

ОСОБЛИВОСТІ ОГЛЯДУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У статті досліджено сутність терміну «електронний документ», досліджені властивості та особливості електронного документа, які відрізняють його від інших засобів доказування. Досліджено сутність слідчого огляду електронних документів і особливості його проведення, пов'язані зі збором і дослідженням електронних документів. Вивчено особливості процесуального закріплення електронних доказів, а також тактичні особливості оформлення результатів слідчого огляду як самостійної процесуальної дії. У статті досліджені найбільш оптимальні та раціональні прийоми, які дозволяють досягти мети огляду електронних документів. Проаналізовані особливості огляду електронних документів, які розміщені в мережі Інтернет, а також узагальнено основні правила поведінки з електронними документами під час здійснення кримінального провадження.

Ключові слова: електронний документ, огляд електронних документів, слідчий огляд, тактичні прийоми, дослідження документів.

Постановка проблеми. Науково-технічний прогрес, глобальна інформатизація суспільства створюють передумови для більшості науковців стверджувати, що світ стоїть на порозі нового етапу свого розвитку – від постіндустріального до інформаційного (цифрового) суспільства, головним атрибутом якого є інформаційні технології.

Комп'ютерні технології не просто проникають в усі сфери суспільного життя, а й створюють новий простір його існування – віртуальний, цифровий, який закономірно стає частиною злочинного світу. Одночасно із розвитком новітніх технологій виникають й якісно нові типи злочинів, нові способи їх вчинення, об'єктивна сторона злочинів та її окремі елементи стають частиною віртуального простору, який містить в собі ознаки кримінальних правопорушень.

Огляд електронних документів, дослідження цифрових доказів, пошук віртуальних слідів стають традиційними слідчими діями, вчинення яких стає однією з умов розслідування злочинів. У зв'язку із цим, криміналістичне вчення перестає існувати в її традиційному уявленні, а електронні документи стають головним джерелом криміналістично значимою інформації.

Стан дослідження. Досліджуваний у даній статті проблематиці, а також її окремим питанням присвячували свої праці такі науковці, як: В.І. Алексейчук, Р.С. Белкін, А.Г. Волеводз, А.Ф. Волобуєв, В.А. Журавель, Н.І. Клименко,

К.М. Ковальов, В.О. Коновалова, Д.Я. Мирський, О.В. Одерій, М.В. Салтевський, М.Я. Сегай, В.Ю. Шепітько та ін.

Метою даної статті є аналіз сутності та правової природи електронних документів, дослідження тактичних прийомів проведення слідчого огляду електронних документів, а також узагальнення основних правил поведінки із електронними документами.

Для досягнення поставленої мети визначено наступні завдання:

- проаналізувати сутність та правову природу електронних документів як самостійних джерел доказової інформації в кримінальному провадженні;
- визначити специфіку, ознаки та сутнісні характеристики електронних документів;
- дослідити основні тактичні прийоми проведення слідчого огляду електронних документів;
- охарактеризувати особливості оформлення результатів слідчого огляду електронних документів як самостійної процесуальної дії;
- узагальнити правила поведінки із електронними документами під час проведення досудового розслідування кримінальним правопорушень.

Виклад основних положень. Однією з найскладніших процесуальних дій під час здійснення досудового розслідування є слідчий огляд електронних документів, складність якого полягає у відсутності достатніх теоретичних

досліджень у даному напрямку, а як наслідок – відсутність узагальнених тактичних прийомів огляду електронних документів.

Положення Кримінального процесуального кодексу України визначають «документ» як спеціально створений з метою збереження інформації матеріальний об'єкт, що 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.

Нормативне визначення «електронного документа» міститься в Законі України «Про електронний документ та електронний документообіг», відповідно до частини 1 статті 5 якого електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [1].

Разом з тим, електронний документ в криміналістичному значенні має певні відмінності від його нормативного визначення. Так, Т.Е. Кукарнікова визначає електронний документ як об'єкт, що несе інформацію, яка має значення для встановлення обставин, що підлягають доказуванню у кримінальному провадженні, та існує тільки в електронному середовищі у вигляді, допустимому для використання у кримінальному провадженні.

