

**Цифрові докази у судовому
процесі: документи, метадані,
листування, месенджери,
відео, геолокація, скриншоти,
цифрова експертиза та
практика Верховного Суду**

Науково-практичний посібник є комплексним дослідженням правової природи, процесуального статусу, способів отримання, фіксації, збереження, дослідження та оцінки цифрових доказів у судовому процесі України.

Актуальність дослідження зумовлена стрімкою цифровізацією суспільних відносин і переходом значної частини юридично значущої інформації в електронне середовище. Електронні документи, електронне листування, повідомлення в месенджерах, матеріали соціальних мереж, фотографії, відеота аудіозаписи, дані геолокації, інформація з мобільних пристроїв, вебсторінок, електронних реєстрів та інформаційних систем дедалі частіше використовуються як засоби доказування в цивільному, кримінальному, адміністративному й господарському судочинстві.

Видання розраховане на адвокатів, суддів, прокурорів, слідчих, судових експертів, державних службовців, науковців, викладачів і здобувачів юридичної освіти, а також усіх правників, діяльність яких пов'язана з використанням електронної та цифрової інформації в процесі доказування.

Р. В. Гайворонський

ЦИФРОВІ ДОКАЗИ У СУДОВОМУ ПРОЦЕСІ:

**електронні документи, метадані, листування, месенджери,
відео, геолокація, скриншоти, цифрова експертиза
та практика Верховного Суду**

Науково-практичний посібник

Харків
«Право»
2026

Гайворонський Р. В.

Г15 Цифрові докази у судовому процесі: електронні документи, метадані, листування, месенджери, відео, геолокація, скриншоти, цифрова експертиза та практика Верховного Суду : наук.-практ. посіб. / Р. В. Гайворонський. – Харків : Право, 2026. – 612 с.

ISBN 978-617-8852-30-6

Науково-практичний посібник є комплексним дослідженням правової природи, процесуального статусу, способів отримання, фіксації, збереження, дослідження та оцінки цифрових доказів у судовому процесі України.

Актуальність дослідження зумовлена стрімкою цифровізацією суспільних відносин і переходом значної частини юридично значущої інформації в електронне середовище. Електронні документи, електронне листування, повідомлення в месенджерах, матеріали соціальних мереж, фотографії, відео-та аудіозаписи, дані геолокації, інформація з мобільних пристроїв, вебсторінок, електронних реєстрів та інформаційних систем дедалі частіше використовуються як засоби доказування в цивільному, кримінальному, адміністративному й господарському судочинстві.

Видання розраховане на адвокатів, суддів, прокурорів, слідчих, судових експертів, державних службовців, науковців, викладачів і здобувачів юридичної освіти, а також усіх правників, діяльність яких пов'язана з використанням електронної та цифрової інформації в процесі доказування.

УДК [34.03(477)+343.98]:004

ПЕРЕДМОВА

Цифровізація суспільних відносин докорінно змінила не лише способи комунікації, укладення правочинів, зберігання інформації та здійснення господарської діяльності, а й механізми реалізації та захисту суб'єктивних прав у суді. Інформація, яка ще донедавна існувала переважно у паперовій формі, сьогодні дедалі частіше створюється, передається, зберігається та відтворюється виключно в електронному середовищі. Відповідно, цифрова інформація стала невід'ємним елементом сучасного доказування.

Електронні документи, електронне листування, повідомлення у месенджерах, матеріали соціальних мереж, фотографії, відеозаписи, аудіофайли, дані геолокації, інформація з мобільних пристроїв, метадані, дані електронних інформаційних систем та інші цифрові об'єкти дедалі частіше використовуються учасниками судових проваджень для підтвердження юридично значущих обставин.

Водночас цифровий доказ істотно відрізняється від традиційних засобів доказування. Його існування нерозривно пов'язане з технічним середовищем, у якому він створюється та зберігається. Зміна файлу, його копіювання, конвертація, редагування, видалення метаданих або навіть спосіб вилучення інформації можуть безпосередньо впливати на можливість встановлення її походження, цілісності та достовірності.

Саме тому сучасний правник повинен знати не лише процесуальні норми, що регулюють електронні докази, а й базові принципи їх технічного існування, фіксації, збереження та перевірки.

Проблематика цифрових доказів набуває особливої актуальності у зв'язку з поширенням електронного документообігу, дистанційної роботи, електронних правочинів, соціальних мереж, месенджерів, хмарних технологій, мобільних пристроїв та інших цифрових сервісів. Значний масив юридично значущої інформації сьогодні існує виключно в цифровій формі.

