АКТУАЛЬНІ ПИТАННЯ ЗАПОБІГАННЯ І ПРОТИДІЇ ПРАВОПОРУШЕННЯМ: КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ

УДК 343.141
DOI https://doi.org/10.32782/2078-3566-2025-2-21

Іван БОГАТИРЬОВ
доктор юридичних наук, професор,
професор кафедри кримінально-виконавчого та кримінального права
Навчально-наукового інституту права, правоохоронної діяльності та психології,
заслужений діяч науки і техніки України
(Пенітенціарна академія України, м. Чернігів, Україна)
vanbogatyrov@gmail.com

Інна СМАЛЬ
аспірантка кафедри кримінально-виконавчого та кримінального права
Навчально-наукового інституту права, правоохоронної діяльності та психології
(Пенітенціарна академія України, м. Чернігів, Україна)

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ: АКТУАЛЬНА ПРОБЛЕМА СЬОГОДЕННЯ

Статтю присвячено комплексному аналізу особливостей використання електронних документів у кримінальному процесі України, оскільки сьогодні кримінальне провадження не може обійтися без електронних доказів, що зумовлено розвитком інноваційних технологій та впровадженням їх у різних сферах суспільної діяльності. У центрі уваги – розмежування понять «електронний документ» та «електронний доказ», яке має ключове значення для належного збирання, дослідження та оцінки інформації в електронному вигляді. Обґрунтовано необхідність законодавчого визначення як електронних доказів узагалі, так і електронного документа як одного з їхніх різновидів зокрема. У межах дослідження розглянуто сучасні технологічні засоби, що використовуються для гарантування цілісності та автентичності електронних доказів, зокрема клітка Фарадея, апаратне шифрування даних, система контролю ланцюга збереження, технології електронного підпису та офлайн-сховища. Зроблено висновок, що впровадження надійних механізмів контролю та захисту не лише сприяє збереженню інформації в електронному вигляді, а й відповідає вимогам належного поводження з доказами в умовах цифрового середовища. Сформульовано авторське визначення поняття електронного документа. Електронний документ – це вид електронного доказу, що має зафіксовану інформацію в електронній формі, створений, збережений або переданий із використанням електронних засобів, який містить обов'язкові реквізити, зокрема електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Ключові слова: *кримінальне правопорушення, використання, електронний документ, кримінальний процес, провадження, розслідування, електронний доказ, ідентифікація.*

ORCID ID: https://orcid.org/0000-0003-4001-7256

ORCID ID: https://orcid.org/0000-0003-1747-7342

Постановка проблеми. Українська наука кримінального процесуального права єдина в тому, що електронні документи відіграють роль як у механізмах учинення кримінальних правопорушень і приховування їхніх слідів, так і в процесі збирання, фіксації та дослідження доказової інформації, яка має значення у кримінальному провадженні.

Звичайно, порядок використання електронних документів та їхній статус у кримінальному процесуальному праві України повинні бути детально врегульовані національним законодавством України. Поряд із цим, за нашим дослідженням, таке врегулювання не відповідає сучасній академічній доктрині права, а тому потребує виокремлення в ній наявних прогалин у використанні електронних документів у процесі розслідування кримінального провадження.

Метою статті є окреслення ключових підходів до використання електронних документів у процесі доказування, виявлення прогалин та недоліків у нормативному регулюванні електронних доказів та надання відповідних пропозицій щодо його вдосконалення.

