УДК 343.140.01

Ратнова Аліна Володимирівна –
ад'юнкт кафедри кримінального процесу та криміналістики
ІПФПНП №1 Львівського державного університету внутрішніх справ

Alina V. Ratnova –
PhD student of the criminal procedure and forensic of Faculty No.1,
Lviv State University of Internal Affairs
(26 Horodotska Street, Lviv, 79000, Ukraine)

Класифікація електронних документів, як джерел доказів у кримінальному провадженні

У статті розглядаються існуючі класифікації електронних документів, як джерел доказів у кримінальному провадженні. Проаналізовано наукові дослідження, слідчо-судову практику та обґрунтовано критерії класифікації електронних документів.

Ключові слова: *документ, електронний документ, метадані, підстави класифікації, доказування.*

В статье рассматриваются существующие классификации электронных документов, как источников доказательств в уголовном производстве. Проанализированы научные исследования, следственно-судебную практику и обоснованы критерии классификации электронных документов.

Ключевые слова: *документ, электронный документ, метаданные, основания классификации, доказывание.*

A.V. Ratnova Classification of Electronic Documents as Sources of Evidence in Criminal Proceedings

The article is devoted to the study of existing types of classification of electronic documents as sources of evidence in criminal proceedings. The same classifications as for documents may be applied to electronic documents. Attention is drawn to the fact that electronic documents can be classified according to other specific criteria.

The division of electronic documents by stages of production is considered and the possibility of distinguishing between the original and the duplicate electronic document is substantiated. The division of electronic documents by a combination of metadata into peers; two-rank; three-level; four-rank, five-rank. According to access to information, metadata of electronic documents can be divided into open and hidden. Any user can receive open metadata, and hidden metadata can be obtained only after using special software. Electronic documents are divided according to the degree of protection into open and closed (use of electronic digital signature, passwords, etc.).Electronic documents are classified by source and it is established that files can be created by a user or a computer system depending on the settings of the software and hardware. Electronic documents can be classified according to their location: computer, smartphone, tablet, video camera, "smart" home appliances, Internet server are by nature types of computers. According to the form, electronic documents can be divided into video recordings, audio recordings, electronic messages, websites and information in electronic form.

Classification of electronic documents makes it possible to develop tactics for collecting, checking and evaluating electronic documents, to improve forensic methods of investigating crimes in which electronic documents are evidence.

Keywords: *document, electronic document, metadata, grounds for classification, proving.*

Постановка проблеми. Електронний документ як джерело доказу, незважаючи на поширеність його використання у доказуванні залишається одним з найменш дослідженим та вивченим інститутом. Відсутність єдиних вимог збирання, перевірки, оцінки електронних

документів утруднює досягненню завдань кримінального провадження, закріплених у КПК України. Тому, класифікація електронних документів за різними критеріями слугуватиме вдосконаленню вимог перевірки та оцінки електронних документів, розробленню нової тактики та методики роботи з таким видом доказів,

Аналіз останніх досліджень і публікацій. Питанням класифікації електронних документів у своїх роботах приділяли увагу такі вчені: С.Й. Гонгало, Т.Е. Кукарникова, Ю.Ю. Орлов, С.С. Чернявський, О.В. Шведова та інші.

Водночас, незважаючи на дослідження вищевказаних науковців, залишаються **невирішеними раніше проблеми** класифікації електронних документів з урахуванням їх особливостей.

Метою статті є аналіз існуючих класифікацій документів та обґрунтування необхідності виділення окремої класифікації електронних документів.

Виклад основного матеріалу. Класифікація доказів – це поділ з метою дослідження складових частин цієї системи, яка має теоретичне і практичне значення для кримінального провадження. Завдяки такому поділу з'ясовуються особливості збирання, перевірки і оцінки доказів, їх значимість для доведення тих чи інших обставин, що входять до предмета доказування. Таке багатопланове значення класифікації доказів свідчить, що провести поділ доказів за однією ознакою чи властивістю неможливо [1, с.17].

Вважаємо, електронний документ можна класифікувати за тими ж критеріями, які застосовуються до документів як джерел доказів. В той же час, електронні документи, враховуючи їх особливості, мають інші додаткові класифікуючі ознаки.

