Чернявський С. С.,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
проректор Національної академії
внутрішніх справ

Орлов Ю. Ю.,
доктор юридичних наук, професор,
головний науковий співробітник
Національної академії
внутрішніх справ

ЕЛЕКТРОННЕ ВІДОБРАЖЕННЯ ЯК ДЖЕРЕЛО ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Введено поняття електронних відображень як джерела доказів у кримінальному провадженні. Встановлено їх відмінності від документів. Виділено форми та запропоновано класифікацію електронних відображень. Досліджено особливості належності, допустимості, достовірності, а також оцінки електронних відображень як доказів.

Ключові слова: *докази, джерела доказів, електронне відображення.*

Введено понятие электронных отображений как источника доказательств в уголовном производстве. Установлены их отличия от документов. Выделены формы и предложена классификация электронных отображений. Исследованы особенности относимости, допустимости, достоверности, а также оценки электронных отображений как доказательств.

Ключевые слова: *доказательства, источники доказательств, электронное отображение.*

Сьогоднішнє покоління людей є свідком стрімких процесів інформатизації соціального буття. Інформаційно-телекомунікаційні технології охопили майже всі сфери життєдіяльності суспільства й держави. Одним з наймасштабніших технічних проектів слала глобальна комп'ютерна мережа (Інтернет), суттєвою особливістю якої є здатність відображати безліч

соціальних фактів і процесів, а також певних соціально значимих дій фізичних та юридичних осіб.

Такі дії можуть, зокрема, містити склад кримінального правопорушення, що дає правознавцям можливість говорити про нове соціальне явище – кіберзлочинність, яка характеризується нетрадиційними способами вчинення злочинів. Швидкість зростання злочинності в глобальній комп'ютерній мережі є найбільшою порівняно з іншими видами злочинів, включаючи торгівлю наркотиками та зброєю.

Крім того, інформація в Інтернет-середовищі може свідчити про вчинення певного правопорушення (яке, до речі, не обов'язково має належати до категорії кіберзлочинів), містити відомості про його сліди та шкідливі наслідки.

Інформатизація суспільного життя об'єктивно позначається на особливостях кримінального процесу. Зокрема, це стосується такої важливої категорії, як джерела доказів.

Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів чинне законодавство визнає показання, речові докази, документи та висновки експертів.

Згідно зі ст. 95 КПК України показання – це відомості, які надаються особою в усній або письмовій формі під час допиту щодо відомих їй обставин у кримінальному провадженні, що мають значення для цього кримінального провадження. Допитуваною особою можуть бути підозрюваний, обвинувачений, свідок, потерпілий та експерт. Під показаннями розуміють повідомлення особою відомостей про фактичні обставини, що мають значення для кримінального провадження, отримане у порядку, встановленому КПК України.

Речовими доказами є матеріальні об'єкти, що містять відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження (ст. 98 КПК України). До речових доказів належать знаряддя вчинення кримінального правопорушення, предмети, що зберегли на собі його сліди, були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення.

Під висновком експерта розуміють докладний опис проведених експертом досліджень і зроблені за їх результатами висновки, обґрунтовані відповіді на запитання, поставлені особою, яка залучила експерта, або слідчим суддею чи судом, що доручив проведення експертизи (ст. 101 КПК України).

Висновок експерта є самостійним процесуальним джерелом доказів. Разом з тим слід зауважити, що з гносеологічної точки зору, він виявляється похідним від предмету експертного дослідження – речового доказу або документа.

Відповідно до ст. 99 КПК України документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. Частина 2 цієї статті встановлює, що до документів можуть належати, зокрема, матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні).

Запровадження в кримінальному процесуальному законі новітньої категорії «електронні носії інформації» викликано практичною потребою у визнанні цих об'єктів джерелом доказів у кримінальному провадженні. Буквальне тлу-

мачення тексту ст. 99 дозволяє зробити висновок, що під «електронними носіями інформації» слід розуміти будь-які електронні носії, зокрема ті, що є вбудованими в комп'ютерні пристрої, підключені до інформаційної мережі. Такі носії можуть містити матеріали в будь-якій формі (письмовій, графічній, фотографічній, відео-, звукозапис тощо).