Особливого значення ця проблема набуває в умовах судового спору. Перед адвокатом постає не лише питання про те, чи містить певний електронний файл необхідну інформацію, а й низка інших принципів питань: хто створив цей файл, коли і за яких обставин він був

створений, чи зазнавав він змін, де зберігався його оригінал, яким способом інформація була отримана, чи можливо підтвердити її автентичність та чи відповідає спосіб її подання до суду вимогам процесуального законодавства.

Особливо складними є ситуації, коли доказом виступає електронне листування або повідомлення в месенджері. Сам факт існування скріншота повідомлення ще не завжди дозволяє встановити особу його автора, час створення, повноту контексту спілкування та відсутність технічного втручання. Аналогічні проблеми виникають щодо фотографій, відеозаписів, аудіофайлів, публікацій у соціальних мережах та інформації з вебсторінок.

Окремий напрям становлять метадані. Технічна інформація про час створення файлу, пристрій, за допомогою якого він був створений, географічні координати, характеристики файлу, відомості про його редагування та інші технічні параметри можуть мати істотне значення для встановлення достовірності цифрового доказу. Водночас метадані можуть бути змінені, видалені або втрачені, що потребує особливого підходу до їх дослідження.

Не менш важливим є питання геолокації. Дані GPS, мобільних операторів, навігаційних сервісів та мобільних пристроїв можуть використовуватися для встановлення місцезнаходження особи або пристрою у певний момент часу. Такі відомості можуть мати доказове значення у цивільних, адміністративних, господарських та кримінальних провадженнях, однак їх оцінка потребує врахування способу отримання, точності та технічних особливостей відповідних даних.

Складність цифрового доказування зумовлює також зростання ролі судових експертиз. Комп'ютерно-технічна, телекомунікаційна, експертиза відео-, звукозапису, дослідження електронних документів та інші спеціальні дослідження можуть бути необхідними для встановлення факту створення, зміни, копіювання або видалення цифрової інформації.

Окремим викликом сучасному правосуддю стає поширення технологій штучного інтелекту та deepfake. Цифровий контент сьогодні може бути не просто змінений, а створений штучно таким чином, що його зовнішні характеристики майже не відрізняються від справжнього матеріалу. Це ставить перед судом, сторонами та експертами

принципово нове завдання – визначити не лише зміст доказу, а й достовірність його цифрового походження.

У цьому контексті особливого значення набуває практика Верховного Суду, яка поступово формує критерії оцінки електронних і цифрових доказів. Судова практика дозволяє простежити підходи до визначення належності, допустимості, достовірності та достатності цифрової інформації, а також встановити межі використання скріншотів, електронного листування, електронних документів, матеріалів із соціальних мереж та інших цифрових джерел.

Важливе значення мають також стандарти, сформовані Європейським судом з прав людини щодо справедливості судового провадження, змагальності сторін, рівності процесуальних можливостей, права на повагу до приватного життя та допустимості втручання держави в електронні комунікації.

Це видання має на меті комплексно дослідити цифрові докази як сучасний інструмент судового доказування та сформувати практичний алгоритм роботи з ними.

Автор не обмежується аналізом законодавчих положень. Основний акцент зроблено на практичних питаннях: як правильно виявити цифровий доказ, яким способом його зафіксувати, як забезпечити його збереження, як підтвердити автентичність, коли необхідно залучати експерта, як витребувати інформацію у володільця відповідної інформаційної системи, як заперечувати проти цифрового доказу іншої сторони та яким чином довести його неналежність або недопустимість.

Особливу увагу приділено проблемі так званого «ланцюга збереження» цифрового доказу. Для цифрової інформації принципово важливо не лише те, що саме вона містить, а й те, яким шляхом вона потрапила до суду. Втрата оригіналу, відсутність відомостей про джерело, невстановлений спосіб копіювання, можливість редагування або відсутність технічної інформації можуть поставити під сумнів доказове значення відповідного цифрового об'єкта.

Практична цінність видання полягає також у систематизації типових процесуальних помилок. У багатьох випадках сторона спору має юридично значущу цифрову інформацію, але не може належним чином використати її в суді через неправильну фіксацію, відсутність оригіналу, неналежне оформлення, неможливість ідентифікувати

джерело або несвоєчасне звернення із клопотанням про витребування чи забезпечення доказів.

Окремий практичний блок видання присвячений процесуальним документам. Зразки клопотань, заяв, заперечень, адвокатських запитів та інших документів покликані допомогти правнику перейти від теоретичного розуміння цифрового доказу до його безпосереднього використання у конкретній справі.