На думку К.А. Сергєєвої, електронний документ – це матеріальний носій, на якому за допомогою електронних апаратно-технічних і програмних засобів зафіксована інформація, яка має змістове значення, що засвідчує будь-який факт або подію, що підтверджує право на що-небудь; яка може бути перетворена у форму, придатну для однозначного сприйняття людиною, та має атрибути для ідентифікації [5, с. 183].

На нашу думку, під електронним документом необхідно розуміти будь-яку інформацію, представлену в електронній формі, що має значення для розслідування кримінальних правопорушень, дослідження якої здійснюється за допомогою спеціальних програмно-технічних засобів.

Пізнання сутності того чи іншого об'єкта здійснюється через дослідження його ознак та характерних властивостей, які визначають індивідуальність об'єкта дослідження, визначають причини його виокремлення серед інших об'єктів оточуючого світу. Електронні докумен-

ти володіють власними специфічними ознаками, які, в свою чергу, визначають специфіку огляду таких документів як самостійної процесуальної дії.

Перш за все, електронний документ не має матеріальної форми існування. За своєю сутністю електронний документ – це двійковий комп'ютерний код, який створений за допомогою комп'ютерних засобів та існує на технічних носіях. Він не має матеріального виразу та існує у нематеріальній формі на спеціальних засобах.

Відсутність матеріальної форми існування зумовлює нерозривний взаємозв'язок електронного документа із технічним носієм, на якому такий документ зберігається. Електронний доказ не може існувати поза межами технічного носія. Наприклад, будь-яка криміналістично значима інформація, яка знаходиться в мережі Інтернет, має свій технічний носій – сервер, а тому при розслідування окремих кримінальних правопорушень мета досудового розслідування може бути досягнута лише після отримання доступу до такого носія. Разом з цим, електронний документ не має нерозривного зв'язку із певним технічним носієм, може вільно переміщуватися в електронній мережі без технічного носія та існувати одночасно на кількох технічних носіях.

Зважаючи на те, що електронний документ – це певний комп'ютерний код, то такий код може бути прочитаний лише за допомогою спеціальних засобів, які забезпечують тлумачення цифрового коду та його перетворення в доступну для сприйняття форму. Одночасно із цим, така особливість електронного документа як доказу зумовлює особливість його слідчого огляду як окремої процесуальної дії. Слідчий або інший учасник кримінального провадження не може дослідити електронний документ без спеціальних засобів, а тому, як правило, така процесуальна дія здійснюється за допомогою спеціального обладнання на робочому місці слідчого. При цьому огляд та дослідження фізичного носія електронного документа не є дослідженням самого електронного документа. В такому разі фізичний носій може виступати лише в якості речового доказу.

Під час огляду електронних документів варто брати до уваги, що електронний документ є більш «вразливим» доказом у порівнянні з традиційними засобами доказування. Вразливість електронного доказу полягає в тому, що він може

бути або легко знищений, або зміст якого може бути змінений, модифікований тощо без будь-яких очевидних ознак. Як правило, такі ознаки не можливо встановити шляхом традиційного дослідження змісту електронного документа, що, в свою чергу, може спричинити втрату важливої криміналістично значимої інформації.

Наприклад, злочинець вносить зміни до комп'ютерного коду електронного доказу та змінює інформацію про час його створення. Невідповідність часу створення документа іншим обставинам злочину може призвести до неможливості його розкриття або до створення «цифрового алібі», що виключає можливість притягнення особи до кримінальної відповідальності. При цьому зміни до електронного документа, пов'язані зі зміною його комп'ютерного коду, неможливо встановити під час огляду електронного документа слідчим.

«Вразливість» електронного документа зумовлює необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи. Зокрема, на рівні з традиційними правилами поведіння із документами, необхідно враховувати технічні особливості збирання, зберігання та використання інформації.

Процес огляду електронних документів в цілому відповідає загально прийнятому алгоритму дій, які вчиняються слідчим під час огляду звичайних документів. Такий комплекс дій повинен складатися з наступного: 1 – пошук і виявлення документів; 2 – візуальний огляд зовнішнього стану без зміни умов сприйняття; 3 – фіксація за допомогою фотозйомки; 4 – фіксація в протоколі відповідної слідчої дії (фіксуються всі дії посадових осіб, стан документа і виявлені сліди); 5 – виявлення слідів рук (на фізичному носії електронного документа); 6 – виявлення слідів зміни первісного змісту; 7 – підготовка до упаковки; 8 – упаковка [2, с.129].