У частині 3 ст. 99 КПК України законодавець застосовує термін «електронний документ», очевидно, розуміючи під ним електронний носій інформації із зафіксованими на ньому відомостями. При цьому, кримінальне процесуальне законодавство не дає визначення електронного документа. Логічним буде зробити припущення, що запропонований в КПК України термін «електронний документ» слід розуміти як різновид, одну з форм існування іншого джерела доказів – документа.

Дійсно, документ в його «класичному» сприйнятті й «електронний документ» мають суттєву спільну рису – в них інформація зберігається й передається шляхом опису подій і фактів за допомогою знакових систем (текстів, графіки, малюнків, креслень тощо). Проте, на наше переконання, це твердження не може бути підставою для ототожнення документів й так званих «електронних документів».

Справа в тому, що між «класичними» документами й так званими «електронними документами» є багато відмінностей, які стосуються не лише форми подання інформації, а також її змісту і, крім того, – походження доказу, його природи, можливостей експертного дослідження.

По-перше, «класичний» документ завжди створює людина. «Електронний документ» в Інтернет-середовищі може бути сформований не лише людиною, але й безпосередньо інформаційною системою (наприклад, трафіки з'єднань абонентів мобільного зв'язку, динамічні бази банківських проводок, білінгові системи, log-файли реєстрації тощо). Отже, на відміну від «класичного» документа, «електронний документ» може не мати автора. Проте, створення «електронного документа» машиною відбувається внаслідок певних дій особи в інформаційній мережі (телефонування, перерахування грошей, відвідування сайтів тощо). Процес формування такого «документа» є подібним до процесу формування речового доказу, який містить сліди злочину: він формується природним (технічним) шляхом й незалежно від бажання людини, але внаслідок її дій.

По-друге, змістом «класичного» документа є текст, малюнки, креслення, схеми, фотозображення, а також фонограми та відеограми. Змістом «електронного документа», окрім зазначеного, може бути також інформація в нових, «некласичних» формах – комп'ютерні програми у вигляді виконуваних модулів, банки (бази) даних, а також мережева технологічна інформація (наприклад, про з'єднання користувачів в месенджерах).

По-третє, «класичний» документ не існує окремо від матеріального носія. Як джерело доказів документ є, насамперед, певним матеріальним об'єктом із зафіксованими на ньому відомостями. Сліди кримінального правопорушення, які знайшли відображення на документі, мають матеріальну природу. Натомість «електронні документи», які обертаються в інформаційній мережі, багаторазово перезаписуючись з одного матеріального носія на інший відповідно до специфіки «хмарних» технологій, являють собою інформацію, так би мовити, «в чистому вигляді». В загальному випадку вони не прив'язані до певного матеріального носія. Отже, у випадку «електронних документів» ми вимушені стикатися з новим різновидом ідеальних слідів, раніше не знаних криміналістичною наукою.[1]

У зв'язку з цим варто зауважити, що в теорії кримінального процесу докази

[1] Зауважимо, що «класичні» ідеальні сліди є слідами пам'яті людини. На відміну від «електронних документів» вони чітко прив'язані до певного матеріального носія – конкретної особи (свідка, потерпілого, підозрюваного, обвинуваченого).

прийнято класифікувати на «особисті» та «речові», виходячи з тієї гіпотези, що будь-яка подія відображається у свідомості людей-спостерігачів, а також у матеріальній обстановці у вигляді її змін [3, с. 258–263]. Особисті докази виходять від осіб, а речові виражаються у фізичних ознаках матеріальних об'єктів. Зокрема, до особистих доказів відносять показання, документи (в тому числі протоколи процесуальних дій та додатки до них) та висновки експерта.

З винайденням комп'ютера, здатного, наряду з людиною, відображати події соціальної природи та зберігати на технічному носієві, класичний поділ доказів на особисті та речові, на нашу думку, стає неповним. «Електронні документи» мають властивості як особистих доказів (ідеальність слідів, відображення подій і фактів за допомогою знакових систем), так і речових доказів (можливість формування технічним шляхом й незалежно від людини, незмінюваність їх змісту в ході кримінального провадження). Значення «електронного документа» для кримінального провадження визначається його змістом (так само, як і особистого доказу), а також місцем та обставинами його виявлення (як речового доказу).