Ми погоджуємося з думкою Гонгало С.Й. про те, що ***за стадіями виготовлення електронні документи поділяються на оригінали, дублікати, копії та витяги***[2, с.34]**.** Однак, не вважаємо, що цей поділ є досить умовним.

У ч. 3, ч.4, ст. 99 КПК надано визначення, що є оригіналом та дублікатом документа. Відповідно, оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке ж значення, як документу.

Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

Отже, оригіналом електронного технічного документа є той, який створений та зберігається на первинному носії інформації. Наприклад, оригінал відеозапису з камер відеоспостереження зберігається на носії інформації, на який записується відео. Дублікатом (копією) такого відеозапису є його копіювання, переміщення, поширення на інший носії інформації.

На нашу думку, роздруківка веб-сторінки, частини відео, фото чи іншого файлу не можуть бути визнані ні оригіналом ні копією електронного документа та самостійно не може бути використана як доказ. Візуалізована у паперовій формі сторінка може бути використана лише як додаток до проведеної слідчої (розшукової) дії. Правильне виготовлення дубліката електронного документа забезпечує його допустимість під час перевірки доказів у суді.

Наприклад, Зарічний районний суд м. Суми вироком від 28 квітня 2016 року за обвинуваченням в скоєнні гр. П. кримінальних правопорушень, передбачених ч. 2 ст. 407, ч. 3 ст. 15, ч. 1 ст. 258-3 КК України визнав роздруківки місця знаходження радіоелектронного засобу неналежними і недопустимими доказами. Відсутність первинних носіїв та вказаних відомостей в роздруківці та протоколі ставить під сумнів достовірність інформації, що міститься в них, та дає суду підстави стверджувати, що втручання у приватне спілкування гр. П. відбулось не у спосіб, що встановлений КПК України [3].

Також, під час розгляду у судовому засіданні кримінального провадження щодо обвинувачення гр. Ф. у вчиненні кримінального правопорушення, передбаченого ч.1 ст.258-3 КК України, Апеляційний суд м. Києва зазначив, що не можуть бути джерелом доказування та є

недопустимими доказами фотокартки та скріншоти, отримані внаслідок моніторингу сторінок користувачів, яких орган досудового розслідування ототожнює з представниками ДНР, у соціальних мережах «Вконтакте» і «Одноклассники», оскільки достовірність інформації, яка в них міститься, викликає обґрунтовані сумніви та вони отримані у спосіб, не передбачений кримінальним процесуальним законом [4].

Відповідно до ч. 3, ч.4, ст. 99 КПК сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції, узагальнення документів, які незручно повністю досліджувати в суді, а на вимогу суду – зобов'язані надати документи у повному обсязі.

Так як електронний документ може містити великий обсяг інформації, то доцільно створювати витяги, узагальнення, компіляції. Витягом, компіляцією чи узагальненням електронного документа є копіювання та виділення за допомогою технічних пристроїв частини інформації, яка встановлює наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Витяг із документа — частина тексту документа. Витягом електронного документа є частина електронного документа. У витязі з електронного документа, частина інформації та зміст ідентично відтворюються з основного документа.

Узагальнення та компіляція електронного документа, на нашу думку, необхідна тоді, коли уся інформація є важливою та не підлягає окремому виділенню частини.

Обсяг та форма такого виокремлення інформації чітко не встановлені та фактично визначаються за внутрішнім переконанням слідчого та прокурора під час досудового розслідування. Головним завданням є відсіяти інформацію, яка не є суттєвою та виявити інформацію, яка має значення під час доказування. Наприклад, вирізання частини звукозапису чи відеозапису, збільшення частини фотографії чи зображення, узагальнення змісту сторінки веб-сайту тощо. Ця дія є суб'єктивною, тому оцінити правильність складання скороченого чи узагальненого електронного документа може лише суд. Таким чином, якщо слідчим чи прокурором зроблено витяг, компіляцію чи узагальнення електронного документа, то його разом із повним за обсягом і змістом оригіналом необхідно долучати до матеріалів кримінального провадження.

