УДК 343.9
DOI 36919/3041-1149(Print).3.2024.90-95

М. М. Фрідман-Козаченко,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
та криміналістики,
Академія Адвокатури України
email: mariiafridman@gmail.com
ORCID ID 0000-0003-1154-8170;
П. Ю. Кравчук,
кандидат юридичних наук, доцент,
декан юридичного факультету,
ПВНЗ «Європейський університет»
email: petro.kravchuk@e-u.edu.ua
ORCID ID 0000-0003-4246-974X

ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Стаття присвячена питанням визначення й аналізу дослідження електронних документів. На актуальність обраної теми впливають як швидкий розвиток технологій, так і складність у протидії та запобіганні злочинності в цій сфері, що обумовлюється технічними особливостями таких процесів, а це зі свого боку сприяє збільшенню правопорушень з використанням електронних документів.

Проведення огляду електронних документів і дослідження їх змісту здійснюється залежно від їх носіїв: фізичних, які можна вилучити; публікацій у мережі «Інтернет» (облікових записів) і на віддалених інтернет-серверах. Дослідження електронних документів здійснюється відповідно до експертиз, які розроблені для дослідження документів і речових доказів. Зазвичай електронні документи досліджують у процесі проведення таких експертиз: семантико-текстуальної, лінгвістичної, фототехнічної, портретної, комп'ютерно-технічної тощо. На якість проведення експертизи впливають спосіб вилучення, пакування та зберігання об'єктів (технічних носіїв інформації), які надані на дослідження. Відсутність єдиних правил дослідження, потрібних технічних засобів та інструментарію спричиняє труднощі під час призначення та проведення експертиз.

Ключові слова: *електронні документи, електронні докази.*

Постановка проблеми та її актуальність. Зростаюча глобалізація та розвиток сучасних технологій приводить до того, що електронні документи можуть бути розміщені або збережені будь-де. Особливо це стосується випадків кіберзлочинності, оскільки кіберзлочинність є проблемою транскордонного співробітництва. Однак усе частіше електронні документи стосуються усіх видів кримінальних правопорушень. Отже, недостатньо повідомити, що електронні документи мають значення лише у провадженнях про кіберзлочини.

Правильне збирання, зберігання та аналіз цих доказів є досить важливими. Будь-яке порушення процедур може призвести до спотворення доказів і, як наслідок, до неправильних рішень, тому дослідники та правоохоронці повинні дотримуватися чітких стандартів, щоб гарантувати допустимість електронних доказів у суді.

Аналіз останніх досліджень і публікацій. Дослідження електронних документів опрацьовували науковці, як-от: Є. П. Бєгалов, Р. І. Благута, С. Й. Гонгало, А. В. Коваленко, А. В. Мовчан, О. А. Самойленко, О. В. Сіренко та інші.

Мета статті полягає у визначенні основних засад використання та дослідження електронних документів під час кримінального провадження.

Виклад основного матеріалу дослідження. Електронні докази щороку набувають усе більшої актуальності та здатні відкривати нові горизонти в розслідуванні й вимагають особливої обережності та професіоналізму.

У більшості випадків під час дослідження електронних документів у кримінальному провадженні слідчий, дізнавач, прокурор повинні залучати спеціаліста чи експерта. Це пов'язано із можливою відсутністю навичок роботи з окремими видами електронних документів і можливістю легкої зміни або знищення важливої інформації, відсутністю сучасного технічного обладнання та ліцензійного програмного забезпечення для роботи з електронними документами.

Зазвичай участь спеціаліста закінчується після виготовлення копії електронного документа. Слідчий або дізнавач здійснює огляд електронного документа самостійно. Проте, якщо існують сумніви в достовірності електронного документа, пошкоджений технічний носій інформації, наявні інші неполадки роботи пристрою, складно віднайти відомості, які становлять інтерес (вони приховані або зашифровані) чи існують інші випадки, коли є потреба в спеціальних знаннях, варто призначати проведення експертизи електронних документів.

З урахуванням існуючих джерел доказів і відсутності окремого виду досліджень електронних документів вони можуть досліджуватись як документ або як речовий доказ.

