ПРОТИДІЯ ЗЛОЧИННОСТІ: ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ

УДК 343.146:343.982:343.34

Орлов Ю. Ю. – доктор юридичних наук, старший науковий співробітник, головний науковий співробітник відділу організації наукової роботи Національної академії внутрішніх справ, м. Київ;
Чернявський С. С. – доктор юридичних наук, професор, проректор Національної академії внутрішніх справ, м. Київ

Використання електронних відображень як доказів у кримінальному провадженні

Досліджено питання придатності електронних відображень для використання їх як доказів у кримінальному провадженні. Проаналізовано особливості належності, допустимості, достовірності, оцінювання та зберігання електронних відображень як доказів.

Ключові слова: електронне відображення, доказ, кримінальне провадження, допустимість, належність, достовірність доказів.

Електронне відображення є формою зберігання відомостей за допомогою знакових систем, тому за цією ознакою воно не відрізняється від «класичного» паперового документа. Водночас на підставі попереднього наукового дослідження властивостей електронних відображень автори дійшли висновку, що їх потрібно вважати самостійним джерелом доказів у кримінальному провадженні [1].

Електронні відображення не прив'язані до певного матеріального носія, тому не наділені індивідуальними криміналістичними ознаками. Унаслідок цього оригінали електронних відображень, на відміну від «класичних» документів, цілком ідентичні копіям. Електронні відображення засвідчують не лише факти людської діяльності, а й технологічні процеси в інформаційній системі, пов'язані з діями людини.

© Орлов Ю. Ю., Чернявський С. С., 2017

На відміну від «класичних» документів, вони можуть містити необмежений обсяг інформації, природним шляхом змінюватися в часі. Особливості функціонування електронних відображень можуть впливати на порядок їх огляду слідчим.

Отже, постає питання щодо придатності фактичних даних, що містяться в електронних відображеннях, для їх використання як доказів у кримінальному провадженні.

У загальному випадку вирішення питання щодо придатності фактичних даних зумовлене їх належністю, допустимістю й достовірністю.

Належність електронного відображення встановлюють на підставі ст. 85 Кримінального процесуального кодексу (КПК) України [2]. Важливим аспектом належності електронного відображення є його здатність установлювати факт, який належить до предмета доказування.

Дослідження змісту електронного відображення та інформації в сервісних опціях операційної системи про нього надає можливість установити:

– подію кримінального правопорушення (наприклад, виявляючи сайт із забороненим контентом або з контентом, оприлюднення якого обмежено законом);

– особу правопорушника (зокрема, шляхом установлення його фізичної адреси за IP-адресою комп'ютера, вивчення даних його акаунта);

– спосіб, обставини вчинення злочину (наприклад, аналізуючи зміст електронного листування, результати моніторингу банківських рахунків тощо);

– характер і розмір шкоди, завданої злочином, яка може полягати в порушенні функціонування певних електронних відображень, неправомірному перерахуванні електронних грошових коштів, передплаті ненаданих послуг (товарів), підробленні документів, порушенні авторських прав тощо.

Вивчення слідчим електронного відображення також дає змогу підтвердити факти, раніше встановлені іншими доказами, і отримати аргументи для спростування фактів, що належать до інших слідчих версій.

Актуальним є питання *допустимості* фактичних даних, що містяться в електронних відображеннях, як доказів у кримінальному провадженні. Допустимість визначають на загальних підставах, тобто вони мають відповідати вимогам

кримінального процесуального закону щодо їх джерела, умов, способів отримання й процесуального закріплення.

Відповідно до ст. 93 КПК України, електронні відображення збирають шляхом проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій, проведення інших процесуальних дій. Зокрема, електронні відображення можуть бути виявлені під час обшуку (ст. 234), огляду (ст. 237), а також тимчасового доступу до речей і документів як заходу забезпечення кримінального провадження (ст. 159). Згідно з ч. 1 ст. 159 КПК України, тимчасовий доступ до електронних інформаційних систем або їхніх частин, мобільних терміналів систем зв'язку здійснюють шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їхніх частинах, мобільних терміналах систем зв'язку, без їх вилучення [2]. Цю норму можна тлумачити як засіб забезпечення можливості використання «копій» електронних відображень як джерела доказів у кримінальному провадженні.

