'ютері здійснюють за певними атрибутами, використовуючи, зокрема, опції «Пошук» операційної системи Windows. Також може бути застосовано допоміжні спеціалізовані програми (наприклад, програма автоматичного збору інформації про апаратне і програмне забезпечення комп'ютерного засобу, яка є складовою дистрибутиву Ubuntu 16.04) (Havlovskyi et al., 2017, p. 31).

Властивості знайдених файлів і папок (авторство, дата й час створення, змінювання, останнього відкриття, дані архівації, контрольні суми тощо) встановлюють з використанням стандартних інструментів операційної системи (опція «Властивості»).

Фіксація електронних слідів у загальному випадку є складним завданням, яке виконують у різний спосіб залежно від виду електронних слідів, їхньої динамічності (змінюваності в часі), обставин виявлення тощо.

Фіксацію електронних слідів, виявлених в окремому комп'ютері, здійснюють шляхом копіювання змісту носіїв інформації, виготовлення скриншотів, здійснення фото- та відеофіксації роботи комп'ютерних програм, роздруківки електронних документів, опису в протоколі слідчої дії тощо. За необхідності використовують спеціалізоване програмне забезпечення. Наприклад, уже згадуваний нами дистрибутив Ubuntu 16.04 містить уніфікований набір програм, серед яких: 1) програма для запису відеограм екрана монітора XvidCap Screen Capture; 2) програма для підрахунку контрольних сум Hash Checker; 3) програма Tsclient 0.150 для віддаленого керування операційними системами Windows з підтримкою протоколу віддаленого робочого столу RDP (Remote Desktop Protocol); 4) програма для форматування підключених носіїв тощо (Havlovskyi et al., 2017, p. 31).

Фіксацію електронних слідів в інформаційній мережі здійснювати значно складніше у зв'язку з їх динамічністю (плинністю) і нелокальним характером. У цьому випадку важливо своєчасно зафіксувати певний слід, поки він назавжди не зник з мережі. Для розв'язання цієї проблеми видається доцільним внести зміни в чинне кримінальне процесуальне законодавство щодо врегулювання правовідносин органів розслідування з інтернет-провайдерами й операторами мобільного зв'язку. Досвід розвинених країн засвідчує доцільність процесуальної регламентації таких дій:

– негайне збереження інтернет-провайдером (оператором зв'язку) електронних відображень, які містять відомості, що можуть бути використані як доказ обставин, котрі підлягають доказуванню в кримінальному провадженні;

– зберігання (запис) інформації, що циркулює на певних інтернет-ресурсах або щодо певних IP-адрес, протягом визначеного часу (Orlov, & Cherniavskyi, 2017, p. 16).

Негайне збереження і тимчасовий запис мережевої інформації провайдер (оператор) має здійснювати на підставі вимоги слідчого, прокурора, слідчого судді або суду. Доступ сторонам кримінального провадження до збереженої інформації провайдер (оператор зв'язку) має надавати на підставі ухвали слідчого судді, суду за умов і в порядку, передбаченому ст. 159–166 КПК України.

З огляду на особливості електронних слідів, процес їх *криміналістичної ідентифікації* набуває нового змісту, який виходить за межі традиційної парадигми. З позицій класичної експертології він мав би полягати у встановленні ідентичності (збігу) цифрових кодів, записаних на різних матеріальних носіях інформації: у запам'ятовувальному пристрої інформаційної системи й на автономному носієві, який містить зразок для порівняльного дослідження. Проте, оскільки ці коди зазвичай не є доступними для безпосереднього спостереження, ідентифікацію мають пройти електронні відображення цих матеріальних слідів[1].

Матеріальні сліди в інформаційно-телекомунікаційній системі не мають індивідуальних криміналістичних ознак, проте через свою інтегральну (комбінаторну) природу вони утворюють унікальні ідеальні образи (двійкові коди). Ця унікальність (неповторність) кодів дає змогу здійснювати їх порівняння (ідентифікацію). На думку автора, здатність до ідентифікації передається й електронним слідам, оскільки вони формуються на підставі відповідних двійкових

[1] В експертній практиці вже доводилося виконувати подібні завдання. З появою інформаційних технологій ідентифікаційні дослідження дактилоскопічних, балістичних та інших слідів почали проводити не на матеріальних об'єктах, а на їхніх електронних відображеннях, здійснюючи попереднє «оцифровування» зображень цих слідів. Отже, сучасні ідентифікаційні дослідження часто полягають у порівнянні трасологічних моделей у формі електронних відображень.