Видання розрахована насамперед на адвокатів, суддів, прокурорів, слідчих, працівників правоохоронних органів, судових експертів, науковців, викладачів та здобувачів юридичної освіти. Водночас вона може бути корисною кожному практикуючому юристу, який стикається з електронною інформацією у цивільному, кримінальному, адміністративному чи господарському процесі.

Цифровізація правосуддя не означає автоматичної цифровізації доказування. Навпаки, чим більшу частину суспільних відносин переноситься у цифрове середовище, тим вищими стають вимоги до автентичності, цілісності та достовірності цифрової інформації.

Сучасний суд має оцінювати не лише зміст цифрового доказу, а й історію його походження, спосіб отримання, технічні характеристики, можливість зміни та контекст використання. А сучасний адвокат повинен уміти працювати з цифровим доказом від моменту його виявлення до моменту судової оцінки.

Саме на вирішення цього практичного завдання спрямоване це науково-практичне видання.

Автор сподівається, що запропонований матеріал стане корисним інструментом для формування належної доказової стратегії, допоможе уникати типових процесуальних помилок та сприятиме подальшому розвитку української судової практики у сфері цифрового доказування.

Цифровий доказ уже став невід’ємною частиною сучасного правосуддя. Наступним завданням правової науки і практики є вироблення чітких, передбачуваних та справедливих правил його використання.

АНОТАЦІЯ

У науково-практичному посібнику здійснено комплексне дослідження правової природи, процесуального статусу, способів отримання, фіксації, збереження, дослідження та оцінки цифрових доказів у судовому процесі України.

Актуальність дослідження зумовлена стрімкою цифровізацією суспільних відносин та переходом значної частини юридично значущої інформації в електронне середовище. Електронні документи, електронне листування, повідомлення у месенджерах, матеріали соціальних мереж, фотографії, відео- та аудіозаписи, дані геолокації, інформація з мобільних пристроїв, вебсторінок, електронних реєстрів та інформаційних систем дедалі частіше використовуються як засоби доказування у цивільному, кримінальному, адміністративному та господарському судочинстві.

У виданні досліджено поняття та правову природу цифрового доказу, його співвідношення з електронним доказом, письмовим доказом та іншими засобами доказування. Запропоновано системний підхід до класифікації цифрових доказів залежно від джерела походження, способу створення, форми існування, способу фіксації та характеру інформації.

Окрему увагу приділено питанням **належності, допустимості, достовірності та достатності цифрових доказів**, а також проблемі встановлення їх автентичності. Розглянуто практичні механізми підтвердження походження цифрової інформації, встановлення автора електронного повідомлення, перевірки цілісності файлу та визначення можливості його зміни або редагування.

Значний блок дослідження присвячено **електронним документам та електронному листуванню**, зокрема документам, створеним із використанням електронного підпису, електронній пошті, службовому листуванню, електронним правочинам та інформації, що передається через інформаційно-комунікаційні системи.

Проаналізовано особливості використання як доказів повідомлень у **Telegram, Viber, WhatsApp та інших месенджерів**, а також публікацій, коментарів, фотографій і відеоматеріалів у соціальних мережах.

Особливу увагу приділено проблемі доказового значення скриншотів, встановленню їх джерела, повноти та достовірності.

Окремий розділ присвячено **метаданим**, включаючи EXIF-дані фотографій, технічні характеристики файлів, інформацію про дату та час створення, пристрій, географічні координати, відомості про редагування та інші технічні параметри, які можуть мати значення для встановлення достовірності цифрового доказу.

Досліджено доказове значення **GPS-даних, геолокації, інформації мобільних операторів, даних базових станцій, історії переміщень, інформації мобільних пристроїв та інших технічних джерел**, а також межі їх використання під час доказування.

Особливе місце займають питання використання **фотографій, відеозаписів та аудіозаписів**, у тому числі записів камер відеоспостереження, відеореєстраторів, нагрудних камер, мобільних телефонів та інших цифрових пристроїв. Розглянуто проблеми монтажу, редагування, зміни цифрових файлів та встановлення оригінальності відповідного контенту.

Значну увагу приділено **цифровій та комп'ютерно-технічній експертизі**. Проаналізовано можливості експертного дослідження електронних документів, мобільних пристроїв, комп'ютерів, електронного листування, цифрових фотографій, аудіо- та відеозаписів, а також питання відновлення видаленої інформації та встановлення факту редагування цифрових файлів.