Разом з тим, слідчий огляд електронних документів здійснюється з урахуванням певних особливостей об'єкту дослідження, що впливає як на сам процес дослідження, так і на спосіб процесуального закріплення отриманих результатів.

Так, під час пошуку електронних документів необхідно мати на увазі, що вони завжди розміщені на окремих фізичних носіях (USB-флеш-накопичувач, диски, тощо), або можуть бути розміщені в мережі Інтернет, зокрема,

на спеціальних на спеціальних «хмарних» сервісах зберігання інформації. Будь-які дії з електронними документами необхідно здійснювати за допомогою сертифікованого обладнання із ліцензійним забезпеченням. Несертифіковане обладнання може привести до втрати електронних документів, випадкового знищення реквізитів або окремих складових електронних доказів. За можливості до збирання та вилучення електронних доказів необхідно залучати спеціалістів, які з технічної точки зору забезпечать збереження необхідних документів.

Фізичні носії електронної інформації, на яких може знаходитися криміналістично важлива інформація, вилучаються при огляді місця події, оглядах та обшуках житла чи робочих приміщень, при огляді речей та комп'ютерної техніки учасників кримінального провадження. Якщо електронні докази розміщені на серверах чи жорстких дисках підприємств, установ або організацій, слідчому рекомендується здійснити побайтову копію носія інформації, адже вилучення майна підприємства може призвести до негативних наслідків. За допомогою спеціального обладнання відтворюється ідентична копія електронної інформації, яка знаходиться на технічному носії, після чого самі фізичні носії повертаються власникам. Аналогічні дії необхідно здійснювати, коли виникає необхідність в проведенні комп'ютерно-технічної експертизи.

Перед дослідженням змісту електронного документа слідчий повинен встановити тип фізичного носія, на якому розміщений електронний документ, для підготовки необхідного обладнання для роботи з таким носієм. У разі, якщо технічний носій інформації захищений від будь-якого стороннього доступу до їх змісту, то фізичний носій має бути переданий експерту на предмет встановлення можливого доступу до електронної інформації, яка зберігається на таких носіях. Окрім того, за допомогою експертизи можливо встановити факт втручання до електронного документа, факт внесення яких-небудь змін та час їх здійснення.

Огляд електронних документів, розміщених на фізичному носії інформації, здійснюється шляхом безпосереднього сприйняття слідчим інформації, що міститься в електронному документі, за допомогою службового комп'ютера. В змісті самого протоколу огляду варто зазначити технічні характеристики та серійні номери обладнання, назви та версії програмного забез-

печення, що використовуються в ході слідчого огляду.

Під час дослідження електронного документа особливу увагу необхідно звертати на його формат, розмір, хронологію створення, користувача, яким було створено документ. За допомогою фото- та відеоматеріалів ідентифікуються місце зйомки. В процесі огляду документа слідчий в обов'язковому порядку звертає увагу на найменування та місцезнаходження установи, автора документа, назву виду документа, дату та час його виготовлення, зміст електронного документа, наявність електронного цифрового підпису.

Електронний документ перевіряється на зараження його вірусом, на цілісність і справжність усіх накладених на нього електронних цифрових підписів, включаючи ті, що накладені (проставлені) згідно із законодавством як аналогі печатки чи підпису посадової особи. Також перевіряється наявність супровідної документації – заповненої реєстраційно-контрольної картки в електронній та/чи паперовій формі, повідомлення про прийняття та реєстрацію електронного документа [9, с. 161]. У разі неможливості встановлення вище перелічених обставин, слідчий розглядає можливість призначення комп'ютерно-технічної експертизи.

На завершальному етапі огляду електронних документів, розміщених на фізичному носії інформації, такі документи роздруковуються або копіюються на диск та додаються до протоколу як його невід'ємний додаток, із зазначенням серійних номерів та технічних характеристик обладнання, за допомогою якого створено такий додаток [5, с. 186].

Окрему увагу варто приділити огляду електронних документів, розміщених в мережі Інтернет. Інтернет, соціальні мережі, електронна переписка останнім часом стають одним з найголовніших джерел інформації, яка має значення для розслідування злочинів. Як правило, така інформація має орієнтований характер та використовується в оперативній діяльності.