Призначення та проведення експертизи електронних документів здійснюється на підставі Закону України «Про судову експертизу» й Інструкції про призначення та проведення судових експертиз і експертних досліджень, затвердженої наказом Міністерства юстиції України від 08.10.1998 № 53/5.

На сьогодні відсутній такий вид експертного дослідження, як експертиза електронних документів. Фактично у віртуальному середовищі досліджуємо не сам документ, а файл як носій цього документа. В іншій формі документ не може існувати в електронному (віртуальному) середовищі. Файл – досі ще єдина форма існування електронного документа, що дозволяє його створювати, зберігати, проводити пошук та ідентифікувати. Саме спільність об'єктів, а в окремих випадках і предмета дослідження, пояснює такий характер дослідження [1, с. 47].

Унаслідок учинення злочинів у кіберпросторі утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди, що потребує проведення в таких справах широкого спектра судових експертиз, а саме:

– експертизи комп'ютерної техніки та програмних продуктів;
– експертизи телекомунікаційних систем (обладнання) й засобів;
– технічної експертизи документів;
– експертизи відеозвукозапису;
– експертизи у сфері інтелектуальної власності;
– інших видів експертиз, без проведення яких неможливо отримати потрібні відомості, що свідчать про ознаки складу одного зі злочинів злочинної сукупності, судово-балістичних, судово-хімічних експертиз тощо [2, с. 54].

Під час дослідження електронних документів може проводитися семантико-текстуальна експертиза. Вказану експертизу доцільно призначати для дослідження інформації, наявної у відповідних групах соціальних мереж, повідомлень, в яких містяться заклики, наприклад, до участі у масових заворушеннях, терористичних актах тощо [1, с. 49]. Крім того, така експертиза може проводитись для виявлення ознак погроз і шантажу, примушування до вчинення кримінальних правопорушень та ін.

Також може проводитись лінгвістична експертиза усного мовлення, яка потрібна для ідентифікації особи, голос якої наявний на відео- чи фонограмі, встановлення мовних особливостей і визначення типу висловлювань.

Об'єктами такого дослідження можуть бути голосові повідомлення, записані та відправлені електронною поштою або за допомогою соціальних мереж, відео-, аудіозаписи тощо. Якщо потрібно встановити, чи належить голос на записі певній особі, варто надати, крім досліджуваного запису, зразок запису голосу особи.

Однією з видів експертиз, якою може досліджуватись електронний документ, є фототехнічна експертиза. Об'єктом такого дослідження є цифрові фотографії – оригінали та копії, покадрові зображення відеозапису. Уксперти проводять аналіз з метою встановлення автентичності зображень, вивчаючи метадані, як-от час і місце їх створення, а також можливі маніпуляції із зображеннями (ознаки монтажу), встановлення розмірів на зображеннях та їх порівняння, можливе покращення якості зображення, а також встановлення пристрою, за допомогою якого було воно створено, й інших ідентифікаційних ознак.

Комп'ютерно-технічна експертиза може призначатись для виявлення інформації, яка міститься на комп'ютерних носіях. Так, наприклад, в організаторів незаконного переправлення осіб через державний кордон може вилучатися комп'ютерна техніка, мобільні телефони тощо. У безпосередніх виконавців, відповідно, мобільні телефони, GPS-навігатори, відеореєстратори тощо [3, с. 189–190]. Аналогічно це можуть бути технічні пристрої, які вилучені під час проведення досудового розслідування всіх інших видів кримінальних правопорушень: проти життя та здоров'я, власності, незаконного обігу наркотичних засобів і прекурсорів тощо.

Комп'ютерна експертиза досліджує значну кількість різноманітних цифрових пристроїв і джерел даних. У дослідженнях можуть використовуватися як програмні, так і апаратні засоби. Так, Національна поліція України в своїй роботі використовує програмно-апаратний комплекс «Cellebrite UFED TOUCH 2 Ultimate» [4, с. 125–126], який може використовуватись у межах оперативно-розшукових справ і кримінальних проваджень, зокрема в процесі огляду мобільних пристроїв та/або SIM-карт. За результатом такого огляду формується електронний звіт, який підписується алгоритмом хешування, записується на носій електронної інформації та додається до протоколу як додаток.

