

Я. В. Неділько, доктор філософії в галузі права (PhD), асистент
Київський національний університет імені Тараса Шевченка
Навчально-науковий інститут права
Кафедра кримінального процесу та криміналістики
вул. Володимирська, 60, Київ, 01033, Україна
e-mail: yaroslavnedilko@knu.ua
ORCID iD: <https://orcid.org/0000-0003-1483-3479>

ДОКТРИНА ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: НАЦІОНАЛЬНІ ОСОБЛИВОСТІ ТА СВІТОВІ ТЕНДЕНЦІЇ

Статтю присвячено дослідженню місця та ролі електронних доказів у кримінальному провадженні. Зауважено, що з появою засобів інформаційно-комп'ютерних технологій (смартфонів, планшетів, ноутбуків тощо), які злочинці почали використовувати у своїх протиправних цілях, виникає новий вид доказів – електронні докази. Серед вітчизняних вчених не існує єдності думок щодо визначення поняття, місця та ролі електронних доказів у кримінальному провадженні. Це викликано не лише відсутністю нормативного закріплення електронних доказів у Кримінальному процесуальному кодексі України (КПК України), але і специфікою їх порядку виявлення, дослідження, вилучення, зберігання та оцінці.

Наголошено, що в КПК України не міститься визначення поняття «електронних доказів», однак воно наводиться у Кодексі адміністративного судочинства України (КАС України), Господарському процесуальному (ГПК України) та Цивільному процесуальному кодексах України (ЦПК України).

Зауважено про використання в науковій літературі схожих понять: «цифровий доказ», «електронно-цифровий доказ», «електронний (цифровий) доказ» тощо.

У статті вживається поняття саме «електронний доказ», оскільки в міжнародних нормативних актах, зокрема в актах Європейського Союзу, переважно вживається термін *electronic evidence* (електронний доказ).

Наводиться порівняльний аналіз підходів закріплення та регулювання електронних доказів у законодавстві зарубіжних країнах, зокрема Латвії, Угорщини, Сінгапуру, Великої Британії та США. Детально наводиться як національна так і зарубіжна судова практика щодо дослідження електронних доказів у кримінальному провадженні.

Сформовані пропозиції щодо можливого закріплення електронних доказів у кримінальному процесуальному законодавстві України двома шляхами, а саме: закріплення поняття електронних доказів у КПК України, встановивши його визначення та вказавши, що саме може відноситися до електронних доказів та створення окремого закону, який буде визначати процедуру дослідження, збирання, зберігання та аналізу електронних доказів. Встановлення чітких і зрозумілих процедур належності та допустимості електронних доказів у кримінальному провадженні.

Ключові слова: електронні докази, цифрові докази, кримінальне провадження, досудове розслідування, допустимість доказів, міжнародний досвід, кримінальний процес, судова практика.

Постановка проблеми. У науці кримінального процесуального права тривалий час точаться дискусії серед вчених щодо визначення поняття, місця та ролі електронних доказів у кримінальному провадженні. Вони викликані не лише відсутністю нормативного закріплення електронних доказів у Кримінальному процесуальному кодексі України (КПК України), але і специфікою їх порядку виявлення, дослідження, вилучення, зберігання та оцінці.

Мета статті. Оскільки останнім часом переважна більшість обвинувачень ґрунтується на електронних доказах (файли, електронні листи, зображення та відео розміщені на сайтах тощо), постає нагальна потреба у дослідженні доктрини електронних доказів у системі кримінального процесуального права.

Аналіз останніх досліджень і публікацій. Особливу увагу проблемам визначення електронних доказів приділили вчені, зокрема: Г. К. Авдєєва, Н. М. Ахтирська, В. В. Вапнярчук, М. В. Гуцалюк, О. В. Капліна, О. В. Сіренко, І. Ю. Та-тулич, В. Г. Хахановський та інші.

Виклад основного матеріалу. Традиційно, переважна частина доказів мали фізичну форму, наприклад, паперові документи, знаряддя вчинення кримінального правопорушення тощо.

Проте, з появою засобів інформаційно-комп'ютерних технологій (смартфонів, планшетів, ноутбуків тощо), які злочинці почали використовувати у своїх протиправних цілях, виникає новий вид доказів – електронні.

Наприклад, один із перших задукоментованих випадків, пов'язаних зі злочинним використанням комп'ютера, стався у 1966 році в штаті Міннеаполіс (США). Програміст М. А. Беннет, маючи доступ до комп'ютерної системи Національного міського банку Міннеаполіса, написав код, який змінив програмне забезпечення так, що у звітах не відображалось перевищення кредитного ліміту на його особистому рахунку. Це давало йому можливість незаконно користуватися коштами банку у власних інтересах. У зв'язку з виходом з ладу комп'ютерної системи, банк вимушений був повернутися до ручної обробки звітів, що і дало виявити невідповідності на рахунку Беннета. За проведеним ФБР розслідуванням, у січні 1967 року Беннет отримав умовний строк. Цю справу в історії вважають першою, що пов'язана зі злочинним використанням комп'ютера [1].