Разом з тим, в мережі Інтернет можуть бути розміщені докази, які можуть бути використані в якості електронних документів під час кримінальних проваджень. Наприклад, розповсюдження викрадених творів науки або літератури в мережі Інтернет є окремим складом злочину, передбаченим ст. 176 КК України. Основним доказом є електронні матеріали, викладені в світовій мережі, а тому завданням слідчого є

виявлення таких документів, фіксування факту розповсюдження електронних документів та належне оформлення результатів слідчого огляду.

У протоколі огляду слід зазначити серійний номер службового комп'ютера, назву та версію операційної системи, яка встановлена на даному комп'ютері, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі Інтернет [5, С. 187].

Головним атрибутом електронного документа, розміщеного в мережі Інтернет, є його адреса (домен). Окрім домену, в протоколі огляду необхідно вказувати URL веб-сторінки, який завжди є індивідуальним, а тому використовується як один з способів ідентифікації необхідної веб-сторінки, на якому розміщені електронні матеріали, що мають значення для розгляду справи. В протоколі огляду веб-сторінки в мережі Інтернет обов'язково вказуються стандартні реквізити документа: назва, автор та час створення електронних документів, якщо такі відомі, призначення документа, стислий зміст та інші викладені в ньому обставини, які мають значення для розслідування злочину.

Як вже було зазначено вище, властивістю електронних документів є їх вразливість. Особливо це стосується електронних документів, розміщених в мережі Інтернет. Особа, яка має доступ до таких доказів, має можливість їх оперативно знищити, змінити їхній зміст, у зв'язку із чим, електронний документ, як головний доказ, який відображає подію злочину, буде відповідно знищений чи змінений. Одночасно із цим, електронні докази в мережі Інтернет можуть бути знищені інтернет-провайдерами, в розпорядженні яких знаходяться сервери. Інформація, яка зберігається на серверах, є досить об'ємною, а тому інтернет-провайдери намагаються її оперативно оновлювати задля можливості використання такого простору.

Одним з способів фіксування електронних документів, розміщених в мережі Інтернет, є вилучення серверів, на яких зберігаються електронні докази. Будь-яка інформація, яка передається за допомогою інформаційно-телекомунікаційних систем, зберігається на спеціальних технічних носіях – серверах, та у спеціальному вигляді – log-файлі. Відповідні log-файли можуть бути вилучені в інтернет-провайдерів та інших суб'єктів, які беруть участь у процесі інформаційно-телекомунікаційної передачі даних та у фактичному володінні яких знаходяться сервери.

Разом з тим, відповідно до ч. 3 ст. 99 КПК України оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке ж значення, як документу. Відповідна норма дозволяє використовувати в якості електронних документів інформацію, яка знаходиться в мережі Інтернет, без отримання безпосереднього доступу до фізичних носіїв такої інформації. Сервери, на яких розміщені електронні документи, що мають значення для кримінального провадження, можуть бути розміщені в будь-якій точці світу, що значно ускладнює процес отримання доступу до таких серверів та завдає шкоди кримінальному провадженню.

У зв'язку із цим, веб-сторінка із електронним документом, що оглядаються, можуть бути роздруковані та в письмовому вигляді додані до протоколу огляду. Якщо електронний документ містить фото-, відео-, аудіо матеріали, відповідні частини електронного документа повинні бути збережені та записані на фізичний носій інформації, який також стає невід'ємною частиною протоколу огляду електронного документа.

Висновки наукового дослідження і перспективи подальших розробок у даному напрямку. Електронний документ – це будь-яка інформація, представлена в електронній формі, що має значення для розслідування кримінальних правопорушень, дослідження якої здійснюється за допомогою спеціальних програмно-технічних засобів.

Сутність електронних документів пізнається через їх характерні ознаки, які полягають у відсутності матеріальної форми, наявності тісного взаємозв'язку із технічним носієм інформації, необхідності використання спеціальних технічних пристроїв для тлумачення змісту електронних документів, а також «вразливості» електронних документів, що полягає у відсутності стабільної структури та можливості змінювати їхній зміст без очевидних ознак втручання.