Отже, в зазначеному поділі доказів «електронні документи» мають займати відокремлене місце. На нашу думку, з позицій сьогодення докази можна поділити на «речові», «особисті» та «електронні». При цьому електронні докази за своїми властивостями займають проміжне місце між «особистими» та «речовими». Критерієм такого поділу є середовище, в якому відбувається відображення події (матеріальний світ, свідомість людини, технічна інформаційна система). При цьому електронні докази можуть походити від осіб (так само, як і «особисті»), а також бути результатом функціонування інформаційної системи, виражаючись у фізичних ознаках матеріальних об'єктів-носіїв інформації (як «речові»).

По-четверте, незалежність «електронних документів» від матеріального носія має своїм наслідком те, що у них можуть бути відсутні індивідуальні криміналістичні ознаки, які зазвичай притаманні «класичним» документам. У випадку «класичних» документів джерелом доказів може бути виключно оригінал документа як носій цих ознак. Копія документа може бути визнана допустимою для підтвердження його змісту, лише якщо:

– оригінал документа втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає;

– оригінал документа не може бути отриманий за допомогою доступних правових процедур;

– оригінал документа знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони (ч. 5 ст. 99 КПК України).

Натомість, незалежність «електронного документа» від носія дозволяє говорити про відсутність криміналістично значимої різниці між оригіналом і копією. В загальному випадку, поняття «оригінал» і «копія» до цього виду доказів є незастосовними[1]. Отже, експертиза не має можливості визначити оригінальність «електронного документа» з Інтернет-середовища.

Зважаючи на цю обставину, неможливо визначити, яким доказом є «електронний документ» – первинним чи похідним. Тому кожен такий документ потребує ретельної перевірки щодо його походження та достовірності. Крім того, він має бути підкріплений іншими доказами.

Разом з тим у ряді випадків експертиза здатна визначити справжність (автентичність)»електронного документа», відсутність в ньому ознак фальсифікації.

Крім того, сучасні експертні методики уможливлюють дати відповідь на пи-

[1] Чинна редакція ч. 3 ст. 99 КПК України встановлює, що оригіналом електронного документа є його відображення, якому надається таке ж значення, як документу. Разом з тим Кодекс не дає визначення поняттю «відображення електронного документа».

тання, чи сформований «електронний документ» на даному комп'ютері або чи переписаний він з іншого носія. Такий висновок експерта може бути підкріплений непрямими доказами (наприклад, інформацією в сервісних опціях операційної системи щодо властивостей файла чи показаннями свідків) або на оціночними доказами (наприклад, намагання користувача даного комп'ютера знищити інформацію в Інтернеті).

По-п'яте, «класичний» документ є статичним, будучи одного разу складеним, він не змінює свого змісту з часом (якщо не враховувати спроб його навмисної фальсифікації). Натомість, «електронний документ» може постійно змінюватись природним шляхом (наприклад, листування електронною поштою, стан банківського рахунку або ж функції віддаленого управління в комутаційних комп'ютерних програмах). Тому для кримінального процесу важливим є своєчасне копіювання «електронного документа» з мережі Інтернет, доки він містить відомості про фактичні обставини, що мають значення для розслідування.

По-шосте, «класичні» документи зазвичай є цілісним об'єктом, доступ до окремих частин якого (сторінок, абзаців тексту тощо) є незалежним. Слідчий, прокурор, слідчий суддя може оглядати такий документ у довільному порядку. На відміну від «класичних» «електронні документи» (сайти, прикладні виконувані програми, електронні бази даних) часто є складеними з окремих фрагментів, порядок доступу до яких залежить від структури «електронного документа». Послідовність огляду окремих фрагментів, частин документа задається алгоритмом функціонування програми, який зазвичай є багаторівневим й розгалуженим. Це накладає обмеження на процедуру огляду «електронних документів», яка через вказані причини може займати значний час.