кодів. Ідентифікація електронних слідів, що мають ідеальну природу, є криміналістичною новацією, яка потребує розроблення необхідного нормативно-правового й методичного забезпечення[1].

Під час розроблення методик ідентифікації слід ураховувати, що електронні відображення часто є динамічними, тобто такими, що допускають змінювання в часі в процесі їх функціонування (наприклад, інтернет-сайти, прикладні комп'ютерні програми, електронні бази даних, трафіки чатів тощо). Отже, наявність відмінностей в електронних слідах не завжди може бути підставою для експертного висновку щодо їх неідентичності. Такі відмінності можна розглядати як хибні (Granovskiy, 1965, p. 85-86). Вирішуючи питання щодо суттєвості наявних відмінностей, слід з'ясувати, чи могли вони виникнути внаслідок природного функціонування електронного відображення. У загальному випадку предметом ідентифікаційного дослідження мають стати: 1) змістовне наповнення електронного відображення; 2) програмний інтерфейс як система засобів спілкування з користувачем; 3) алгоритм функціонування електронного відображення. Зазначені особливості необхідно враховувати під час створення методик ідентифікації електронних відображень різних типів (інтернет-сайтів, баз даних, текстових, фото- й відеофайлів, змісту електронної пошти та месенджерів, вихідних і виконуваних модулів комп'ютерних програм, трафіків комунікацій тощо).

В електронних відображеннях, так само як і в інших об'єктах криміналістичної ідентифікації, можна виокремити загальні й окремі (індивідуальні) ідентифікуючі ознаки. Загальні ознаки втілюють суттєві властивості відображення та надають можливість визначити його тип (групу). Для певного типу комп'ютерної програми й інтернет-сайту загальною ознакою може бути алгоритм функціонування; для баз даних, текстових файлів і трафіків комунікацій – форма подання даних та їх загальний зміст тощо. Окремі ознаки відтворюють властивості певних частин, елементів досліджуваних електронних відображень і дають змогу виокремити певне відображення з групи однорідних. Для комп'ютерної програми цими ознаками можуть бути особливості функціонування певних опцій, налаштування користувача тощо; для баз даних і текстових файлів – час внесення змін, відмінності у форматі окремих частин тексту, наявність унікальної інформації тощо. У своїй сукупності спільно із загальними ознаками вони можуть бути покладені в основу ідентифікації. Водночас ідентичні електронні сліди можуть мати відмінності в окремих ознаках через їхню динамічну (змінювану) природу. Отже, відмінність у певних ознаках досліджуваного електронного відображення та зразка не завжди означатиме неідентичність порівнюваних відображень.

Перелік питань, які можуть бути поставлені перед експертом під час діагностичного дослідження, є необмеженим. Експертна практика не пішла шляхом виокремлення діагностичного дослідження електронного відображення як самостійного виду досліджень, а передбачає проведення його під час експертизи комп'ютерної техніки й програмних продуктів, регламентованої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5 ("Nakaz Ministerstva yustytsii", 1998). До орієнтовного переліку вирішуваних цією експертизою питань належать, зокрема, такі:

– чи міститься на цьому носієві певна інформація та в якому вигляді;

– чи містить носій досліджуваного комп'ютера інформацію про певні дії користувача;

– чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації;

– чи могла бути створена зазначена інформація на цьому комп'ютері, чи її перенесено з іншого носія;

– яким чином певна інформація перенесена до досліджуваного комп'ютера (носія);

– чи містить накопичувач інформації досліджуваного комп'ютера певне програмне забезпечення.

Деякі питання цієї експертизи стосуються безпосередньо дослідження властивостей і можливостей електронних відображень, зокрема:

– яка технологія та хронологія створення певного електронного документа;

– які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять певну інформацію;

– чи можливим є виконання певних дій за допомогою цього програмного продукту;

– чи можливо виконати певне завдання за допомогою цього програмного продукту;

– чи реалізовано в цьому програмному продукті (програмному коді) функції, передбачені технічним завданням на його розроблення.