Слідча практика доводить, що під час обшуку й огляду приміщення, місцевості електронні відображення, які містять відомості, що мають значення для кримінального провадження, можуть бути виявлені:

– в обшукуваному (оглянутому) приміщенні, на місцевості: на автономному електронному носії (флешка, автономний електронний накопичувач), спеціалізованому пристрої (смартфон, цифровий фотоапарат чи диктофон тощо) або на пристрої пам'яті стаціонарного комп'ютера чи ноутбука;

– у Інтернет-мережі поза межами обшукуваного (оглянутого) приміщення, місцевості, а саме на віддаленому сервері, доступ до змісту якого здійснюють із комп'ютера, розміщеного в зазначеному приміщенні.

Отже, КПК України доцільно доповнити вказівкою щодо особливостей копіювання електронних відображень і вилучення комп'ютерної техніки під час обшуку, огляду та тимчасового доступу до речей і документів.

Електронні відображення може бути отримано також під час проведення негласних слідчих (розшукових) дій: аудіо-, відеоконтролю особи (ст. 260), зняття інформації з транспортних телекомунікаційних мереж (ст. 263), зняття інформації з електронних інформаційних систем (ст. 264), установлення місцезнаходження радіоелектронного засобу (ст. 268),

спостереження за особою, річчю або місцем (ст. 269), моніторингу банківських рахунків (ст. 269[1]), аудіо-, відеоконтролю місця (ст. 270), контролю за вчиненням злочину (ст. 271). У такому разі їх оформлюють як додаток до протоколу відповідної слідчої (розшукової) дії [2].

Згідно з ч. 2 ст. 99 КПК України, матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, можуть бути зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність». Такі матеріали зазвичай формують у вигляді оперативних документів, а також електронних відображень (фотографій, фоно- і відеограм у цифровому форматі). Їх можуть використовувати в кримінальному провадженні як докази.

Частина 2 ст. 93 КПК України містить вказівку на інший спосіб збирання електронних відображень як доказів: вони можуть бути витребувані від органів державної влади, органів місцевого самоврядування, службових та фізичних осіб, підприємств, установ та організацій. До підприємств, які відіграють ключову роль у забезпеченні обігу електронних зображень і мають технічні можливості щодо їх збереження, належать такі: 1) провайдери Інтернет-послуг; 2) оператори мобільного зв'язку. Водночас їхні відносини з органами розслідування нині процесуально не врегульовані, що призводить до численних непорозумінь, необґрунтованих вилучень слідчими мережевої комп'ютерної техніки у провайдерів. Такі дії можуть спричиняти порушення прав користувачів мережі Інтернет і визнання судом одержаних доказів недопустимими, а також небажання провайдерів надавати інформацію правоохоронним органам.

Тому до глави 15 КПК України необхідно внести зміни, які чітко визначатимуть зміст правовідносин з Інтернет-провайдерами й операторами мобільного зв'язку щодо збереження електронних зображень у провайдерів та надання їх слідчому, прокурору, слідчому судді та суду в інтересах кримінального судочинства. Назву глави 15 слід подати в такій редакції «Тимчасовий доступ до речей, документів та електронних зображень».

Досвід розвинутих країн дає підстави для висновку про доцільність процесуальної регламентації зазначених дій:

– негайного збереження Інтернет-провайдером електронних зображень, які містять відомості, що можуть бути використані як

доказ факту чи обставин, установлюваних під час кримінального провадження;

– зберігання інформації, що циркулює на певних Інтернет-ресурсах або щодо певних IP-адрес протягом певного часу.

Такі дії має ініціювати слідчий, прокурор, слідчий суддя або суд шляхом надання провайдеру припису про негайне збереження або зберігання інформації. Вимоги до змісту припису необхідно визначити в КПК України.

Збереження та зберігання інформації Інтернет-провайдер здійснює без дозволу суду. Водночас передання Інтернет-провайдером збереженої інформації органам розслідування відбувається лише за наявності дозволу суду, оскільки ця інформація може містити відомості, які стосуються приватного життя особи, зокрема це:

1) зміст електронної кореспонденції;

2) запис телефонних переговорів між абонентами стільникової мережі та між користувачами в Інтернет-месенджері;

3) відомості про факти зв'язку між абонентами (користувачами) мережі;

4) персональні дані.

Про факт отримання інформації з Інтернету орган розслідування має повідомити особу, кореспонденцію чи переговори якої контролювали. Терміни повідомлення потрібно визначити в КПК України так, щоб вони не перешкоджали кримінальному провадженню.