Якщо раніше слідчі або оперативні працівники задовольнялися даними з телефонної книги, SMS, MMS, викликами, графічними та відеофайлами, то нині фахівців просять «витягти» більшу кількість даних, зокрема: дані з програм обміну повідомленнями, з електронної пошти, історію відвідування ресурсів мережі «Інтернет», дані про геолокацію, видалені файли й іншу видалену інформацію тощо. Усі ці відомості можна витягти такими спеціальними програмними забезпеченнями, як «Мобільний криміналіст», «Magnet AXIOM», «Magnet Forensics» і «Belkasoft Evidence Center» [4, с. 127–129].

Смартфони є сховищем значної кількості інформації, яка може вплинути на результати розслідування. Під час експертного дослідження телефонних пристроїв доцільним є підключення до точок WI-FI, геолокаційних даних, дослідження історії листувань, роботи в мережі «Інтернет», інформації із соціальних мереж, месенджерів та інших додатків.

За допомогою судової комп'ютерно-технічної експертизи електронних документів можливе вирішення таких завдань: відтворення та роздрук усієї або частини інформації, яка міститься на фізичних носіях, зокрема і в нетекстовій формі; відновлення інформації, що раніше містилась на фізичних носіях і в подальшому була стерта або змінена з різних причин; встановлення часу введення, зміни, знищення чи копіювання певної інформації; розшифрування закодованої інформації, підбір паролів і відкриття системи захисту інформації; встановлення авторства, місця, засобів підготовки та способу виготовлення документів (файлів, програм). Аналогічні завдання розв'язуються в ході інформаційно-комп'ютерної експертизи.

Належність електронного документа є його властивістю, яка полягає в можливості встановлювати чи спростовувати обставини й факти, які підлягають доказуванню. Електронні документи можуть встановлювати подію кримінального правопорушення, винуватість особи, форму вини та мотив правопорушника, вартість завданої шкоди або мати допоміжне значення для складання версій, їх перевірки, встановлення можливих місць вчинення злочину та можливих учасників тощо.

Для визнання електронних документів допустимими варто здійснити перевірку сукупності таких умов, як: належний суб'єкт, належний спосіб, належне джерело, належна форма фіксації. Сторона обвинувачення здійснює збирання електронних документів лише в законодавчо закріплений спосіб, натомість законодавець допускає можливість порушення способу чи форми закріплення електронних документів стороною захисту, потерпілим чи його представником, які не завжди впливають на їх допустимість. Для визнання допустимими електронних документів, доступ до технічного носія яких неможливо отримати (віддалений сервер), було б доречним внести відповідні зміни до Кримінального процесуального кодексу України.

Достовірність електронних документів полягає у відображенні в них фактів об'єктивної дійсності, які мають значення для кримінального провадження. Встановлення достовірності електронних документів є завжди суб'єктивною оцінкою особи, яка її здійснює, що проводиться за допомогою їх зіставлення з іншими доказами в кримінальному провадженні, які стосуються одного і того самого факту, який доказується.

Співробітниками Дніпропетровського НДЕКЦ МВС України розроблено Інформаційний лист щодо особливостей призначення та проведення судових експертиз за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів». В Інформаційному листі зазначено, що об'єктами комп'ютерно-технічного дослідження є будь-які комп'ютерні носії інформації, флеш-накопичувачі, лазерні диски, сервери, системні блоки персональних комп'ютерів, портативні комп'ютери, планшетні комп'ютери, термінали мобільного зв'язку (комунікатори, мобільні телефони, smart-годиники, смартфони), відеореєстратори тощо.

До таких об'єктів застосовуються певні вимоги. Насамперед на дослідження потрібно надати сам носій інформації та у більшості випадків весь апаратно-технічний комплекс, у складі якого перебував носій інформації. Усі предмети дослідження обов'язково повинні бути окремо упаковані з унеможливленням доступу до них, увімкненні чи підключенні до мережі живлення або інтернет-мережі. Якщо потрібно встановити відповідність програмних продуктів певним параметрам, то на дослідження надається носій із копією досліджуваного програмного продукту чи програмного коду та технічна документація до них (технічне завдання, інструкція встановлення, налаштування, користувача тощо). Усі об'єкти дослідження надають разом з блоками живлення, а також, у разі потреби, з інформацією про паролі доступу (кодами доступу до панелі адміністрування), даними графічних ключів, цифрових PIN-кодів або із зазначенням у постанові ініціатора (ухвалі суду) даних про їх відсутність у розпорядженні досудового слідства.