Самостійний напрям дослідження становить проблема **фальсифікації цифрових доказів**. Розглянуто способи підроблення електронного листування, скриншотів, фотографій, відео та аудіозаписів, зміни метаданих, монтажу цифрового контенту, а також сучасні технології створення синтетичної інформації.

Окремий розділ присвячено **штучному інтелекту, deepfake та цифровим доказам**. Досліджено нові ризики, пов'язані зі створенням штучно згенерованих фотографій, відео та аудіозаписів, проблеми встановлення походження такого контенту та необхідність розвитку нових підходів до перевірки його достовірності.

Особливе практичне значення має аналіз **судової практики Верховного Суду** щодо електронних і цифрових доказів. Систематизовано підходи касаційних судів до оцінки електронного листування,

електронних документів, скриншотів, інформації із соціальних мереж, відео-, аудіоматеріалів та інших цифрових джерел доказової інформації.

Також досліджено практику **Європейського суду з прав людини** у частині права на справедливий суд, принципу змагальності, рівності сторін, права на ефективне представлення доказів, захисту приватного життя та допустимості втручання держави в електронні комунікації.

Практична спрямованість видання полягає у формуванні **покровового алгоритму роботи адвоката з цифровими доказами** – від їх виявлення та фіксації до подання суду й аргументованого заперечення проти цифрових доказів іншої сторони.

У виданні наведено зразки процесуальних документів, зокрема клопотань про витребування та забезпечення цифрових доказів, клопотань про призначення експертизи, заперечень щодо допустимості та достовірності цифрової інформації, адвокатських запитів та інших документів, необхідних для ефективного використання цифрових доказів у судовій практиці.

Окремо систематизовано **типові помилки адвокатів та інших учасників процесу** при роботі з цифровою інформацією: подання лише скриншота без підтвердження його походження, відсутність оригінального файлу, неможливість ідентифікувати автора, неналежне збереження цифрової інформації, втрата метаданих, відсутність відомостей про спосіб отримання доказу та інші обставини, які можуть впливати на його доказову силу.

Науково-практичне видання поєднує **теоретичний аналіз, законодавство, судову практику та прикладні рекомендації**, що дозволяє використовувати його як для наукового дослідження проблем цифрового доказування, так і безпосередньо у практичній юридичній діяльності.

Видання розраховане на адвокатів, суддів, прокурорів, слідчих, судових експертів, державних службовців, науковців, викладачів і здобувачів юридичної освіти, а також усіх правників, діяльність яких пов'язана з використанням електронної та цифрової інформації у процесі доказування.

Ключові слова: цифрові докази, електронні докази, електронний документ, електронний підпис, електронне листування, месенджери, соціальні мережі, скриншот, метадані, геолокація, GPS, цифрові сліди, відеозапис, аудіозапис, цифрова експертиза, комп'ютерно-технічна експертиза, фальсифікація доказів, deepfake, штучний інтелект, доказування, допустимість доказів, належність доказів, достовірність доказів, Верховний Суд, Європейський суд з прав людини.

Зміст

Передмова	3
Анотація	7
Вступ	11

РОЗДІЛ І. ЦИФРОВІ ДОКАЗИ ЯК НОВА КАТЕГОРІЯ

СУДОВОГО ДОКАЗУВАННЯ	70
1.1. Поняття цифрового доказу	70
1.2. Правова природа цифрової інформації	73
1.3. Цифровий доказ як об'єкт процесуального доказування	75
1.4. Співвідношення цифрового доказу й електронного доказу	77
1.5. Цифровий доказ і традиційний письмовий доказ	78
Загальний висновок до підрозділів 1.1–1.5	81
1.6. Цифровий доказ як самостійне джерело доказової інформації	82
1.7. Класифікація цифрових доказів	84
1.8. Первинні та похідні цифрові докази	87
1.9. Оригінал і копія цифрового доказу	88
1.10. Проблема автентичності цифрової інформації	89
1.11. Достовірність, належність і допустимість цифрових доказів	90
1.12. Ризики зміни та фальсифікації цифрової інформації	92
Загальний висновок до підрозділів 1.6–1.12	94