У більшості розвинутих країн провайдер має право знищити збережену за приписом слідчого, прокурора, судді або суду інформацію через 12 місяців, якщо впродовж цього часу її не передано до органу розслідування за дозволом суду.

У деяких країнах (Велика Британія, Франція) інформацію, отриману від провайдера, орган розслідування оплачує відповідно до прейскуранта, затвердженого урядом. Це спонукає провайдерів до активної допомоги правоохоронцям. Кошти на сплату послуг провайдерам враховують під час фінансування правоохоронного органу. На нашу думку, такий досвід доцільно впровадити у правоохоронну практику України.

Результати збереження та зберігання динамічного (змінюваного) електронного відображення провайдер зазвичай надає слідчому, прокурору, слідчому судді та суду у формі статичних зображень (так званих скриншотів – миттєвих копій

змісту екрана монітора), які фіксують стан динамічного електронного відображення в певний момент часу, а також у вигляді файлів звуко- та відеозапису.

Під час кримінального розслідування може виникнути потреба запобігти злочину, про загрозу вчинення якого стало відомо з наявних матеріалів, використовуючи можливості мережі Інтернет. Із цією метою в КПК України слід запровадити норму щодо надання органом розслідування із санкції прокурора припису провайдеру на блокування роботи певного Інтернет-ресурсу або певної IP-адреси (негайного або на певний строк), який є обов'язковим для виконання провайдером.

З-поміж умов допустимості «класичного» документа як джерела доказів потрібно виокремити такі: 1) має бути відомим автор документа (установа, організація, підприємство, посадова особа або громадянин); 2) зміст документа повинен відповідати компетенції та фактичній обізнаності автора. Це надає можливість перевірити доказ. Умови допустимості слід висувати й до електронних відображень, що їх сформувала людина. Наприклад, пост (повідомлення) на форумі чи у блозі, відправлений під ніком (мережевим псевдонімом), який не можна перевірити, є анонімним і не може бути використаний під час доказування. Відомості про автора (укладача) електронного відображення не завжди зафіксовані на цьому відображенні, передусім якщо воно містить заборонений контент або безпосередньо призначено для вчинення злочину. Це відрізняє електронне відображення від «класичного» документа, де відомості про автора часто містяться у вигляді найменування, реквізитів, прізвища, підпису тощо.

До електронних відображень, які створені інформаційною системою в автоматичному режимі, вимогу щодо встановлення особи автора як умову допустимості доказу, очевидно, висувати не слід. Подеколи необхідно призначити комп'ютерно-технічну експертизу щодо визначення можливості формування певного електронного відображення конкретним апаратно-програмним комплексом з метою встановлення належності доказу.

Доказове значення мають електронні зображення, призначені як для передавання відомостей іншим особам (користувачам мережі, абонентам зв'язку), так і для користування власне автором (електронні щоденники, приватні облікові записи тощо).

Якщо проблему допустимості електронних відображень можна розв'язати шляхом внесення необхідних змін до кримінального процесуального законодавства, то відповідь на питання щодо їх *достовірності* як джерел доказів потребує застосування сучасних методик експертного дослідження. Електронне відображення буде достовірним доказом, якщо його істинність у значенні відповідності об'єктивній дійсності є встановленою й не викликає розумних сумнівів у чинній парадигмі знань.

У сфері судової експертизи напрацьовано чимало методик, які дають змогу виконати низку завдань щодо визначення певних властивостей електронних відображень. Деякі із цих завдань було нормативно закріплено в наказі Міністерства юстиції України [3]. Отже, до основних завдань експертизи комп'ютерної техніки та програмних продуктів належать такі:

– виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

– установлення відповідності програмних продуктів певним версіям чи вимогам щодо його розроблення;

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

Експертиза комп'ютерної техніки і програмних продуктів встановлює:

– чи міститься на носії певна інформація та в якому вигляді;

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

– чи здійснювали на досліджуваному накопичувачі певні процедури з метою знищення інформації;

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

– у який спосіб певну інформацію перенесено до досліджуваного комп'ютера (носія);

– якою була технологія та хронологія створення певного електронного документа;

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

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

– які функціональні несправності наявні в досліджуваному комп'ютерному обладнанні, окремих його складових і пристроях, як ці несправності впливають на роботу обладнання загалом;

– чи можливе виконання певних дій за допомогою цього програмного продукту;

– чи можливе виконання певного завдання за допомогою цього програмного продукту;

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

Для дослідження інформації, що міститься на комп'ютерному носієві, експерту надають безпосередньо носій. Для встановлення відповідності програмних продуктів певним параметрам експерт отримує носій з копією досліджуваного програмного продукту або програмного коду (виконуваного або вихідного модуля комп'ютерної програми). Проте регламентованої методики проведення експертних досліджень електронних відображень, яким послуговуються в комп'ютерній мережі, досі не розроблено.