Аналіз публікацій, у яких започатковано вирішення цієї проблеми. Проблеми використання електронних документів у кримінальних провадженнях досліджувалися низкою науковців, серед яких: А.П. Запотоцький, С.О. Ковальчук, Д.М. Цехан, Ю.Ю. Орлов, С.С. Чернявський, О.П. Метелев, Н.М. Ахтирська, А.В. Столітній, О.В. Сіренко, М.В. Гуцалюк, В.Г. Гавловський, Д.О. Алєксєєва-Процюк, О.М. Брисковська, С.М. Стахівський, С.Й. Гонгало, Є.Г. Коваленко, О.В. Шведова, С.А. Крушинський, А.В. Ратнова, В.В. Білоус, О.С. Степанов, М.М. Стоянов, А.В. Коваленко, В.В. Лисенко, Б.В. Шабаровський, Г.К. Авдєєва, В.В. Марков, Р.Р. Савченко, А.В. Шевчишин, М.В. Дєєв, В.С. Сезонов, А.В. Піддубна, Д.Б. Сергєєва, Т.М. Мирошниченко, С.О. Шульгін, І.А. Смаль та ін.

Відсутність єдності серед сучасних учених-процесуалістів у розумінні поняття електронного документа та порядку його використання у кримінальних провадженнях засвідчує наукову й практичну актуальність вибраної тему дослідження.

Виклад основного матеріалу. Ураховуючи предмет нашого дослідження, зауважимо, що електронними документами в кримінальному провадженні, по суті, є ті відомості, що зафіксовані в електронній формі, які можуть розглядатися як різновид документа або речового доказу та підлягають доказуванню у межах кримінального провадження. Однак такі документи мають специфічні технічні особливості, зокрема вони підлягають ризику втрати цілісності, достовірності та автентичності через можливість несанкціонованого втручання, технічні збої або порушення у процесі їх зберігання.

Звичайно, за нашим дослідженням, утручання можуть мати різний характер, зокрема: несанкціоноване змінення вмісту файлів або баз даних, видалення або приховування інформації, підробка метаданих (часу створення, авторства тощо), технічні несправності носіїв інформації, вірусні атаки чи недотримання процедур безпеки під час зберігання та передачі доказів. Кожен із зазначених випадків може поставити під сумнів автентичність та доказову силу електронного документа, що ускладню можливість використання його як доказу.

З огляду на це, надзвичайно важливим є впровадження надійних механізмів контролю цілісності та автентичності електронних доказів, а також забезпечення безперервності ланцюга зберігання та передачі інформації в електронному вигляді. Ураховуючи, що в сучасних умовах зміни електронних даних можуть бути здійсненні навіть дистанційно, наприклад через радіочастотні сигнали, для захисту доказів застосовуються спеціалізовані технічні засоби, зокрема такі, як екранування носіїв інформації у клітках Фарадея, які блокують зовнішні електромагнітні впливи.

У процесі дослідження нами враховано також наукові напрацювання у суміжних галузях знань, зокрема в галузі технічних наук. Так, професор, доктор технічних наук В.М. Ахрамович досліджував питання захисту електронних даних на різних стадіях їх функціонування, зокрема акцентуючи увагу на методах зберігання інформації у стані спокою [1, с. 151].

Зазначені положення мають особливу прикладну значущість для кримінального процесу, оскільки належне технічне забезпечення збереження електронних даних на стадії спокою є важливим чинником у забезпеченні можливості подальшого використання відповідної інформації як електронного доказу. Такий міждисциплінарний підхід дає змогу враховувати технічні засоби забезпечення цілісності, автентичності та достовірності електронної інформації, що у подальшому впливає на відповідність електронних доказів вимогам належності, допустимості та достовірності у кримінальному провадженні.

У процесі аналізу наукової літератури та рекомендацій міжнародних організацій, зокрема ISO/IEC 27037:2012, та досліджень провідних фахівців у сфері цифрової криміналістики, зокрема, E. Casey, нами було систематизовано перелік сучасних технологічних засобів, які використовуються для забезпечення цілісності та автентичності електронних доказів.