РОЗДІЛ ІІ. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ВИКОРИСТАННЯ

ЦИФРОВИХ ДОКАЗІВ	96
2.1. Конституційні засади доказування	96
2.2. Цифрові докази в цивільному процесі	106
2.3. Цифрові докази в адміністративному судочинстві	123
2.4. Цифрові докази у господарському процесі	132
2.5. Цифрові докази у кримінальному провадженні	146
2.6. Електронні докази у процесуальному законодавстві України	164
2.7. Законодавство про електронні документи	175
2.8. Електронний підпис і його доказове значення	177
2.9. Законодавство про електронні довірчі послуги	178
2.10. Захист персональних даних у процесі використання цифрових доказів	179
2.11. Правове регулювання інформації в інформаційно- комунікаційних системах	180

2.12. Співвідношення відкритості судового процесу й захисту цифрової інформації	182
--	-----

РОЗДІЛ III. ЕЛЕКТРОННІ ДОКУМЕНТИ ЯК ДОКАЗИ.....185

3.1. Поняття електронного документа	185
3.2. Реквізити електронного документа	187
3.3. Електронний підпис.....	189
3.4. Кваліфікований електронний підпис.....	190
3.5. Електронна печатка.....	191
Науково-практичний висновок до підрозділів 3.1–3.5	193
3.6. Електронний документ без електронного підпису	194
3.7. Надсилання електронного документа	196
3.8. Електронна пошта як спосіб передачі документа.....	197
3.9. Документи з електронних систем.....	199
3.10. Дані з державних електронних реєстрів	200
3.11. Вебсторінки та вебдокументи	203
3.12. Проблема встановлення автора електронного документа.....	205
3.13. Перевірка цілісності електронного документа	206
3.14. Зберігання електронного доказу	208

РОЗДІЛ IV. ЕЛЕКТРОННЕ ЛИСТУВАННЯ

ТА ПОВІДОМЛЕННЯ В МЕСЕНДЖЕРАХ.....212

4.1. Електронна пошта як доказ.....	212
4.2. Листування між сторонами спору	213
4.3. Листування адвоката з клієнтом	215
4.4. Листування працівника з роботодавцем	216
4.5. Листування у цивільних правовідносинах	218
Науково-практичний висновок до підрозділів 4.1–4.5	220
4.6. Telegram як джерело доказової інформації.....	221
4.7. Viber як джерело доказової інформації	225
4.8. WhatsApp та інші месенджери.....	229
4.9. Повідомлення в соціальних мережах	231
4.10. Голосові повідомлення	232
Науково-практичний висновок до підрозділів 4.6–4.10	234
4.11. Видалені повідомлення	234
4.12. Проблема встановлення особи автора повідомлення	236
4.13. Скриншот листування.....	238
4.14. Відеозапис екрана як спосіб фіксації листування.....	239
4.15. Належність і допустимість електронного листування	241

Науково-практичний висновок до підрозділів 4.11–4.15	243
--	-----

РОЗДІЛ V. СКРИНШОТИ, ВЕБСТОРІНКИ

ТА СОЦІАЛЬНІ МЕРЕЖІ	245
5.1. Скриншот як цифровий доказ.....	245
5.2. Правова природа скриншота.....	246
5.3. Вимоги до належного оформлення скриншота.....	248
5.4. Скриншот вебсторінки	249
5.5. Скриншот профілю користувача	251
Науково-практичний висновок до підрозділів 5.1–5.5	252
5.6. Публікації у Facebook	253
5.7. Публікації в Instagram.....	257
5.8. YouTube та відеоконтент	261
5.9. TikTok та інші цифрові платформи	263
5.10. Видалена інформація з інтернету	266
Науково-практичний висновок до підрозділів 5.6–5.10	267
5.11. Вебархіви	268
5.12. Нотаріальне посвідчення вебсторінки	270
5.13. Протокол огляду вебсторінки.....	272
5.14. Типові помилки при поданні скриншотів до суду	273
Науково-практичний висновок до підрозділів 5.11–5.14	275

РОЗДІЛ VI. МЕТАДАНИ ТА ТЕХНІЧНА ІНФОРМАЦІЯ

6.1. Поняття метаданих	277
6.2. Види метаданих.....	278
6.3. Метадані електронного документа.....	280
6.4. Метадані фотографії	282
6.5. EXIF-дані	283
6.6. Практичний алгоритм дослідження метаданих	285
Науково-практичний висновок до підрозділів 6.1–6.6	285
6.7. Метадані відеофайлів	286
6.8. Метадані електронної пошти.....	287
6.9. Дата та час створення файлу.....	288
6.10. Інформація про пристрій	289
6.11. IP-адреса як джерело доказової інформації.....	290
6.12. MAC-адреса та інші технічні ідентифікатори.....	291
6.13. Хеш-значення та встановлення цілісності файлу	293
Науково-практичний висновок до підрозділів 6.7–6.13	294
6.14. Значення метаданих для встановлення достовірності доказу	295