У разі необхідності проведення експертного дослідження електронного відображення, яке є «шпигунською» програмою, може бути призначено експертизу телекомунікаційних систем і засобів, яка встановлює:

– чи наявний факт передання (отримання) інформації в телекомунікаційній системі та в який спосіб;

– за допомогою яких програмних засобів здійснювали несанкціоноване під'єднання до телекомунікаційної мережі.

Якщо постає потреба в експертному дослідженні електронних відображень, які є файлами цифрового звуко- та відеозапису, то слідчий, прокурор, слідчий суддя, суд призначає експертизу відеозвукозапису, основними завданнями якої є:

– ототожнення особи за фізичними параметрами голосу;

– установлення технічних умов і технології отримання відеозвукозапису.

Ідентифікаційну експертизу з ототожнення осіб проводять за традиційними методиками, тому вона не передбачає технологічних ускладнень. Натомість установлення автентичності цифрової фонограми (відеограми) залишається проблемним питанням для експертів, на яке слідчий, прокурор, слідчий суддя, суд не завжди можуть отримати відповідь.

Останніми роками розроблено низку новітніх методик для встановлення автентичності цифрових сигналограм (наприклад, винаходи, розроблені в Національній академії внутрішніх справ, захищені патентами України № 54627, 60403, 73631), що надають можливість виявляти сліди монтажу (фальсифікації) в електронних відображеннях, що містять цифрові фоно-, відеограми, а також цифрові фотографії. На підставі винаходів розроблено експериментальні експертно-аналітичні комп'ютерні програми «Академія» та «Фрактал», які дають змогу встановлювати автентичність цифрових сигналограм і визначати електронний пристрій, на якому їх сформовано.

Зважаючи на наявність технологічної можливості фальсифікування електронних відображень, на нашу думку, доцільно запровадити поняття *«підроблене електронне відображення»,* яке можна тлумачити як електронне зображення з ознаками фальсифікування (підроблення), підтвердженими висновком експерта.

Підроблене електронне відображення слід відрізняти від *імітаційного електронного відображення*, що змістовно може бути ідентичне справжньому, проте його використовують з метою імітації справжнього електронного відображення, зокрема такого, що має офіційний статус (Інтернет-портали, сайти з ліцензованою діяльністю), а також імітування ділового та приватного електронного листування. Основною ознакою імітаційного електронного відображення є його створення від імені іншої фізичної або юридичної особи, зокрема, шляхом використання мережевого акаунта (облікового запису) іншої особи.

Важливим є питання *оцінювання* електронних відображень як доказів. Відповідно до ч. 1 ст. 94 КПК України, слідчий, прокурор, слідчий суддя, суд оцінюють докази за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, з позицій належності, допустимості, достовірності, а сукупність зібраних доказів – з позицій достатності та взаємозв'язку для прийняття процесуального рішення.

Оцінювання електронних відображень як доказів, з огляду на їхні особливості (змінюваність у часі, незалежність від матеріального носія, ідентичність оригіналу та копії,

регламентованість доступу до окремих частин електронного відображення), необхідно здійснювати комплексно, зіставляючи з іншими доказами в кримінальному провадженні.

У процесі оцінювання електронного відображення зіставляють окремі відомості та з'ясовують причини виявлених протиріч.

Якщо факт кримінального правопорушення позначився на декількох електронних відображеннях, слід зіставити зміст усіх цих відображень на предмет виявлення можливих протиріч.

Електронні відображення, які мають статус офіційних, підлягають перевірці й оцінюванню на загальних підставах.

Під час оцінювання електронних відображень, які містять відомості про факти електронних комунікацій абонентів (користувачів), задля забезпечення достовірності доказів, не підтверджених іншими доказами, потрібно перевірити технічну інформацію, наявну в електронних пристроях усіх задіяних абонентів, яка має збігатися за своїми параметрами (телефонні номери або IP-адреси абонентів, дата, час, тривалість комунікації).