Одним із найбільш складних є спосіб ***класифікації документів залежно від комбінацій метаданих***– структурованих закодованих даних, які характеризують електронний документ та мають доказове значення у кримінальному провадженні [5, с.83].Залежно від комбінації метаданих електронні документи можуть бути поділені на однорангові (наприклад з розширенням *.wav, *.gif); дворангові; трирангові; чотирирангові, п'ятирангові (наприклад гіпертекст) [6, с.35].

За доступом до інформації, метадані електронних документів можна поділити на відкриті та приховані. До відкритих метаданих можна віднести ті, які звичайний користувач створює самостійно або може побачити за допомогою перевірки властивостей документа. Наприклад, до них можна віднести дату та час створення, зміни, якщо це електронний лист, то ім'я адресата, дату надсилання документу тощо. Приховані метадані доступні користувачеві лише за допомогою використання спеціального технічного забезпечення та відповідних програм. Встановлення прихованих метаданих під час проведення експертизи електронного документа дозволяє встановити так звані «електронні сліди» створення, редагування, видалення чи зміни документа.

За ступенем захисту електронні документи можна поділити на відкриті та закриті. Для захисту електронних документів існує велика кількість спеціальних засобів: електронний цифровий підпис, шифрування поштових відправлень та мережевого трафіку, використання систем захисту від несанкціонованого доступу в мережах, установка пароля на документі, тощо [7, с.73].

За джерелом походження виділяються файли, які створюються користувачем та комп'ютерною системою (тобто самим електронним середовищем) [8, с.10; 7, с.69]. Автоматично створюються кеш-файли, cookie-файли, метадані за замовчуванням налаштувань програми тощо. Більшість електронних документів створюються користувачем та

передбачають введення інформації особисто. При підключенні до Інтернету, велика кількість інформації про діяльність користувача записується і зберігається у комп'ютері. Кеш-файли найчастіше використовуються експертами під час дослідження електронних документів. Окрім кеш-файлів, браузер також може зберігати cookie-файли, а саме інформацію про певного користувача у браузері та передачі на веб-сайт, який раніше відвідувався. Наприклад, збереження паролю та логіну особистої сторінки, або ж веб-сайт пропонує інформацію, послугу, товар, яким ви раніше цікавились на іншому сайті. Аналіз судової практики вказує на те, що слідчі не часто, однак звертаються до суду для отримання інформації про дані з файлів cookie, що зберігаються на пристрої, в тому числі ідентифікатори і налаштування файлів cookie [9, 10], файли cookie для користування поштовою скринькою [11,12] тощо.

Класифікацію електронних документів можна здійснити за їх місцем розташуванням: комп'ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер та інші. Інформація про місцезнаходження електронного документа необхідна під час отримання санкціонованого доступу до нього та встановлення його особливостей, які створюються внаслідок існування на певному технічному носії інформації.

Ми не погоджуємося з думкою, що не існує відмінностей в електронних документах, якими можна було б обґрунтувати виділення будь-яких електронних документів (наприклад, аудіо- та відеозаписи) в самостійний підвид, так як абсолютно байдуже, яка інформація (текст, відеозапис, аудіозапис і т. п.) записана на машинному носії [7, с.63].

Вважаємо, що електронні документи ***за формою можна поділити на відеозаписи, аудіо записи, електронні повідомлення, веб-сайти та інформацію у електронній формі [8, с.10].*** Під час аналізу судової практики встановлено, що найчастіше судами досліджується такий вид електронного доказу, як відеозапис. Це можуть бути як відеозаписи з подією вчинення злочину так і відеозаписи зі слідчими діями, слідчими експериментами тощо. Також, є випадки дослідження судом аудіозапису (телефонних розмов з повідомленням про злочин, аудіозапис із плачем дитини та звуками ударів тощо). Окрім цього, бувають випадки дослідження скріншотів електронних сторінок з листуванням [13].

Теоретичне та практичне значення класифікації електронних документів полягає у тому, що вона допомагає правильно використовувати їх як докази, сприяє збиранню, перевірці (дослідженню їх для встановлення наявності чи відсутності ознак втручання) та оперуванню ними в доказуванні під час розслідування та судового розгляду [14, с.33].