6.15. Видалення або зміна метаданих	299
Науково-практичний висновок	303

РОЗДІЛ VII. ФОТОГРАФІЇ, ВІДЕО- ТА АУДІОЗАПИСИ.....304

7.1. Цифрова фотографія як доказ	304
7.2. Відеозапис як доказ.....	305
7.3. Аудіозапис як доказ.....	306
7.4. Відеореєстратори	307
7.5. Камери відеоспостереження	308
7.6. Нагрудні камери поліцейських	312
7.7. Відеозаписи з мобільних телефонів	324
7.8. Відеозаписи з безпілотних літальних апаратів	325
7.9. Монтаж і редагування відео.....	326
7.10. Встановлення оригінальності відеозапису	327
7.11. Голосова ідентифікація.....	328
7.12. Цифрова фото- та відеотехнічна експертиза	329
Науково-практичний висновок	332

РОЗДІЛ VIII. ГЕОЛОКАЦІЯ ТА ДАНІ

МОБІЛЬНИХ ПРИСТРОЇВ.....333

8.1. Геолокація як доказ	333
8.2. GPS-дані.....	337
8.3. Дані мобільного оператора.....	341
8.4. Інформація про місцезнаходження мобільного телефона.....	344
8.5. Дані Google Maps і аналогічних сервісів	346
Науково-практичний висновок до підрозділів 8.1–8.5	348
8.6. Історія переміщень.....	349
8.7. Геомітки фотографій.....	350
8.8. Дані Wi-Fi	351
8.9. Дані Bluetooth.....	351
8.10. Базові станції мобільного зв'язку	352
8.11. Встановлення місцезнаходження особи	353
8.12. Межі доказового значення геолокації	354

РОЗДІЛ IX. ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ

ПРОВАДЖЕННІ.....356

9.1. Цифрові докази та кримінальне доказування.....	356
9.2. Тимчасовий доступ до електронної інформації.....	357
9.3. Обшук цифрових пристроїв.....	358

9.4. Огляд мобільного телефона	360
9.5. Огляд комп'ютера	361
9.6. Копіювання цифрової інформації.....	363
9.7. Вилучення електронних носіїв	364
9.8. Комп'ютерно-технічна експертиза	366
9.9. Відновлення видалених файлів	367
9.10. Цифрові сліди кримінального правопорушення.....	368
9.11. Ланцюг збереження цифрового доказу	369
9.12. Недопустимість цифрового доказу.....	370
Практичний висновок	371

РОЗДІЛ X. ЦИФРОВА ЕКСПЕРТИЗА

10.1. Поняття цифрової експертизи.....	372
10.2. Комп'ютерно-технічна експертиза	373
10.3. Експертиза мобільних пристроїв.....	374
10.4. Експертиза електронних документів.....	375
10.5. Експертиза електронного листування	376
10.6. Експертиза аудіо- та відеозаписів.....	377
10.7. Встановлення факту редагування файлу	379
10.8. Відновлення видаленої інформації.....	381
10.9. Питання, які можуть бути поставлені експерту	383
10.10. Типові помилки при призначенні експертизи	385
10.11. Оцінка висновку експерта судом	386
Загальний висновок до підрозділів 10.7–10.11	389

РОЗДІЛ XI. ФАЛЬСИФІКАЦІЯ ЦИФРОВИХ ДОКАЗІВ

11.1. Поняття цифрової фальсифікації.....	390
11.2. Підробка електронного документа	392
11.3. Монтаж фотографій	393
11.4. Монтаж відео	395
11.5. Редагування аудіозаписів	396
Загальний висновок до підрозділів 11.1–11.5.....	398
11.6. Фальсифікація листування	398
11.7. Підробка скріншотів	400
11.8. Видалення або зміна метаданих	401
11.9. Deepfake як новий вид цифрової фальсифікації	403
11.10. Способи перевірки достовірності цифрового доказу	404
Загальний висновок до підрозділів 11.6–11.10.....	407

РОЗДІЛ XII. ШТУЧНИЙ ІНТЕЛЕКТ, DEEPFAKE

І ЦИФРОВІ ДОКАЗИ	408
12.1. Штучний інтелект як фактор трансформації доказування.....	408
12.2. Генерований штучним інтелектом контент.....	409
12.3. Deepfake-фотографії.....	411
12.4. Deepfake-відео.....	412
12.5. Синтетичний аудіозапис.....	414
Загальний висновок до підрозділів 12.1–12.5.....	416
12.6. Проблема встановлення походження цифрового контенту.....	416
12.7. Автоматизовані системи перевірки цифрових доказів.....	418
12.8. Використання ШІ адвокатом при аналізі доказів.....	420
12.9. Межі використання ШІ в судовому доказуванні.....	422
12.10. Перспективи правового регулювання.....	423
Загальний науково-практичний висновок.....	425