Оцінюючи електронні відображення, слід з'ясувати:

1) походження електронного відображення та час його створення (на якому комп'ютері створено, хто є автором (укладачем), коли було створено і коли внесено зміни);

2) справжність (автентичність) електронного відображення, його належність до кримінального провадження (чи відповідає задекларована належність електронного відображення юридичній або фізичній особі фактичній належності; чи відповідає реальна діяльність, здійснювана шляхом застосування електронного відображення, проголошеній на цьому відображенні, чи має значення електронне відображення для кримінального провадження);

3) джерело обізнаності особи, яка сформувала зміст електронного відображення;

4) дотримання під час створення електронного відображення вимог закону (чи підлягає це відображення офіційній реєстрації та чи зареєстроване воно; чи підлягає ліцензуванню діяльність, яку здійснюють із застосуванням електронного відображення, чи видано ліцензію);

5) наявність інших даних, що підтверджують достовірність змісту електронного відображення;

6) відомості про Інтернет-провайдера, на серверах якого зберігається електронне відображення.

Для оцінювання електронних відображень може бути проведено слідчі (розшукові) дії, які передбачають допит авторів (укладачів), призначення експертизи (комп'ютерної техніки і програмних продуктів, матеріалів цифрового відеозвукозапису), зіставлення електронних відображень з іншими джерелами доказів, що засвідчують певні обставини кримінального правопорушення. Обсяг перевірки електронних відображень залежить від виду останніх. Зокрема, меншим є обсяг перевірки відображень, створених інформаційною системою в автоматичному режимі ніж створених людиною. Обсяг перевірки електронного відображення, яке містить заборонений контент, менше, за обсяг перевірки відображення, що містить відомості про факти комп'ютерного шахрайства.

Оцінювання електронних відображень слідчим, прокурором, слідчим суддею та судом, як й інших доказів у кримінальному провадженні, має бути всебічним (з огляду на всі обвинувальні та виправдувальні докази), повним (на підставі результатів зіставлення з іншими доказами, з необхідними висновками) й неупередженим (об'єктивним).

Електронні відображення *зберігають* на носієві в матеріалах кримінального провадження в опечатаному конверті (якщо це можливо з огляду на розміри матеріального носія) або разом із цими матеріалами в окремому опечатаному пакованні (якщо носій має значні розміри). Слід ужити заходів для запобігання можливому несанкціонованому знищенню зафіксованої на носієві інформації (шляхом розмагнічування, електричного пробою, механічного руйнування носія тощо).

Якщо електронне відображення розміщено в Інтернеті, то для його збереження потрібно копіювати на автономний носій (у вигляді скриншотів). Якщо ж для розслідування важливим є процес функціонування динамічного електронного відображення в комп'ютерній мережі, у протоколах слідчих (розшукових) дій необхідно зазначити Інтернет-посилання на нього.

З огляду на специфіку електронних відображень, доцільно розробити проект Порядку зберігання електронних відображень, який має бути затверджений постановою Кабінету Міністрів України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні / Ю. Ю. Орлов, С. С. Чернявський // Юридичний часопис Національної академії внутрішніх справ. – 2017. – № 1 (13). – С. 12–24.

2. Кримінальний процесуальний кодекс України [Електронний ресурс] : Закон України від 13 квіт. 2012 р. № 4651-VI. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/4651-17. – Назва з екрана.

3. 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 [Електронний ресурс] : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0001-13. – Назва з екрана.

REFERENCES

1. 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, Legal journal of the National Academy of Internal Affairs, 1 (13),* 12-24 [in Ukrainian].

2. Kryminalnyi protsesualnyi kodeks Ukrainy: vid 13 kvit. 2012 r. No. 4651-VI [Criminal Procedural Code of Ukraine from April 13, 2012, No. 4651-VI]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/4651-17 [in Ukrainian].

3. Nakaz Ministerstva yustytsii Ukrainy pro zatverdzhennia Instruktsii pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen ta Naukovo-metodychnykh rekomendatsii z pytani 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 the approval of the Instruction on the appointment and conduct of forensic examinations and expert studies and Scientific and methodological recommendations on the preparation and appointment of forensic examinations 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 [in Ukrainian].

Стаття надійшла до редколегії 21.07.2017