Завдання діагностичного дослідження виконують здебільшого з використанням широкого спектру стандартних можливостей операційної системи комп'ютера, застосовуючи за необхідності спеціалізовані утиліти (диспетчери файлів, диспетчери завдань, переглядачі, діагностики апаратного та програмного забезпечення тощо).

Наукова новизна

У статті запропоновано поняття електронного сліду як відображення на моніторі обчислю-

[1] У судовій практиці застосовують процедуру, яка віддалено нагадує процес ідентифікації ідеальних слідів. Ідеться про встановлення допустимості як доказів показань із чужих слів відповідно до ст. 97 КПК України.

вального пристрою матеріального сліду в інформаційно-телекомунікаційній системі. Рекомендовано розглядати електронне відображення як форму вияву електронних слідів. Обґрунтовано думку щодо ідеальної природи електронних слідів. Доведено помилковість тлумачення електронних слідів як слідів віртуальних. Аргументовано, що інтегральна (комбінаторна) природа матеріальних слідів в інформаційно-телекомунікаційній системі дає підстави вважати їх і створювані ними електронні сліди такими, що набувають індивідуальних криміналістичних ознак через неповторність двійкових кодів і завдяки чому можуть бути придатними для криміналістичної ідентифікації. Досліджено особливості виявлення та фіксації електронних слідів. Встановлено, що їх виявлення та фіксацію проводять за спеціальними методиками шляхом застосування програмного забезпечення загального і спеціального призначення.

Висновки

Викладене дає підстави для таких висновків:

1. Матеріальний слід в інформаційно-телекомунікаційній системі – це двійковий код у її запам'ятовувальному пристрої, який утворюється шляхом зміни фізичного стану низки елементарних носіїв інформації.

2. Електронний слід – це ідеальне електронне відображення (статичне чи динамічне) на моніторі обчислювального пристрою (комп'ютера, термінала мобільного зв'язку тощо) матеріального сліду в інформаційно-телекомунікаційній системі.

3. Сліди в елементарних носіях інформації не мають індивідуальних криміналістичних ознак. Проте їхня інтегральна (комбінаторна) природа дає підстави стверджувати, що матеріальні сліди в інформаційно-телекомунікаційній системі та створювані ними електронні сліди набувають цих ознак і можуть бути придатними для криміналістичної ідентифікації.

4. Виявлення та фіксацію електронних слідів здійснюють за спеціальними методиками шляхом застосування програмного забезпечення загального та спеціального призначення. Наявні проблеми щодо виявлення та фіксації електронних слідів потребують законодавчого врегулювання.

5. Електронні відображення мають загальні й окремі ідентифікуючі ознаки. Водночас ідентичні електронні сліди можуть мати відмінності в окремих ознаках через їхню динамічну природу.

REFERENCES

Granovskii, G.L. (1974). *Osnovy trasologii. Osobennaia chast [The basics of trasology. Special part].* Moscow: VNII MVD SSSR [in Russian].

Granovskiy, G.L. (1965). *Osnovy trasologii. Osobennaia chast [The basics of trasology. Special part].* Moscow: VNII MVD SSSR [in Russian].

Havlovskyi, V.D., Hutsaliuk, M.V., & Khakhanovskyi, V.H. (et al.). (2017). *Osoblyvosti vykorystannia elektronnykh tsyfrovykh dokaziv u kryminalnykh provadzhenniakh [Features of the use of electronic digital evidence in criminal proceedings]*. M.V. Hrebeniuk (Eds.). Kyiv: MNDTs pry RNBO Ukrainy [in Ukrainian].

Iakimov, I.N. (1935). *Osmotr [Inspection].* Moscow [in Russian].

Matijević, M. (2018). Kriminalistika - otkrivanje i dokažuvanje (T. I, II) (vrijeme prolazi, djela ostaju) [Criminology - Detection and Proof (Volume I, II) (time passes, works remain)]. *Bezbjednost Policija Građani, Security Police Citizens, 12(3-4),* 3-23. doi: https://doi.org/10.7251/bpg1603003m [in Serbian].