Крім того, «електронний документ» може мати дуже великий обсяг, що вимірюється гігабайтами інформації. Такий обсяг не є характерним для «класичних» документів. Тому оглянути весь вміст такого «електронного документа» може бути утруднено.

По-сьоме, за критерієм відношення до кримінального провадження «класичні» документи можуть бути розділені на три групи:

1) документи, складені незалежно від кримінального провадження, але які містять опис події, яка стала предметом провадження, або встановлюють окремі факти, обставини, що мають відношення до кримінального провадження;

2) які фіксують обставини події, наявність чи відсутність складу злочину, складені на стадії порушення кримінального провадження;

3) які фіксують фактичні дані, відомі їх укладачу особисто чи з інших документів, складені за пропозицією органів розслідування і суду чи за проханням учасників процесу в період кримінального провадження [3, с. 681].

Натомість «електронні документи» можуть бути складені виключно незалежно від кримінального провадження. При цьому вони містять опис події, яка стала предметом провадження (наприклад, результат моніторингу дій користувача, який здійснює шахрайство в комп'ютерній мережі), або є засобом вчинення злочину (наприклад, імітаційний сайт, призначений для здійснення Інтернет-маркетингу), або ж встановлюють окремі факти, обставини, що мають відношення до кримінального провадження (наприклад, трафіки з'єднань абонентів мобільного зв'язку, які можуть бути свідками події).

Отже, за критерієм відношення до кримінального провадження електронні відображення є подібними до речових доказів.

Ці відмінності «класичних» документів від так званих «електронних документів» у своїй сукупності дозволяють, на нашу думку, говорити про два різних джерела доказів. «Електронні документи» як джерела доказів у кримінальному провадженні, на нашу думку, не є до-

кументами у традиційному розумінні. Через цю обставину, а також з метою уникнути термінологічної плутанини, автор пропонує позначати їх спеціальним терміном «електронне відображення» й вважати самостійним джерелом доказів у кримінальному провадженні й окремим видом доказів.

Відповідно, частину 2 ст. 84 КПК України пропонується викласти в редакції: «Процесуальними джерелами доказів є показання, речові докази, документи, електронні відображення, висновки експертів».

Електронне відображення може існувати в різних формах, зокрема: поіменована область даних – файл; масив даних з унікальною Інтернет-адресою – сайт; сукупність систематизованих даних – база даних; комбінація комп'ютерних інструкцій і даних – комп'ютерна програма; засіб обміну відомостями – мессенджер тощо. Воно може бути статичним (файл) або динамічним, змінюваним (Інтернет-сайт, чат, трафік). Проте, в будь-якому випадку основною властивістю електронного відображення залишається його цілісність, системність, структурованість. Воно сприймається людиною як єдиний цілісний об'єкт, змістом якого є певні відомості, які можуть бути використані як доказ у кримінальному провадженні.

Отже, КПК України пропонується доповнити статтею 100^1 такого змісту:

«Стаття 100^1. Електронні відображення

1. Електронним відображенням є цілісна система відомостей та (або) комп'ютерних інструкцій в інформаційній мережі або на технічному носієві, яка може бути використана як доказ факту чи обставин, що встановлюються під час кримінального провадження.

2. До електронних відображень, за умови наявності в них інформації, передбаченої частиною першою цієї статті, належать:

1) портали, сайти в комп'ютерній мережі;

2) електронні бази даних;

3) файли та групи файлів;

4) зміст електронної пошти, чатів;

5) вихідні та виконувані модулі комп'ютерних програм;

6) інші відомості та (або) комп'ютерні інструкції в інформаційній мережі або на технічному носієві».

Відповідно параграф 4 Глави 4 «Докази і доказування» КПК України повинен мати назву «§ 4. Речові докази, документи й електронні відображення».

Електронні відображення можна класифікувати за різними критеріями.

Залежно від авторів (укладачів) можна виділити електронні відображення, які створені:

– юридичною або фізичною особою, що мають офіційний статус (Інтернет-портали, сайти з ліцензованою діяльністю, ділове електронне листування);

– приватними особами (приватне електронне листування, звуко- та відеозаписи тощо);

– інформаційною системою в автоматичному режимі (трафіки з'єднань абонентів зв'язку, бази банківських проводок та ін.).