До таких засобів належать:

– клітка Фарадея, що застосовується для ізоляції електронних пристроїв від зовнішніх сигналів. Це особливо важливо під час вилучення мобільних пристроїв, які можуть бути піддані віддаленому знищенню або зміні інформації [15; 16, с. 6];

– апаратне шифрування даних, що надає можливість захистити інформацію безпосередньо під час її запису на носій. Пристрої апаратного шифрування (Hardware Encryption Devices) дають змогу здійснити шифрування даних на етапі запису на носій та розшифрування під час зчитування, що дає можливість захистити інформацію від стороннього доступу. Так, у книзі Еогана Кейсі «Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet», зокрема в 4-му та 9-му розділах, детально розглядаються такі методи збереження та захисту інформації в електронному вигляді, зокрема на стадії її зберігання. Також ідеться про застосування хеш-функцій для забезпечення цілісності електронних даних [14];

– система контролю ланцюга збереження, яка дає змогу фіксувати кожен етап взаємодії з електронними доказами [17];

– технології електронного підпису, які забезпечують перевірку автентичності походження електронних документів, а також фіксацію дати та часу їх створення [10];

– офлайн-сховища, що унеможливлюють доступ до носіїв інформації в електронному вигляді [1, с. 153].

Застосування зазначених засобів не лише сприяє збереженню інформації в електронному вигляді, а й відповідає вимогам належного поводження з доказами в умовах цифрового середовища.

У процесі дослідження нами враховано той факт, що загальне визначення електронних документів усе ж таки міститься у Законі України «Про електронні документи та електронний документообіг». Так, відповідно до ст. 5 цього Закону, електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [10].

Утім, на нашу думку, таке визначення електронного документа відображає лише загальне правове розуміння електронного документа як об'єкта правового захисту, але не містить суттєвих характеристик, які визначають його роль та ознаки як доказового елемента в кримінальному провадженні. Для використання електронного документа як доказу у кримінальному процесі необхідно враховувати додаткові критерії, які встановлено кримінальним процесуальним законодавством і спрямовані на підтвердження достовірності, цілісності, автентичності та відповідності вимогам кримінального судочинства.

Про це зазначають і науковці Л.Г. Остапчук та І.А. Смаль, які наголошують, що не будь-який електронний документ може бути доказом у кримінальному процесі. По-перше, електронний документ повинен містити в собі інформацію (відомості), які встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального прова-

дження та підлягають доказуванню. По-друге, він повинен містити в собі інформацію, яка зберігається на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (у тому числі в мережі Інтернет), що дає можливість доступу до такої інформації в будь-який момент. По-третє, електронний документ повинен бути отриманий із дотриманням процесуальних правил збирання доказів [8, с. 124].

У цьому контексті ми також підтримуємо позицію А.С. Запотоцького про те, що «електронні документи» з'являються у кримінальному провадженні, так би мовити, у «готовому вигляді», а Кримінальний процесуальний кодекс лише регламентує порядок їх збирання та дослідження, але не порядок складання, тоді як форма, обов'язкові реквізити та порядок складання протоколів за результатами слідчих (розшукових) дій із метою дотримання достовірності доказів регламентовано у КПК України. Протоколи є завжди письмовими документами, які складені згідно з вимогами КПК України, тоді як електронні документи мають іншу форму [3, с. 9].

Натомість у подальшому глибшому науковому осмисленні ми дійшли висновку, що для кримінального процесу необхідно враховувати специфіку електронного документа, серед яких – наявність обов'язкових реквізитів, що відрізняють його від інших видів електронних доказів і визначають його юридичну значущість. Таким чином, електронний документ слід розглядати як окремий вид електронних доказів із відповідними критеріями автентичності, достовірності та цілісності.

Своєю чергою, С.О. Ковальчук відзначив, що зміст електронних доказів становлять фактичні дані, на підставі яких можуть бути встановлені факти й обставини, що мають значення для кримінального провадження і підлягають доказуванню, та які існують в електронно-цифровій формі. До таких доказів можуть належати шкідливі програми, віруси, програми, які були об'єктом протиправних дій, комп'ютерні сліди, кошти та інші цінності в електронній формі, електронні документи та ін. Такі докази створено та існують об'єктивно незалежно від волі правоохоронних органів та суду, містять доказову інформацію та не містять ознак предметності [4, с. 121–122].