Висновки. На підставі аналізу слідчо-судової практики, наукових досліджень узагальнено та вдосконалено класифікацію електронних документів у кримінальному провадженні. Встановлено, що електронні документи за стадіями виготовлення поділяються на оригінали, дублікати, копії та витяги. За комбінацією метаданих електронні документи можуть бути поділені на однорангові, дворангові, трирангові, чотирирангові, п'ятирангові. В залежності від доступу до метаданих можна поділити на електронні документи з відкритими та прихованими метаданими. За ступенем захисту електронні документи можна поділити на відкриті та закриті. За джерелом походження виділяються документи, які створюються користувачем та комп'ютерною системою. Класифікацію електронних документів можна здійснити за їх місцем розташуванням: комп'ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер, тощо. Електронні документи за формою можна поділити на відеозаписи, аудіо записи, електронні повідомлення, веб-сайти.

Систематизація критеріїв класифікації електронних документів дає можливість розробити тактику збирання, перевірки та оцінки електронних документів, вдосконалити криміналістичну методику розслідування окремих видів кримінальних правопорушень, у яких доказами можуть виступати електронні документи.

Список використаних джерел:

1. Стахівський С.М. Кримінально-процесуальні засоби доказування: автореферат дисертації на здобуття наукового ступеня доктора юридичних наук: 12.00.09. Київ, 2005. 31 с.
2. Гонгало С.Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку. Дисертація. Острог, 2013. 190 с.
3. Вирок Зарічного районного суду м. Суми від 28 квітня 2016 року. Справа № 591/2665/15-к. Провадження № 1-кп/591/40/16. Єдиний державний реєстр судових рішень: веб-сайт. URL: http://reyestr.court.gov.ua/Review/57452822.
4. Ухвала Апеляційного суду м. Києва від 29 червня 2017 року. Справа № 760/15925/15-к. ЗаконОнлайн: веб-сайт. URL: https://zakononline.com.ua/court-decisions/show/67858013.
5. Ратнова А.В. Використання метаданих під час проведення експертизи електронного документа у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування*: тези доповідей учасників науково-практичного семінару (30 листопада 2018 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. С. 81-83.
6. Гонгало. С.Й. Классификация электронных документов как объектов судебной технико-криминалистической экспертизы документов. *Вестник Томского государственного университета*. 2013. № 367. С. 95–97.
7. Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике: дисс. … к.ю.н. Воронеж, 2003. 204 с.
8. Каламайко А. Ю. Електронні засоби доказування в цивільному процесі: автореф. дис. ... канд. юрид. наук: 12.00.03. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків. 2016. 20 с.
9. Ухвала Печерського районного суду м. Києва від 12.07.2018 року Справа № 757/32158/18-к. Єдиний державний реєстр судових рішень: веб-сайт. URL: http://reyestr.court.gov.ua/Review/75396252.
10. Ухвала Печерського районного суду м. Києва від 12.07.2018 року. Справа № 757/32174/18-к. Єдиний державний реєстр судових рішень: веб-сайт. URL: http://reyestr.court.gov.ua/Review/75396270.
11. Ухвала Старокостянтинівського районного суду Хмельницької області від 21.03.2018 року. Справа № 683/362/17. Єдиний державний реєстр судових рішень: веб-сайт. URL: http://reyestr.court.gov.ua/Review/72967641.
12. Ухвала Галицького районного суду м. Львова від 11.05.2018 року Справа № 461/1143/18. Єдиний державний реєстр судових рішень: веб-сайт. URL: http://reyestr.court.gov.ua/Review/73935448.
13. Аналіз судової практики місцевих судів м. Харкова і Харківської області, Апеляційного суду Харківської області та Харківського апеляційного суду щодо використання електронних доказів (доказів вчинення злочину, які можна отримати в електронній формі) по справам, які перебували на розгляді у 2018 та 2019 роках. Харківський апеляційний суд: веб-сайт. URL: https://hra.court.gov.ua/sud4818/inshe/inf_court/uzag20k1.
14. Гонгало С.Й. Електронні документи як об'єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат*. №1 (148), 2013. С.33-36.