Судові органи вперше зіштовхнулися з новими для того часу злочинними проявами, що були пов'язані з необхідністю дослідження електронних даних як доказів.

Особливої актуальності питання дослідження електронних доказів набуває і в наш час.

Звертаючись до визначення поняття електронний доказ, варто зазначити, що в науковій літературі також вживаються наступні поняття: «цифровий доказ», «електронно-цифровий доказ», «електронний (цифровий) доказ» тощо.

Оминаючи наукові дискусії з приводу використання зазначених понять, вважаємо за доцільне застосовувати термін «електронний доказ», оскільки в міжнародних нормативних актах, зокрема в актах Європейського Союзу, переважно вживається термін *electronic evidence* (електронний доказ) [2; 3].

Попри те, що в КПК України не міститься визначення поняття «електронних доказів», однак воно наводиться у Кодексі адміністративного судочинства України (КАС України), Господарському процесуальному кодексі (ГПК України) та Цивільному процесуальному кодексі України (ЦПК України).

Так, у ст. 99 Кодексу адміністративного судочинства України під електронними доказами розуміється інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема електронні документи (текстові документи, графічні зображення, плани, фотографії, відео-та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [4].

Подібні визначення поняття електронних доказів містяться і в ст. 96 ГПК України та ст. 100 ЦПК України.

Відсутність визначення поняття електронних доказів у КПК України, на наш погляд, може пояснюватися тим, що законодавець не наважується вносити відповідні зміни в кримінальне процесуальне законодавство, а продовжує традиційно використовувати дефініції «документи» та «речові» докази, при цьому розглядаючи електронні докази як їх аналоги не виділяючи окремо.

Так, згідно ст. 99 КПК України електронні докази вважаються документами, а матеріальні носії, на яких вони розміщені, визнаються речовими доказами. Документом – є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [5]. Крім того, до документів, можуть належати: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) [5].

Відсутність визначення поняття електронних доказів у кримінальному процесуальному законодавстві змушує судову практику самостійно напрацьовувати підходи до їх тлумачення та застосування.

Наприклад, у Постанові колегії суддів Другої судової палати ККС ВС від 06 лютого 2024 року наголошується, що не надання стороною обвинувачення з будь-яких підстав протоколу проведення слідчого експерименту за участю потерпілого не може зашкодити справедливому судовому розгляду з урахуванням того, що проведення цієї слідчої дії відбулося без порушення будь-яких прав і свобод людини, передбачених Конвенцією та Конституцією України, а наданий технічний носій інформації, на якому зафіксовано проведення цієї слідчої дії, за обставин цього кримінального провадження, є електронним доказом, на якому міститься інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи [6].

У іншій Постанові колегії суддів Третьої судової палати ККС ВС від 12 червня 2024 року було зазначено, що основними доказами в кримінальних провадженнях щодо злочинів проти основ національної безпеки України є електронні (цифрові) докази, до яких належать: матеріали фотозйомки, звуко-запису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), що містяться у відкритих (інтернет; різноманітні засоби масової інформації; соціальні мережі) чи закритих мережах (приватні месенджери та телеграм канали; особисте листування з використанням комп'ютерної техніки і мобільних телефонів, флешносії, карти пам'яті тощо) [7].

Разом з тим, у 2020 році було підготовлено проєкт Закону «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів», де пропонувалось визначити у ст. 100-1 КПК України поняття «електронний доказ», під яким би розумілася інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [8].

Зазначений законопроект у січні 2021 року було прийнято у першому читанні за основу та направлено Комітету Верховної Ради України з питань правоохоронної діяльності на доопрацювання з урахуванням зауважень і пропозицій суб'єктів права законодавчої ініціативи та внесення його на розгляд Верховної Ради України у другому читанні. Законопроект у другому читанні не розглядався [9].

У ряді зарубіжних країн поняття «електронних доказів» закріплено у кримінальному процесуальному законодавстві.

Зокрема, згідно зі ст. 136 КПК Латвії, електронними доказами у кримінальному провадженні можуть бути факти у вигляді обробленої електронної інформації, що зберігається або передається автоматизованими пристроями чи системами обробки даних [10].

У Кримінальному процесуальному кодексі Угорщини (ст. 205) наводиться визначення «електронних даних» – це будь-яке представлення фактів, інформації та термінів, що придатне для технічної обробки інформаційною системою, включаючи будь-яку програму, яка реалізує функцію інформаційної системи [11].