Перелік питань, який може бути поставлений перед експертом, не є вичерпним. Перед призначенням судової експертизи варто обов'язково проконсультуватися з експертом (спеціалістом) із проведення комп'ютерно-технічних досліджень [5].

Електронні документи можуть досліджуватись за допомогою проведення семантико-текстуальної експертизи, лінгвістичної, фототехнічної, портретної, комп'ютерно-технічної та інших видів експертиз. Наразі залишається неврегульованим питання дослідження електронних документів на усіх стадіях кримінального провадження, оскільки відсутні чіткі правила такого дослідження, інструментарій, технічні засоби та кадри.

Збирання електронних документів умовно можна поділити на два етапи: отримання доступу чи вилучення фізичного носія інформації та дослідження й аналіз його змісту. Це пов'язано з тим, що способи отримання фізичного носія інформації регламентовані в Кримінальному процесуальному кодексі України щодо «традиційних доказів», натомість візуалізація та відображення електронного документа у формі, яка може бути сприйнята людиною, потребує використання технічних пристроїв, спеціального програмного забезпечення та залученням спеціаліста. Відтак можемо отримати електронний документ у формі оригіналу чи копії.

До способів збирання електронних документів стороною обвинувачення відносимо: отримання його від особи, яка надає добровільно; витребування й отримання речей, документів тощо; проведення слідчих (розшукових) дій (огляд, обшук); проведення негласних слідчих (розшукових) дій. На окрему увагу заслуговує тимчасовий доступ до речей і документів як захід для забезпечення дієвості кримінального провадження з метою встановлення (пошуку) фактичних даних, які надалі через проведення слідчих (розшукових) дій (наприклад, огляд) будуть оформлені як доказ.

Вважаємо, що добровільна видача повинна здійснюватись одночасно із поданням клопотання про долучення доказів, а форма, зміст, строк розгляду вимоги про витребування документів і речових доказів варто закріпити, відповідно, у Кримінальному процесуальному кодексі України.

Проведення тимчасового доступу до електронних документів є заходом забезпечення кримінального провадження, який проводиться у випадках, коли відомі точні відомості про електронний документ або такі відомості містять охоронювану законом таємницю.

Для отримання доступу до приватної інформації, яка міститься на технічному пристрої, варто зазначати про таку потребу в разі підготовки клопотання про проведення обшуку.

Проведення огляду електронних документів і дослідження їх змісту здійснюється залежно від їх носіїв: фізичних, які можна вилучити; публікацій у мережі «Інтернет» (облікових записів) і на віддалених інтернет-серверах. Зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем є основними негласними слідчими (розшуковими) діями, за допомогою яких здійснюється збирання електронних документів.

Висновки. У сучасному світі щодня зростає кількість електронних документів, які охоплюють наше життя в усіх сферах. Вони зберігають значну кількість інформації про наші дії та зв'язки і можуть стати важливими доказами під час кримінального провадження. Тому дослідження електронних документів та електронних доказів стає актуальним завданням для правоохоронних органів в Україні.

Однією з основних переваг електронних документів є їх можливість зберігатися в незміненому вигляді та бути легкодоступними для експертного дослідження. Це робить їх надійними доказами в судовому процесі. Крім того, електронні докази можуть виявити важливі зв'язки між підозрюваними та іншими особами, які можуть бути використані для розкриття злочинів, а національне законодавство повинно бути відповідним до сучасних вимог щодо захисту електронних даних і доказів.

Перспективи розвитку українського законодавства щодо умов використання електронних документів як доказів у кримінальному провадженні є актуальною тематикою сьогодення, де використання цифрових технологій стає все більш поширеним. З урахуванням швидкого розвитку інформаційних технологій, де багато доказів зберігаються в електронній формі, важливо розглядати можливості використання електронних документів як доказів у кримінальних провадженнях в Україні. Нині українське законодавство швидко адаптується до цифрової епохи, зокрема визнає правомірність використання електронних документів як доказів у судових процесах. Проте існують певні виклики й перешкоди, які потрібно вирішувати для ефективного використання електронних документів як доказів у кримінальному провадженні.