References:

1. Stakhivskyi S.M. Kryminalno-protsesualni zasoby dokazuvannia: avtoreferat dysertatsii na zdobuttia naukovoho stupenia doktora yurydychnykh nauk: 12.00.09. Kyiv, 2005. 31 s.
2. Honhalo S.Y. Sudova tekhniko-kryminalistychna ekspertyza dokumentiv: suchasni mozhlyvosti doslidzhennia ta perspektyvy rozvytku. Dysertatsiia. Ostroh, 2013. 190 s.
3. Vyrok Zarichnoho raionnoho sudu m. Sumy vid 28 kvitnia 2016 roku. Sprava № 591/2665/15-k. Provadzhennia № 1-kp/591/40/16. Yedynyi derzhavnyi reiestr sudovykh rishen: veb-sait. URL: http://reyestr.court.gov.ua/Review/57452822.
4. Ukhvala Apeliatsiinoho sudu m. Kyieva vid 29 chervnia 2017 roku. Sprava Sprava № 760/15925/15-k. ZakonOnlain: veb-sait. URL:https://zakononline.com.ua/court-decisions/show/67858013.

5. Ratnova A.V. Vykorystannia metadanykh pid chas provedennia ekspertyzy elektronnoho dokumenta u kryminalnomu provadzhenni. *Protsesualne ta kryminalistychne zabezpechennia dosudovoho rozsliduvannia:* tezy dopovidei uchasnykiv naukovo-praktychnoho seminaru (30 lystopada 2018 roku) / upor. A.Ya. Khytra. Lviv: LvDUVS. S. 81-83.

6. Honhalo. S.Y. Klassyfykatsyia elektronnykh dokumentov kak obektov sudebnoi tekhnyko-krymynalystycheskoi ekspertyzy dokumentov. *Vestnyk Tomskoho hosudarstvennoho unyversyteta*. 2013. № 367. S. 95–97.

7. Kukarnykova T. E. Elektronnyi dokument v uholovnom protsesse y krymynalystyke: dyss. … k.yu.n. Voronezh, 2003. 204 s.

8. Kalamaiko A. Yu. Elektronni zasoby dokazuvannia v tsyvilnomu protsesi: avtoref. dys. ... kand. yuryd. nauk: 12.00.03. Nats. yuryd. un-t im. Yaroslava Mudroho. Kharkiviu 2016. 20 s.

9. Ukhvala Pecherskoho raionnoho sudu m. Kyieva vid 12.07.2018 roku Sprava № 757/32158/18-k. Yedynyi derzhavnyi reiestr sudovykh rishen: veb-sait. URL: http://reyestr.court.gov.ua/Review/75396252.

10. Ukhvala Pecherskoho raionnoho sudu m. Kyieva vid 12.07.2018 roku. Sprava № 757/32174/18-k. Yedynyi derzhavnyi reiestr sudovykh rishen: veb-sait. URL: http://reyestr.court.gov.ua/Review/75396270.

11. Ukhvala Starokostiantynivskoho raionnoho sudu Khmelnytskoi oblasti vid 21.03.2018 roku. Sprava № 683/362/17. Yedynyi derzhavnyi reiestr sudovykh rishen: veb-sait. URL: http://reyestr.court.gov.ua/Review/72967641.

12. Ukhvala Halytskoho raionnoho sudu m. Lvova vid 11.05.2018 roku Sprava № 461/1143/18. Yedynyi derzhavnyi reiestr sudovykh rishen: veb-sait. URL: http://reyestr.court.gov.ua/Review/73935448.

13. Analiz sudovoi praktyky mistsevykh sudiv m. Kharkova i Kharkivskoi oblasti, Apeliatsiinoho sudu Kharkivskoi oblasti ta Kharkivskoho apeliatsiinoho sudu shchodo vykorystannia elektronnykh dokaziv (dokaziv vchynennia zlochynu, yaki mozhna otrymaty v elektronnii formi) po spravam, yaki perebuvaly na rozghliadi u 2018 ta 2019 rokakh. Kharkivskyi apeliatsiinyi sud: veb-sait. URL: https://hra.court.gov.ua/sud4818/inshe/inf_court/uzag20k1.

14. Honhalo S.Y. Elektronni dokumenty yak ob'iekty sudovoi tekhniko-kryminalistychnoi ekspertyzy ta yikh klasyfikatsiia. *Advokat.* №1(148), 2013. S.33-36.