Крім того, залежно від призначення та відповідно до класифікації кіберзлочинів, наданої у міжнародній Конвенції «Про кіберзлочинність», можна виділити електронні відображення:

– призначені для несанкціонованого втручання в роботу комп'ютерів, зміни, знищення або блокування оброблюваної інформації (шкідливі програмні продукти, спам);

– призначені для здійснення комп'ютерного шахрайства (імітаційні сайти Інтернет-маркетингу, Інтернет-банкінгу тощо);

– які містять заборонений контент (сайти з дитячою порнографією, закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади тощо);

– використання яких порушує авторське право та суміжні права (банки

комерційних комп'ютерних програм, аудіо- та відеопродуктів).

Належність електронного відображення визначають відповідно до ст. 85 КПК України. Важливим аспектом належності електронного відображення є його здатність встановлювати факт, який входить до предмету доказування.

Дослідження змісту електронного відображення та інформації в сервісних опціях операційної системи про це відображення, в загальному випадку дозволяє встановити:

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

– особу правопорушника (зокрема, вивчаючи дані його аккаунта, встановлюючи IP-адресу комп'ютера);

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

– характер і розмір шкоди, завданої злочином (які можуть полягати у порушенні функціонування певних електронних відображень, неправомірному перерахуванні електронних грошових коштів, передплаті ненаданих послуг (товарів), підробці документів, порушенні авторських прав тощо).

Дослідження електронного відображення дозволяє також підтвердити факти, раніше встановлені іншими доказами, а також набути аргументів для спростування фактів, що належать до інших слідчих версій.

Актуальним є питання допустимості фактичних даних, які містяться в електронних відображеннях, як доказів у кримінальному провадженні. Допустимість таких фактичних даних визначається на загальних підставах, а саме вони мають відповідати вимогам кримінального процесуального закону відносно їх джерела, умов, способів отримання й процесуального закріплення.

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

Електронні відображення можуть бути отримані також в ході проведення негласних слідчих (розшукових) дій – аудіо-, відеоконтроль 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), моніторинг банківських рахунків (ст. 269[1]), аудіо-, відеоконтроль місця (ст. 270), контроль

[1] Як показує слідча практика, в ході обшуку та огляду приміщення, місцевості електронні відображення, які містять відомості, що мають значення для кримінального провадження, можуть бути виявлені: 1) в обшукуваному (оглянутому) приміщенні, на місцевості: на автономному електронному носієві (флешка, автономний електронний накопичувач), на спеціалізованому пристрої (смартфон, айфон, цифровий фотоапарат, цифровий диктофон тощо) або на пристрої пам'яті стаціонарного комп'ютера (ноутбука); 2) в мережі Інтернет поза межами обшукуваного (оглянутого) приміщення, місцевості, а саме на віддаленому сервері, доступ до змісту якого здійснюється із комп'ютера, розташованого у зазначеному приміщенні.

Отже, КПК України доцільно доповнити вказівкою щодо особливостей вилучення комп'ютерної техніки в ході обшуку, огляду та при тимчасовому доступі до речей і документів.

за вчиненням злочину (ст. 271). У цьому випадку вони оформлюються як додаток до протоколу відповідної слідчої (розшукової) дії.

Згідно з ч. 2 ст. 99 КПК України матеріали, в 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 формуються у вигляді оперативних документів, а також електронних відображень (фотографій, фонограм та відеограм в сучасному цифровому форматі) і можуть використовуватися в кримінальному провадженні як докази. Разом з тим КПК України встановлює, що всі ці матеріали є «документами», що, на наш погляд, не є правильним.

Частина 2 ст. 93 КПК України містить вказівку на інший спосіб збирання електронних відображень: вони можуть бути витребувані від органів державної влади, органів місцевого самоврядування, службових та фізичних осіб, підприємств, установ та організацій. Підприємствами, які відіграють ключову роль у забезпеченні обігу електронних зображень і мають технічні можливості щодо їх збереження, є провайдери Інтернет-послуг (Інтернет-провайдери) та оператори мобільного зв'язку. Разом з тим їх відносини з органами розслідування сьогодні процесуально не врегульовані, що призводить до численних непорозумінь, необґрунтованих вилучень слідчими мережевої комп'ютерної техніки у провайдерів, що веде до порушень прав користувачів мережі Інтернет й до визнання судом здобутих доказів недопустимими, а також породжує небажання провайдерів надавати інформацію правоохоронним органам.