Натомість Ю.Ю. Орлов та С.С. Чернявський пропонують законодавчо визначити самостійним джерелом доказів електронні відображення – цілісну систему відомостей та (або) комп'ютерних інструкцій в інформаційній мережі або на технічному носії, яка може бути використана як доказ факту чи обставин, що встановлюються під час кримінального провадження. Ба більше, учені переконані, і ми їх підтримуємо, що «електронний документ» може не мати автора [7, с. 21].

Така позиція українських учених кореспондується з тим, що електронні докази у цифровому середовищі можуть бути сформовані не лише людиною, а й безпосередньо інформаційною системою (наприклад, трафіки з'єднань абонентів мобільного зв'язку, динамічні бази банківських проводок, білінгові системи, log-файли тощо).

Цікавою для нашого дослідження є також думка українського ученого О.П. Метелева, який зазначає, що основними причинами виділення цифрової інформації, зафіксованої на машинних носіях як самостійного і специфічного джерела відомостей, котрі не входять ані до складу речових доказів, ані до складу документів, є її особлива нематеріальна природа, природно-технічні особливості її створення, обробки, зберігання, передачі в часі й просторі, а також кримінально-процесуальні процедури і техніко-криміналістичні прийоми її пошуку та вилучення, доступу до неї, дослідження та перетворення її на форму, яку сприйматиме людина. У такому разі необхідно оцінювати власне інформацію, а не матеріальний об'єкт, на якому вона зафіксована [6, с. 102–103].

Отже, суттєве значення під час дослідження електронних документів у кримінальному провадженні має розуміння їх двоїстої природи. З одного боку, електронний документ – це інформація, яка має змістовне значення та може підтверджувати або спросто-

вувати обставини, що підлягають доказуванню. З іншого боку, ця інформація невід'ємно пов'язана з матеріальним носієм, на якому вона зберігається (флеш-накопичувач, жорсткий диск, хмарне середовище, сервер тощо).

На наше переконання, така подвійність зумовлює важливість технічного аспекту забезпечення збереження інформації в електронному вигляді, але як доказ оцінюється не сам носій, а зафіксована на ньому інформація в електронному вигляді.

Своєю чергою, Н.М. Ахтирська висловлює думку, що документи на технічних носіях інформації за змістом і зв'язком із кримінальним правопорушенням, можуть бути поділені на речові докази та документи. Перші – це докази використання ІТ під час вчинення «комп'ютерних» правопорушень. Сюди відносять програми зі слідами зміни команд або введення непередбачених команд, створення умов автозаміни програми, несанкціонованої зміни алгоритму і т. д. Другі – носії інформації про обставини, які мають значення для кримінального провадження, котрі в принципі не надто відрізняються від паперових документів – носіїв інформації [2, с. 123].

Ми також погоджуємося з позицією українського дослідника О.В. Сіренко про те, що електронні документи як докази в кримінальному провадженні крізь призму певних обставини можуть існувати у нематеріальному вигляді в межах технічного носія чи каналу зв'язку та сприйняття і дослідження яких можливе за допомогою технічних засобів і програмного забезпечення [11, с. 211].

У процесі розслідування кримінальних правопорушень як на стадії досудового розслідування, так і під час судового розгляду велике значення має правильне розуміння, чи є допустимими як докази матеріали НСРД. Як зазначають українські вчені С.Р. Тагієв, М.С. Пузирьов, С.В. Івашко, «у судах склалася практика про визнання допустимими як докази матеріали НСРД, де були залучені особи без попереднього надання допуску до державної таємниці. Хоча, на нашу думку, під час дослідження доказів, отриманих у результаті НСРД із залученням осіб до конфіденційного співробітництва, повинна бути чітка позиція з посилання на норму Закону України «Про державну таємницю», а не тлумачення законодавчого акта» [13, с. 456].