Nakaz Ministerstva yustytsii Ukrainy "Pro zatverdzhennia Instruktsii pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen ta Naukovo-metodychnykh rekomendatsii z pytan pidhotovky ta pryznachennia sudovykh ekspertyz ta ekspertnykh doslidzhen": vid 8 zhovt. 1998 r. No. 53/5 [Order of the Ministry of Justice of Ukraine "On approval of the Instruction on the appointment and conduct of forensics and expert studies and Scientific and methodological recommendations on the preparation and appointment of judicial expertise and expert studies" from October 8, 1998, No. 53/5]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/z0001-13. doi: https://doi.org/10.33498/louu-2019-09-117.

Orlov, Yu.Yu. (2010). *Osnovy taktyky poshuku informatsii kryminalnoho kharakteru v merezhi Internet [Fundamentals of tactics for finding criminal information on the Internet].* Kyiv: Kyiv. nats. un-t vnutr. sprav [in Ukrainian].

Orlov, Yu.Yu., & Cherniavskyi, S.S. (2017). Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni [Electronic display as a source of evidence in criminal proceedings]. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav, Law Journal of the National Academy of Internal Affairs, 1(13),* 12-24. Retrieved from https://lawjournal.naiau.kiev.ua/index.php/lawjournal/article/view/111 [in Ukrainian].

Orlov, Yu.Yu., & Cherniavskyi, S.S. (2017). Vykorystannia elektronnykh vidobrazhen yak dokaziv u kryminalnomu provadzhenni [Use of electronic displays as evidence in criminal proceedings]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav, Scientific Bulletin of the National Academy of Internal Affairs, 3(104),* 13-25. Retrieved from https://scientbul.naiau.kiev.ua/index.php/scientbul/article/view/612 [in Ukrainian].

Orlov, Yu.Yu., Kukharenko, S.V., & Shkolnyi, V.B. (2011). *Provedennia poshukovykh zakhodiv u merezhi Internet [Searching on the Internet].* (Vols. 1-2). O.M. Dzhuzhi (EDs.). Kyiv: Nats. akad. vnutr. sprav [in Ukrainian].

Shapovalova, G.M., & Shapovalov, V.V. (2016). Kriminalistika i ee rol v preduprezndenii prestupleniy na osnove informatsionnykh tekhnologiy [Forensics and its role in the prevention of crime based on information technology]. *Politseyskaia deiatelnost, Police activity, 2(2),* 187-199. doi: https://doi.org/10.7256/2222-1964.2016.2.17636 [in Russian].

Shevchenko, B.I. (1947). *Nauchnye osnovy sovremennoy trasologii [Scientific basis of modern trasology].* Moscow [in Russian].

Shoroshev, V.V., & Khoroshko, V.O. (2007). Systemy vyiavlennia atak na kompiuterni systemy [Systems for detecting attacks on computer systems]. *Zakhyst informatsii, Protection of information, 4(36), 9,* 5-10. doi: https://doi.org/10.18372/2410-7840.9.4124 [in Ukrainian].

Turchin, D.A. (1983). *Teoreticheskie osnovy ucheniia o sledakh v kriminalistike [Theoretical foundations of the doctrine of traces in forensics].* Vladivostok: Dalnevostoch. gos. un-t [in Russian].

Volobuiev, A.F. (Eds.). (2011). *Kryminalistyka [Criminalistics].* Kyiv: KNT [in Ukrainian].

Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy": vid 5 zhovt. 2017 r. No. 2163-VIII [Law of Ukraine "On the Fundamental Principles of Cyber Security of Ukraine" from October 5, 2017, No. 2163-VIII]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Грановский Г. Л. Основы трасологии. Особенная часть. М. : ВНИИ МВД СССР, 1974. 240 с.

Грановский Г. Л. Основы трасологии. Общая часть. М. : ВНИИ МВД СССР, 1965. 124 с.

Особливості використання електронних цифрових доказів у кримінальних провадженнях : метод. рек. / [В. Д. Гавловський, М. В. Гуцалюк, В. Г. Хахановський та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 70 с.

Якимов И. Н. Осмотр. М., 1935. 107 с.

Матијевић М. Криминалистика – откривање и докажување (Т. I, II) (вријеме пролази, дјела остају). *Безбједност Полиција Грађани.* 2018. Vol. 12. Issue 3–4. С. 3–23. doi: https://doi.org/10.7251/bpg1603003m.

Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: http://zakon3.rada.gov.ua/laws/show/z0001-13. doi: https://doi.org/10.33498/louu-2019-09-117.

Орлов Ю. Ю. Основи тактики пошуку інформації кримінального характеру в мережі Інтернет : метод. рек. Київ : Київ. нац. ун-т внутр. справ, 2010. 23 с.

Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1 (13). С. 12–24. URL: https://lawjournal.naiau.kiev.ua/index.php/lawjournal/article/view/111.

Орлов Ю. Ю., Чернявський С. С. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3 (104). С. 13–25. URL: https://scientbul.naiau.kiev.ua/index.php/scientbul/article/view/612.

Орлов Ю. Ю., Кухаренко С. В., Школьний В. Б. Проведення пошукових заходів у мережі Інтернет : метод. рек. : у 2 ч. / за заг. ред. О. М. Джужі. Київ : Нац. акад. внутр. справ, 2011. Ч. 2. 40 с.

Шаповалова Г. М., Шаповалов В. В. Криминалистика и ее роль в предупреждении преступлений на основе информационных технологий. *Полицейская деятельность.* 2016. № 2 (2). С. 187–199. doi: https://doi.org/10.7256/2222-1964.2016.2.17636.

Шевченко Б. И. Научные основы современной трасологии. М. : 1947. 54 с.

Шорошев В. В., Хорошко В. О. Системи виявлення атак на комп'ютерні системи. *Захист інформації.* 2007. № 4 (36). Т. 9. С. 5–10. doi: https://doi.org/10.18372/2410-7840.9.4124.

Турчин Д. А. Теоретические основы учения о следах в криминалистике : монография. Владивосток : Дальневост. гос. ун-т, 1983. 188 с.

Криміналістика : навч. посіб. / за ред. А. Ф. Волобуєва. Київ : КНТ, 2011. 504 с.

Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

Стаття надійшла до редколегії 09.09.2019

Orlov Yu. – Doctor of Laws, Senior Research Fellow, Chief Senior Research Fellow of the Department of Organization of Scientific Activity and Protection of Intellectual Property Rights of the National Academy of Internal Affairs, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-7696-4744

Electronic Display as a Forensic Object

*The **purpose** of the article is to investigate electronic reflection as a forensic object, to find out the nature of electronic traces, mechanisms of tracing, features of detection, fixation and identification of electronic traces. **Methodology.** To achieve the purpose of the article, the scientific validity and objectivity of its results, a number of general and special methods were applied, including analysis, synthesis, explanation, comparison, deduction, induction, etc. The essence of the concept of material traces in the information and telecommunication system is investigated as a combination of the states of an ordered series of elementary media in the memory device of this system. It is suggested to define these traces as binary codes of information in a «pure form» not tied to a specific material medium. Emphasis is placed on the integral (combinatorial) nature of these traces, which gives them uniqueness. It is noted that the material trace in the elementary information carrier does not have individual forensic features. **Scientific novelty.** The concept of electronic trace as a reflection on the monitor of a computing device of a material trace in the information and telecommunication system is proposed. It is recommended to consider electronic display as a form of electronic trace detection. The opinion about the ideal nature of electronic traces is grounded. The misinterpretation of electronic traces as traces of virtual ones is proved. It is argued that the integral (combinatorial) nature of material traces in the information and telecommunication system gives grounds to consider them and their electronic traces as acquiring individual forensic features because of the uniqueness of binary codes and thus may be suitable for forensic identification. Features of detection and fixation of electronic traces are investigated. It is established that their detection and fixation is carried out by special methods through the use of general and special purpose software. **Conclusions.** Generally, material traces in the information and telecommunication system do not have individual forensic features. However, their integral (combinatorial) nature gives reason to claim that they and the electronic traces they create acquire these characteristics and may be suitable for forensic identification. The detection and fixation of electronic traces is carried out by special methods through the use of general and special purpose software. Existing problems with the detection and fixation of electronic traces need legislative regulation. Electronic displays have common and distinct identifying features. Identical electronic traces may have differences on individual grounds due to their dynamic nature.*

Keywords: electronic display; criminalistics; a forensic object; forensic identification; binary code; evidence.