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

Досвід розвинутих країн дозволяє дійти висновку щодо практичної необхідності процесуальної регламентації таких дій:

– негайне збереження Інтернет-провайдером електронних зображень, які містять відомості, що можуть бути використані як доказ факту чи обставин, що встановлюються 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 на негайне збереження або зберігання інформації. Вимоги до змісту припису мають бути визначені КПК України.

Зберігання та збереження інформації Інтернет-провайдер здійснює без дозволу суду. Разом з тим передача Інтернет-провайдером збереженої інформації органам розслідування має здійснюватися за наявності дозволу суду, оскільки ця інформація може містити відомості, які стосуються приватного життя особи, а саме:

1) зміст електронної кореспонденції;

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

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

4) персональні дані.

Про факт отримання інформації з Інтернету орган розслідування має повідомити особу, кореспонденція чи переговори якої контролювалися. Терміни повідомлення мають визначатися в КПК України з таким розрахунком, щоб вони не заважали кримінальному провадженню.

В більшості розвинутих країн провайдер має право знищити збережену за приписом слідчого, прокурора, судді або суду інформацію по завершенню 12 місяців, якщо протягом цього часу вона не передана до органу розслідування за дозволом суду.

У ряді країн (Велика Британія, Франція) інформацію, отриману від провайдера, орган розслідування оплачує відповідно до прейскуранту, затвердженому урядом. Це спонукає провайдерів до активної допомоги правоохоронцям. Кошти на сплату послуг провайдерам враховують при фінансуванні правоохоронного органу. На нашу думку, такий досвід доцільно врахувати у правоохоронній практиці України.

Слід мати на увазі, що результати негайного збереження та термінового зберігання динамічного (змінюваного) електронного відображення провайдер може надавати слідчому, прокурору, слідчому судді та суду у формі статичних зображень (так званих скриншотів, тобто миттєвих копій змісту екрана монітора), які фіксують стан динамічного електронного відображення у певний момент часу.

Під час кримінального розслідування може виникнути потреба у запобіганні злочину, про загрозу вчинення якого стало відомо з наявних матеріалів, із використанням можливостей мережі Інтернет. З цією метою в КПК України пропонується передбачити норму щодо надання органом розслідування провайдеру припису на блокування роботи певного Інтернет-ресурсу або певної IP-адреси (негайного або на певний строк), який є обов'язковим для виконання провайдером.

Умовами допустимості «класичного» документа як джерела доказів є такі: 1) має бути відомим автор документа (установа, організація, підприємство, посадова особа або громадянин); 2) зміст документа має відповідати компетенції і фактичній обізнаності автора. Це дозволяє перевірити доказ.

Вбачається, що такі умови допустимості слід висувати й до електронних відображень, що їх сформувала людина. Наприклад, пост (повідомлення) на форумі або у блозі, відправлений під ніком (мережевим псевдонімом), який не можна перевірити, є анонімним і не може бути використаний у доказуванні. При цьому слід мати на увазі, що відомості про автора (укладача) електронного відображення далеко не завжди зафіксовані на цьому відображенні, особливо, коли воно містить заборонений контент або прямо призначено для вчинення злочину. Це відрізняє електронне відображення від «класичного» документа, в якому відомості про автора здебільшого присутні на самому документі у вигляді найменування, реквізитів, прізвища, підпису тощо.

До електронних відображень, які створені інформаційною системою в автоматичному режимі, вимогу про відомість автора як умову допустимості доказу, очевидно, висувати не слід. Разом з тим у деяких випадках може виявитися необхідним 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 самим автором (електронні щоденники, приватні облікові записи тощо).