Одним із основних аспектів розвитку українського законодавства є створення надійних систем зберігання та підтвердження електронних доказів. Важливо враховувати захист особистої інформації, запобігати можливості її підробки та забезпечувати конфіденційність даних. Для цього потрібно розробляти спеціалізовані програмні засоби й методи захисту електронних документів. Крім того, важливо вдосконалювати законодавство щодо прийняття й оцінки електронних доказів у судових процесах. Варто чітко визначити процедури та вимоги до електронних документів, а також розробити стандарти для їх використання в кримінальних провадженнях. Також важливо забезпечити можливість експертної перевірки електронних доказів і підтвердження їх автентичності.

Отже, перспективи розвитку українського законодавства щодо умов використання електронних документів як доказів у кримінальному провадженні є обіцяними, проте вимагають комплексного підходу й удосконалення законодавства для забезпечення надійності та ефективності використання таких доказів у судових процесах. Важливо враховувати сучасні вимоги та технологічні зміни для забезпечення справедливості й ефективності кримінальної юстиції в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : дис. … канд. юрид. наук : 12.00.09 / Київський національний університет імені Тараса Шевченка. Київ, 2013. 190 с.

2. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса :ТЕС, 2020. 372 с.

3. Бєгалов Є. П. Розслідування незаконного переправлення осіб через державний кордон України : дис. … канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2020. 278 с.

4. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ДУВС, 2020. 256 с.

5. Інформаційний лист щодо особливостей призначення та проведення судових експертиз за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів». Дніпро : Дніпропетровський НДЕКЦ МВС України, 2018. 5 с.

REFERENCES

1. Gongalo C. Y. Forensic technical and forensic expertise of documents: current research possibilities and development perspectives : div. … Ph. D. legal Sciences : 12.00.09 / Kyiv National University named after T. Shevchenko. Kyiv, 2013. 190 p. [in Ukrainian].

2. Samoilenko O. A. New methods of investigation of crimes committed in cyberspace : monograph / in general. ed. A. F. Volobuyeva. Office : TEC, 2020. 372 c. [in Ukrainian].

3. Behalov E. P. Investigation of the illegal transportation of goods across the state border of Ukraine : div. ... Ph. D. legal of science 12.00.09 / National Academy of Internal Law. Kyiv, 2020. 278 p. [in Ukrainian].

4. Blaguta R. I., Movchan A. V. Latest technologies in the investigation of crimes: state of the art and problems of use : monograph. Lviv : DUVC, 2020. 256 p. [in Ukrainian].

5. Information letter regarding the appointment and conduct of forensic expertise in the specialty 10.9 "Investigation of computer equipment and software products". Dnipro: Dnipropetrovsk NDEKC of the Ministry of the Interior of Ukraine. 2018. 5 c. [in Ukrainian].

M. M. Fridman-Kozachenko, P. Yu. Kravchuk. INVESTIGATION OF ELECTRONIC DOCUMENTS

The article is devoted to the issues of definition and analysis of the study of electronic documents. The relevance of the chosen topic is influenced by both the rapid development of technologies and the complexity of combating and preventing crime in this area, which is determined by the technical features of these processes, and this, in turn, contributes to the increase of offenses involving the use of electronic documents.

The review of electronic documents and monitoring of their contents is carried out depending on their notions: physical notions that can be removed; publications on the Internet (account records) and on remote Internet servers. The examination of electronic documents is carried out in accordance with the expertise developed for the examination of documents and physical evidence. Usually, electronic documents are examined during the conduct of such expertises: semantic-textual, linguistic, photo-technical, portrait, computer-technical and other expertises. The quality of the expert examination is affected by the method of extraction, packaging and storage of objects (technical notions of information) provided for examination. The absence of uniform rules of investigation, necessary technical measures and instrumentation causes difficulties during the appointment and conducting of expert examinations.

Keywords: *electronic documents, electronic evidence.*

Стаття надійшла до редакції 19 серпня 2024 року