РОЗДІЛ XIII. ЦИФРОВІ ДОКАЗИ У ПРАКТИЦІ

ВЕРХОВНОГО СУДУ	427
13.1. Загальні підходи Верховного Суду.....	427
13.2. Практика Касаційного цивільного суду.....	429
13.3. Практика Касаційного кримінального суду.....	431
13.4. Практика Касаційного адміністративного суду.....	433
13.5. Практика Касаційного господарського суду.....	434
13.6. Електронне листування у практиці Верховного Суду.....	435
Науково-практичний висновок до підрозділів 13.1–13.6.....	438
13.7. Скриншоти в судовій практиці.....	438
13.8. Соціальні мережі як джерело доказів.....	440
13.9. Відеозаписи та аудіозаписи.....	442
13.10. Електронні документи.....	443
13.11. Оцінка достовірності цифрових доказів.....	444
13.12. Недопустимість цифрових доказів.....	445
13.13. Правові позиції Верховного Суду: систематизація.....	447
Загальний висновок до розділу.....	449

РОЗДІЛ XIV. ПРАКТИКА ЄСПЛ І МІЖНАРОДНІ

СТАНДАРТИ	450
14.1. Право на справедливий суд.....	450
14.2. Принцип змагальності.....	451
14.3. Рівність сторін.....	452
14.4. Право на ефективне подання доказів.....	453
14.5. Цифрові докази та стаття 6 Конвенції.....	454

14.6. Право на приватність і цифрова інформація	455
14.7. Стаття 8 Конвенції	455
14.8. Перехоплення електронних комунікацій	456
14.9. Доступ держави до цифрових даних	457
14.10. Пропорційність втручання	457
Висновок	459

РОЗДІЛ XV. АЛГОРИТМ РОБОТИ АДВОКАТА З ЦИФРОВИМИ ДОКАЗАМИ

15.1. Виявлення цифрового доказу	461
15.2. Фіксація цифрової інформації	462
15.3. Збереження оригіналу	465
15.4. Створення резервної копії	466
15.5. Встановлення джерела інформації	467
15.6. Перевірка автентичності	471
15.7. Перевірка метаданих	473
15.8. Забезпечення доказів	475
15.9. Подання цифрового доказу до суду	476
15.10. Заперечення проти цифрового доказу іншої сторони	477
15.11. Клопотання про витребування цифрових доказів	478
15.12. Клопотання про призначення експертизи	479
15.13. Робота з оператором електронних комунікацій	481
15.14. Тактика допиту щодо цифрового доказу	482
Практична карта розділу	484
Загальний практичний висновок	485

РОЗДІЛ XVI. ПРОЦЕСУАЛЬНІ ДОКУМЕНТИ

16.1. Клопотання про витребування електронного доказу	486
16.2. Клопотання про забезпечення цифрового доказу	488
16.3. Клопотання про призначення комп'ютерно-технічної експертизи	489
16.4. Клопотання про огляд вебсторінки	491
16.5. Заява про забезпечення доказів	491
16.6. Заперечення проти допустимості цифрового доказу	492
Загальний висновок до підрозділів 16.1–16.6	494
16.7. Заперечення проти достовірності електронного листування	495
16.8. Адвокатський запит щодо цифрової інформації	497
16.9. Заява про витребування даних у провайдера	499
16.10. Зразок протоколу фіксації цифрової інформації	500
Висновок	505