Варто підтримати таку позицію учених, оскільки матеріали НСРД є визначальним для забезпечення їх належного збирання, фіксації, дослідження та подальшої оцінки щодо допустимості, достовірності та достатності під час прийняття процесуальних рішень.

Оскільки предметом нашого дослідження є електронний документ, доцільно наголосити, що електронний документ є одним із видів електронних доказів, який відзначається специфічними ознаками, зокрема вимогами щодо наявності обов'язкових реквізитів, таких як кваліфікований електронний підпис, тоді як інші електронні докази (наприклад, мультимедійні файли, метадані, інформація з камер спостереження, листування у месенджерах) не мають таку формалізовану структуру.

Варто наголосити, що в КПК України, а саме в ч. 3 ст. 99, зазначено, що оригіналом електронного документа є його відображення, якому надається таке ж значення, як документу [5], однак це положення не розкриває правової природи електронного документа, не розмежовуючи його з ширшим за обсягом поняттям електронного доказу. Відсутність чіткого розмежування в кримінальному процесуальному законодавстві призводить до неоднозначного застосування зазначених понять у правозастосовній практиці.

Так, у процесуальних документах та судових рішеннях для позначення одного і того ж об'єкта можуть використовувати різні терміни, що створює плутанину, правову невизначеність і може впливати на оцінку допустимості такого доказу. Як приклад можна навести Постанову ККС ВС від 06.02.2024, справа № 645/6247/16-к, у якій суд для позначення інформації в електронному вигляді як доказ використовує як поняття електронного доказу, надаючи йому визначення, так і поняття електронного документа з огляду на положення Закону України «Про електронні документи та електронний документообіг» [9].

Ми поділяємо позицію дослідниці щодо доцільності законодавчого закріплення положення про електронні докази в окремій главі КПК України [12, с. 231] і, розвиваючи зазначений підхід, уважаємо за доцільне на рівні кримінального процесуального законодавства не лише законодавчо визначити поняття електронних доказів, а й окремо закріпити дефініцію електронного документа як одного з видів такого доказу. Виникає цілком логічне запитання: чому розмежування понять електронного доказу та електронного документа є настільки важливим саме для кримінального процесу? Даючи відповідь на це запитання, зазначимо, що інформація в електронному вигляді може мати різну природу, і від цього залежать спосіб її збирання, рівень вимоги до автентичності, допустимість доказу, методика технічної експертизи.

Висновки. З огляду на результати проведеного дослідження, можна дійти висновку, що чинне кримінальне процесуальне законодавство України не містить визначення електронного документа як окремої категорії доказів, хоча в теорії кримінального процесу вже напрацьовано значну кількість доктринальних підходів до цього поняття. Така прогалина призводить до неоднакового правозастосування, змішування понять електронного документа та електронного доказу, а також ускладнює забезпечення дотримання вимог щодо цілісності, автентичності інформації в електронному вигляді у кримінальному провадженні.

У зв'язку із цим вважаємо за доцільне законодавче розмежування цих понять. Зокрема, пропонується в окремій главі КПК України закріпити визначення електронного доказу як процесуального джерела інформації в електронному вигляді; виокремити електронний документ як один із видів електронних доказів, а також запропонувати авторське визначення поняття електронного документа: електронний документ – це вид електронного доказу, що має зафіксовану інформацію в електронній формі, створений, збережений або переданий із використанням електронних засобів, який містить обов'язкові реквізити, зокрема електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Список використаних джерел

1. Ахрамович В. М. Захист даних на стадіях їх функціонування. *Кібербезпека: освіта, наука, техніка.* 2023. № 1(21). С. 149–161.

2. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2016. Вип. 36(2). С. 123–125.

3. Запотоцький А. П. Документи як процесуальні джерела доказів у кримінальному судочинстві : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 26 с.

4. Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : дис. ... д-ра юрид. наук : 12.00.09. Одеса, 2018. 626 с.

5. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

6. Метелев О. П. Цифрові докази як окремий вид доказів у кримінальному процесі. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення.* 2018. Вип. 10. С. 100–104.

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

8. Остапчук Л. Г., Смаль І. А. До питання правової природи електронного документу та його місця у системі доказів кримінального процесу. *Прикарпатський юридичний вісник*. 2022. Вип. 2. С. 122–127.

9. Постанова Касаційного кримінального суду Верховного Суду у справі № 645/6247/16-к від 06 лютого 2024 р. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/116862907

10. Про електронні документи та електронний документообіг : Закон України від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

11. Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2019. Вип. 14. С. 208–212.

12. Смаль І. А. Проблемні аспекти застосування електронних доказів у кримінальному судочинстві. *Право і суспільство*. 2021. № 4. С. 226–232.

13. Тагієв С. Р., Пузирьов М. С., Івашко С. В. Негласні слідчі (розшукові) дії в умовах війни: окремі теоретичні та практичні аспекти (частина ІІ). *Аналітично-порівняльне правознавство.* 2023. № 2. С. 454–459.

14. Casey E. Digital Evidence and Computer Crime. London : Academic Press, 2000. 780 p.

15. Faraday Bags Are the First Step in Preserving Digital Evidence. *MOSEquipment.* 2023. URL: https://mosequipment.com/blogs/blog/faraday-bags-are-the-first-step-in-preserving-digital-evidence?srsltid=AfmBOoq-5HQMprb1yk-CKfp4ZdiAsyXZNhFEqS6D2ErmrCGQU_HCyvoS

16. Horsman G., Hale R., Firman A. A First Responder Guide to Handling and Seizing Mobile Phones. *SSRN.* 4 Nov 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5007997

17. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva : ISO copyright office, 2012. 38 p.

Надійшла до редакції 23.05.2025

References

1. Akhramovych, V. M. (2023) Zakhyst danykh na stadiiakh yikh funktsionuvannia [Data protection at stages of its functioning]. *Kiberbezpeka: osvita, nauka, tekhnika.* № 1 (21), pp. 149–161. [in Ukr.].

2. Akhtyrska, N. M. (2016) Do pytannia dokazovoi syly kiberinformatsii v aspekti mizhnarodnoho spivrobitnytstva pid chas kryminalnoho provadzhennia [On the probative value of cyber information in the context of international cooperation during criminal proceedings]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Pravo».* Iss. 36 (2), pp. 123–125. [in Ukr.].

3. Zapototskyi, A. P. (2009) Dokumenty yak protsesualni dzherela dokaziv u kryminalnomu sudochynstvi [Documents as procedural sources of evidence in criminal proceedings] : avtoref. dys. ... kand. yuryd. nauk : 12.00.09. Kyiv. 26 p. [in Ukr.].

4. Kovalchuk, S. O. (2018) Vchennia pro rechovi dokazy u kryminalnomu protsesi: teoretyko-pravovi ta praktychni osnovy [Theory of physical evidence in criminal proceedings: theoretical, legal and practical foundations] : dys. ... d-ra yuryd. nauk : 12.00.09 / Natsionalnyi universytet «Odeska yurydychna akademiia». Odesa. 626 p. [in Ukr.].

5. Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine] : Zakon Ukrainy vid 13.04.2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text. [in Ukr.].

6. Metelev, O. P. (2018) Tsyfrovi dokazy yak okremyi vyd dokaziv u kryminalnomu protsesi [Digital evidence as a separate type of evidence in criminal proceedings]. Dosudove rozsliduvannia: aktualni problemy ta shliakhy yikh vyrishennia. Iss. 10, pp.100–104. [in Ukr.].

7. Orlov, Yu. Yu., Cherniavskyi, S. S. (2017) Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni [Electronic representations as a source of evidence in criminal proceedings]. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav.* № 1 (13), pp. 12–24. [in Ukr.].