У порівнянні із оглядом традиційних документів огляд електронних документів є більш об'ємною та складнішою процесуальною дією, яка вимагає використання спеціальних знань, технічних засобів та програмного забезпечення, необхідності залучати спеціалістів для пошуку електронних доказів та їх вилучення під час кримінального провадження. Особливість огляду електронних документів полягає в осо-

бливих правилах фіксації отриманих результатів, необхідності використання фізичних носіїв зберігання електронних документів, а також вчинення додаткових процесуальних дій, спрямованих на забезпечення достовірності електронного документа та з метою подальшого їх використання в якості доказу.

Перспективами подальших розробок у даному напрямку є дослідження способів збирання та процесуального закріплення результатів огляду електронних документів під час розслідування окремих категорій кримінальних правопорушень, а також аналіз останніх наукових та технічних досягнень, спрямованих на встановлення, дослідження та вилучення електронних документів з метою їх використання під час кримінального провадження.

Список використаних джерел:

1. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 р. № 851-15 в редакції від 30.09.2015 // [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/851-15>.
2. Бірюков В.В. Криміналістичне документознавство. – Київ: Паливода А.В. – 2007. – 331 с.
3. Гонгало С.Й. Електронні документи як об'єкти судової техніко-криміналістичної експертизи та їх класифікація / С. Й. Гонгало // Адвокат. – 2013. – № 1. – С. 33-36.
4. Даниленко А.В., Кочура О.О. Електронний документ як джерело доказової інформації у кримінальному провадженні / А.В. Даниленко, О.О. Кочура // Актуальні питання розслідування кіберзлочинів. Матеріали міжнародної науково-практичної конференції. – Х., 2013 р. – С. 147 – 150.
5. Коваленко А.М. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста / А.М. Коваленко // Вісник Національної академії правових наук України. – № 1(88). – 2017 – С. 182-191.
6. Козлов О.О. Проблеми фіксації, збирання та дослідження доказів, отриманих в мережі Інтернет / О. О. Козлов // Вестник Одесской адвокатуры. – 2015. – № 1. – С. 44-47.
7. Одерій О.В. Тактика слідчого огляду комп'ютерних систем та їх елементів / О.В. Одерій, С.О. Корона, С.В. Самойлов. – Донецьк, 2010. – 88 с
8. 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. – С. 12-24.

9. Пчеліна О.В. Особливості огляду електронного документа / О.В. Пчеліна // Актуальні питання розслідування кіберзлочинів. Матеріали міжнародної науково-практичної конференції. – Х., 2013 р. – С. 159 – 162.
10. Цехан Д.М. Цифрові докази: поняття, особливості та місце у системі доказування / Д.М. Цехан // Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція, 2013. – № 5. – С. 256-260.

Хижняк Е. С. Особенности осмотра электронных документов при расследовании уголовных правонарушений

В статье исследована сущность термина «электронный документ», исследованы свойства и особенности электронного документа, которые отличают его от других средств доказывания. Исследована сущность следственного осмотра электронных документов и особенности его проведения, связанные со сбором и исследованием электронных документов. Изучены особенности процессуального закрепления электронных доказательств, а также тактические особенности оформления результатов следственного осмотра как самостоятельного процессуального действия.

В статье исследованы наиболее оптимальные и рациональные приемы, которые позволяют достичь цели осмотра электронных документов. Проанализированы особенности осмотра электронных документов, размещенных в сети Интернет, а также обобщены основные правила обращения с электронными документами при осуществлении уголовного производства.

Ключевые слова: *электронный документ, осмотр электронных документов, следственный осмотр, тактические приемы, исследования документов.*

Khyzhniak E. S. Peculiarities of the digital document review during the investigation of criminal offenses

The article studies the essence of the term “digital document”, the properties and features of the digital documents which distinguish it from other means of proof. The essence of the digital document examination and the peculiarities of its conduct related to the collection and research of digital documents were examined. The article examines the peculiarities of the procedural fixing of digital evidence, as well as the tactical peculiarities of results preparation of the investigative examination as an independent procedural action.

The article examines the most optimal and rational methods that allow to achieve the purpose of examining digital documents. The features of examination of digital documents placed on the Internet are analyzed, as well as general rules for handling digital documents in the implementation of criminal proceedings.

Key words: *digital document, examination of digital documents, investigatory examination, tactical receptions, examination of the documents.*