РОЗДІЛ XVII. ТИПОВІ ПОМИЛКИ ПРИ ВИКОРИСТАННІ ЦИФРОВИХ ДОКАЗІВ	506
17.1. Подання лише скриншота	506
17.2. Відсутність інформації про джерело	507
17.3. Відсутність оригінального файлу	508
17.4. Неможливість ідентифікації автора	509
17.5. Відсутність метаданих	510
17.6. Неналежне зберігання файлу	511
17.7. Монтаж або редагування	512
17.8. Відсутність повного контексту	513
Загальний висновок до підрозділів 17.1–17.8	517
17.9. Неправильне оформлення електронного доказу	518
17.10. Несвоєчасне витребування цифрової інформації	519
17.11. Неправильне формулювання питань експерту	520
17.12. Ігнорування питання конфіденційності	521
17.13. Неправильна оцінка доказової сили цифрової інформації	523
17.14. Таблиця типових помилок і способів їх виправлення	524
17.15. Практичний алгоритм запобігання помилкам	525
Висновок до розділу	525
 РОЗДІЛ XVIII. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ	527
18.1. Алгоритм перевірки цифрового доказу	527
18.2. Чекліст адвоката	530
18.3. Чекліст судді	531
18.4. Чекліст слідчого	533
18.5. Чекліст експерта	533
18.6. Алгоритм фіксування вебсторінки	534
18.7. Алгоритм перевірки соціальних мереж та месенджерів	537
18.8. Загальна карта роботи з цифровим доказом	537
18.9. «Золоте правило» цифрового доказування	538
18.10. Підсумковий чекліст	538
Висновок до підрозділів 18.1–18.10	539
18.11. Алгоритм фіксування листування	540
18.12. Алгоритм роботи з відеозаписом	542
18.13. Алгоритм перевірки скриншота	543
18.14. Алгоритм перевірки метаданих	545
18.15. Алгоритм протидії фальсифікації	546
18.16. Практичні рекомендації щодо підготовки позову	548
18.17. Фінальний чекліст цифрових доказів перед поданням позову	552
Висновок до підрозділів 18.11–18.17	553

Висновки	554
Загальний науково-практичний висновок	565
ДОДАТКИ	567
Додаток 1	
ЗРАЗОК КЛОПОТАННЯ ПРО ВИТРЕБУВАННЯ	
ЦИФРОВОГО ДОКАЗУ	567
Додаток 2	
ЗРАЗОК КЛОПОТАННЯ ПРО ЗАБЕЗПЕЧЕННЯ	
ЦИФРОВОГО ДОКАЗУ	569
Додаток 3	
ЗРАЗОК КЛОПОТАННЯ ПРО ПРИЗНАЧЕННЯ ЦИФРОВОЇ	
ЕКСПЕРТИЗИ	571
Додаток 4	
ЗРАЗОК АДВОКАТСЬКОГО ЗАПИТУ	
ЩОДО ЦИФРОВОЇ ІНФОРМАЦІЇ.....	573
Практична примітка до додатків.....	575
Додаток 5	
ЗАПЕРЕЧЕННЯ ПРОТИ ЦИФРОВОГО ДОКАЗУ,	
ПОДАНОГО ІНШОЮ СТОРОНОЮ	576
Додаток 6	
ЧЕКЛІСТ ПЕРЕВІРКИ ЕЛЕКТРОННОГО ДОКАЗУ	579
Додаток 7	
ЧЕКЛІСТ ПЕРЕВІРКИ СКРИНШОТА	581
Додаток 8	
ЧЕКЛІСТ ПЕРЕВІРКИ ВІДЕОЗАПISУ	583
Додаток 9	
ТАБЛИЦЯ ВИДІВ ЦИФРОВИХ ДОКАЗІВ	586
Додаток 10	
СИСТЕМАТИЗОВАНА ПРАКТИКА ВЕРХОВНОГО СУДУ	
ЩОДО ЦИФРОВИХ ДОКАЗІВ.....	589
Додаток 11	
ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ	
ЩОДО ЦИФРОВОЇ ІНФОРМАЦІЇ ТА ЕЛЕКТРОННИХ ДОКАЗІВ	593
Список використаних джерел	597

Виробничо-практичне і наукове видання

Гайворонський Руслан Володимирович

ЦИФРОВІ ДОКАЗИ У СУДОВОМУ ПРОЦЕСІ:

**електронні документи, метадані, листування, месенджери, відео,
геолокація, скріншоти, цифрова експертиза та практика
Верховного Суду**

Науково-практичний посібник

Видається в авторській редакції

Підписано до друку 01.10.2026. Формат 60×84/16.
Ум. друк. арк. 62. Обл.-вид. арк. 43. Тираж 100 пр. Зам. № 751

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20
Вебсайт: <https://pravo-izdat.com.ua>
E-mail для замовників послуг: verstka@pravo-izdat.com.ua
E-mail для покупців: sales@pravo-izdat.com.ua
Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт Плюс»,
вул. Весніна, 12, м. Харків, 61023, Україна
Тел. (097) 445-07-79
Вебсайт: <https://promart.in.ua>
Свідоцтво суб'єкта видавничої справи ДК № 8388 від 16.07.2025



Перейти на сайт →