Якщо проблему допустимості електронних відображень можна вирішити шляхом внесення необхідних змін до кримінального процесуального законодавства, то відповідь на питання про їх достовірність як джерел доказів потребує розроблення сучасних експертних методик. Електронне відображення буде достовірним доказом, якщо його істинність в сенсі відповідності об'єктивній дійсності є встановленою й не викликає розумних сумнівів в чинній парадигмі знань.

У сфері судової експертизи сьогодні напрацьований ряд методик, що дозволяють вирішити низку завдань щодо визначення певних властивостей електронних відображень. Деякі з цих завдань знайшли нормативне закріплення у наказі Міністерства юстиції України [2]. Так, до основних завдань експертизи комп'ютерної техніки і програмних продуктів належать, зокрема:

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

– установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку;

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

Експертиза комп'ютерної техніки і програмних продуктів вирішує низку питань, серед яких є такі:

– чи міститься на даному носієві певна інформація та у 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 вона перенесена з іншого носія?

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

– яка 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 мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

– чи можливо виконання певних дій за допомогою даного програмного продукту?

– чи можливе вирішення певного завдання за допомогою даного програмного продукту?

– чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Для дослідження інформації, що міститься на комп'ютерному носієві, експерту надається сам носій. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду (виконуваного або вихідного модуля комп'ютерної програми).

У випадку необхідності експертного дослідження електронного відображення, яке є «шпигунською» програмою, може бути призначена експертиза телекомунікаційних систем і засобів, яка має відповісти на питання, зокрема:

– чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб?

– за допомогою яких програмних засобів здійснювалось несанкціоноване підключення до телекомунікаційної мережі?

Разом з тим експертні дослідження електронних відображень, які функціонують безпосередньо в комп'ютерній мережі, сьогодні не проводяться.

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

– ототожнення особи за фізичними параметрами голосу;

– встановлення технічних умов та технології отримання відео-, звукозапису.

Ідентифікаційна експертиза з ототожнення осіб проводиться за традиційними методиками й сьогодні не викликає

технологічних утруднень. Натомість, встановлення справжності (автентичності) цифрової фонограми (відеограми) залишається проблемним питанням для експертів, на яке слідчий, прокурор, слідчий суддя, суд не завжди можуть отримати відповідь.

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

Зважаючи на можливість фальсифікації електронних відображень, на нашу думку, доцільно ввести поняття підробленого електронного відображення, під яким слід розуміти електронне зображення з ознаками фальсифікації (підробки), підтвердженими висновком експерта.

Підроблене електронне відображення слід відрізняти від імітаційного електронного відображення, яке змістовно може не відрізнятися від справжнього, проте використовуватися з метою імітації справжнього електронного відображення, зокрема такого, що має офіційний статус (Інтернет-портали, сайти з ліцензованою діяльністю), а також імітації ділового та приватного електронного листування. Основною ознакою імітаційного електронного відображення є його створення від імені іншої фізичної або юридичної особи, зокрема, використовуючи мережевий аккаунт (обліковий запис) іншої особи.

Важливим є питання оцінки електронних відображень як доказів. Згідно з 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 точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення.

Оцінка електронних відображень як доказів, зважаючи на їх особливості (змінюваність у часі, незалежність від матеріального носія, відсутність різниці між оригіналом та копією, регламентованість доступу до окремих частин електронного відображення) має проводитися комплексно, у співставленні з іншими доказами у кримінальному провадженні.

При оцінці електронного відображення співставляють між собою окремі відомості, що в ньому містяться, а також з'ясовують причини виявлених протиріч.

Якщо факт кримінального правопорушення позначився на кількох електронних відображеннях, слід співставити зміст всіх цих відображень на предмет виявлення можливих протиріч.

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

При оцінці електронних відображень, що містять відомості про факти електронних комунікацій абонентів (користувачів), задля забезпечення достовірності доказів, які не підтверджуються іншими доказами, слід перевірити технічну інформацію, що міститься в електронних пристроях всіх задіяних абонентів, яка має співпадати за своїми параметрами (телефонні номери або IP-адреси абонентів, дата, час, тривалість комунікації).