8. Ostapchuk, L. H., Smal, I. A. (2022) Do pytannia pravovoi pryrody elektronnoho dokumentu ta yoho mistsia u systemi dokaziv kryminalnoho protsesu [On the legal nature of electronic documents and their place in the system of evidence in criminal proceedings]. *Prykarpatskyi yurydychnyi visnyk.* Iss. 2, pp. 122–127. [in Ukr.].

9. Postanova Kasatsiinoho kryminalnoho sudu Verkhovnoho Sudu u spravi № 645/6247/16-k vid 06 liutoho 2024 r. [Resolution of the Cassation Criminal Court of the Supreme Court in case No. 645/6247/16-k dated February 6, 2024]. *Yedynyi derzhavnyi reiestr sudovykh rishen.* URL: https://reyestr.court.gov.ua/Review/116862907. [in Ukr.].

10. Pro elektronni dokumenty ta elektronnyi dokumentoobih [On Electronic Documents and Electronic Document Flow] : Zakon Ukrainy vid 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text. [in Ukr.].

11. Sirenko, O. V. (2019) Elektronni dokazy u kryminalnomu provadzhenni [Electronic evidence in criminal proceedings]. *Mizhnarodnyi yurydychnyi visnyk: aktualni problemy suchasnosti (teoriia ta praktyka)*. Iss. 14, pp. 208–212. [in Ukr.].

12. Smal, I. A. (2021) Problemni aspekty zastosuvannia elektronnykh dokaziv u kryminalnomu sudochynstvi [Problematic aspects of the use of electronic evidence in criminal justice]. *Pravo i suspilstvo.* № 4, pp. 226–232. [in Ukr.].

13. Casey, E. Digital Evidence and Computer Crime. London : Academic Press, 2000. 780 p.

14. Faraday Bags Are the First Step in Preserving Digital Evidence. *MOSEquipment.* квітень 2023. URL: https://mosequipment.com/blogs/blog/faraday-bags-are-the-first-step-in-preserving-digital-evidence?srsltid=AfmBOoq-5HQMprb1yk-CKfp4ZdiAsyXZNhFEqS6D2ErmrCGQU_HCyvoS

15. Horsman, G., Hale, R., Firman, A. (2024) A First Responder Guide to Handling and Seizing Mobile Phones. *SSRN.* 4 Nov. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5007997

16. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva : ISO copyright office, 2012. 38 p.

ABSTRACT

Ivan Bohatyryov, Inna Smal. Use of electronic documents in the criminal process of Ukraine: a pressing issue of today

The article is devoted to a comprehensive analysis of the peculiarities of using electronic documents in the criminal process of Ukraine, as modern criminal proceedings cannot function without electronic evidence. This is due to the development of innovative technologies and their implementation in various spheres of social activity. The focus is on the distinction between the concepts of «electronic document» and «electronic evidence», which is crucial for the proper collection, examination, and evaluation of information in electronic form. The article substantiates the need for legislative definitions of both electronic evidence in general and electronic documents as a specific type of such evidence. The study also examines modern technological tools used to ensure the integrity and authenticity of electronic evidence, including Faraday cages, hardware data encryption, chain-of-custody control systems, electronic signature technologies, and offline storage. It concludes that the implementation of reliable control and protection mechanisms not only helps preserve information in electronic form but also meets the standards of proper evidence handling in a digital environment. The article also proposes an original definition of the term electronic document. «An electronic document is a type of electronic evidence that contains recorded information in electronic form, created, stored, or transmitted using electronic means, and includes mandatory attributes, including the author's electronic signature or a signature equivalent to a handwritten one in accordance with the Law of Ukraine «On Electronic Identification and Electronic Trust Services».

Key words: *criminal offense, use, electronic document, criminal process, proceedings, investigation, electronic evidence, identification.*