В ході оцінки електронних відображень слід з'ясовувати:

1) походження електронного відображення та час його створення (на якому комп'ютері було створено, хто є автором

(укладачем), коли було створено і коли вносилися зміни);

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

3) джерело обізнаності особи, яка сформувала електронне відображення;

4) дотримання при створенні електронного відображення вимог закону (чи підлягає це відображення офіційній реєстрації та чи зареєстроване воно, чи підлягає ліцензуванню діяльність, що ведеться із застосуванням електронного відображення і 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 оцінки електронних відображень можуть бути проведені слідчі (розшукові) дії – допит авторів (укладачів), призначено експертизу (комп'ютерної техніки і програмних продуктів, відео-, звукозапису), зіставлені електронні відображення з іншими джерелами доказів, що засвідчують певні обставини кримінального правопорушення. Обсяг дій з перевірки електронних відображень залежить від виду останніх. Так, обсяг перевірки електронних відображень, створених інформаційною системою в автоматичному режимі, очевидно менший за обсяг перевірки електронних відображень, створених людиною. А обсяг перевірки електронного відображення, яке містить заборонений контент, відповідно менший, ніж обсяг перевірки відображення, що містить відомості про факти комп'ютерного шахрайства.

Оцінка електронних відображень слідчим, прокурором, слідчим суддею та судом, так само, як інших доказів у кримінальному провадженні має бути всебічною (враховуючою всі обвинувальні та виправдувальні доводи), повною (що враховує результати співставлення з іншими доказами та пропонує всі необхідні висновки) й неупередженою (об'єктивною).

Електронні відображення мають зберігатися у матеріалах кримінального провадження в опечатаному конверті (якщо це дозволяють розміри матеріального носія) або разом із цими матеріалами в окремій опечатаній упаковці (якщо носій має значні розміри). При цьому слід вживати заходів щодо убезпечення зафіксованої на носієві інформації від знищення.

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

Зважаючи на специфіку електронних відображень, доцільним вбачається розробити проект «Порядку зберігання електронних відображень», який має бути затверджений постановою Кабінету Міністрів України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року (із змінами та доповненнями) // Відомості Верховної Ради України. – 2013. – № 9–10, 11–12, 13. – Ст. 88.

2. 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 08 жовтня 1998 року № 53/5. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0001–13.

3. Теория доказательств в советском уголовном процессе / Отв. ред. Н. В. Жогин. – М., Юрид. литра, 1973. – 735 с.

Cherniavskyi S., Orlov J. Electronic display as a source of evidence in criminal proceedings

Informatization of social life objectively affects the peculiarities of the criminal process. In particular, this applies to such an important category as the source of evidence.

According to Art. 84 of the CPC of Ukraine, evidence in criminal proceedings are factual data obtained in accordance with the procedure provided for in this Code, on the basis of which an investigator, a prosecutor, an investigating judge and a court determine the presence or absence of facts and circumstances that are relevant to the criminal proceedings and are subject to proof.

The procedural sources of evidence, the current legislation recognizes evidence, material evidence, documents and expert opinions.

On the criterion of criminal proceedings electronic displays are similar to substantive evidence.

Electronic display can exist in various forms, in particular: the named area of data – a file; An array of data with a unique Internet address – a site; Collection of systematized data – database; A combination of computer instructions and data – a computer program; Information exchange tool – messenger and the like. It can be static (file) or dynamic, variable (web site, chat, traffic). However, in any case, the main property of electronic display remains its integrity, systemicity, structuring. It is perceived by man as a single holistic object, the content of which is certain information that can be used as evidence in a criminal proceeding.

Consequently, the CPC of Ukraine is invited to add to Article 1001 the following content:

«Article 1001. Electronic display

1. An electronic display is an integral system of information and (or) computer instructions in the information network or on a technical medium that can be used as proof of the fact or circumstances that are established during the criminal proceedings.

2. Electronic displays, provided the information provided for in part one of this article is in them, includes:

1) portals, sites in the computer network;

2) electronic databases;

3) files and groups of files;

4) the content of e-mail, chats;

5) output and executable modules of computer programs;

6) other information and (or) computer instructions in the information network or on the technical carrier».

Keywords: *evidence, sources of evidence, electronic display.*

Стаття надійшла до редакції журналу 12.05.2017 р.