У Республіці Сінгапур існує Закон «Про докази» [12], який урегульовує правила прийнятності доказів у судових процесах, у тому числі і в кримінальному провадженні. Він містить положення щодо електронних записів та їх використання як доказів у суді.

Під «електронним записом» розуміється запис, створений, переданий, отриманий або збережений за допомогою електронних, магнітних, оптичних або інших засобів в інформаційній системі або переданий з однієї інформаційної системи в іншу.

Окрім цього, в даному Законі наводяться критерії застосування електронних доказів (116A) у кримінальному провадженні:

- 1) якщо не надано доказів, що засіб, який створив певний файл піддавався змінам, то запис файл є належним та допустимим доказом;
- 2) якщо запис був створений третьою особою, яка не є стороною у кримінальному провадженні, то цей запис є належним та допустимим доказом;
- 3) якщо запис був створений стороною провадження, а інша сторона заперечує цей доказ, то доказ вважається належним та допустим.

У Великій Британії також існує окремий нормативний акт: «Про кримінальне правосуддя (Criminal Justice Act 2003) [13], в якому не визначається поняття електронних доказів, однак встановлюється презумпція (правило) належної роботи пристрою. Відповідно до положень нормативного акту, механічні або автоматизовані пристрої працюють належним чином, якщо не доведено протилежне.

Наприклад, у справі Публічного обвинувачення проти Вільяма Елліотта та Роберта Маккі (2013) (The Public Prosecution Service v. William Elliott and

Robert McKee) [14], які були заарештовані за підозрою у крадіжці будівельних матеріалів, під час розслідування поліція використала електронний пристрій для зняття відбитків пальців — Livescan. Відбиток великого пальця Елліотта збігся з відбитком, знайденим на місці вчинення кримінального правопорушення. Однак на момент використання пристрій Livescan не був офіційно затверджений Державним секретарем, як того вимагав Порядок поліції та кримінальних доказів.

Тому, Верховний Суд зауважив, що скани відбитків пальців, отримані за допомогою електронного зчитувача Livescan, були допустимими доказами, навіть якщо на той час даний пристрій не було схвалено Державним секретарем.

Це рішення підкреслює, що в британській судовій практиці основна увага приділяється надійності та достовірності електронних доказів, а не лише формальним процедурам їх отримання. Таким чином, навіть за відсутності офіційного затвердження пристрою, отримані з його допомогою докази можуть бути визнані допустимими, якщо їх достовірність не викликає сумнівів.

У Сполучених Штатах Америки є Закон «Федеральні правила доказування» [15]. У даному нормативному акті, поняття електронного доказу не наводиться. Однак у п. 5 ст. 101 зазначаються основні терміни, та вказується, що посилання на будь-який вид письмового матеріалу або будь-яке інше середовище включає електронно збережену інформацію.

В Законі (901 стаття) встановлюється аутентифікація (підтвердження) доказів. Для того, щоб задовольнити вимогу аутентифікації або ідентифікації предмета доказів, сторона, що подає доказ, повинна надати достатньо доказів для підтвердження того, що предмет є тим, чим він заявляється.

Крім цього, у даному Законі зазначається вимога про достовірність електронних доказів. Зокрема, такими є записи, створені електронними процесами або системами, які дають точний результат і сертифіковані уповноваженою особою.

Слід зауважити, що процес сертифікації передбачає надання відповідного документу, в якому підтверджується достовірність даних або записів. Це може бути сертифікат, підписаний особою, яка бере на себе відповідальність за правильність і достовірність цього запису.

Наприклад, представник організації (ІТ-менеджер), що зберігає електронні дані, може видати сертифікат про те, що файл або електронний запис був створений, збережений і зафіксований в межах звичайної діяльності цієї організації. Сертифікат містить відомості про час створення файлу, його автентичність і відсутність змін з моменту його створення.

Якщо прокурор надає як доказ електронні дані, вилучені з жорсткого диску сервера чи комп'ютера підозрюваного/обвинуваченого, у цьому випадку, технічний експерт, що працював з жорстким диском, надає сертифікат, який підтверджує, що дані були скопійовані з оригінального пристрою за допомогою процесу цифрової ідентифікації. Експерт зазначає, що методи копіювання не змінили зміст даних.

З огляду на міжнародну практику країн Європейського Союзу [2; 3; 16; 17] щодо електронних доказів у кримінальному провадженні, суди застосовують низку критеріїв, які гарантують їхню достатність і допустимість:

1) законність отримання. Докази повинні бути зібрані відповідно до законодавства, без порушення прав людини;

2) автентичність та цілісність. Необхідно підтвердити, що доказ є оригінальним і не був змінений з моменту його отримання. Електронні докази мають бути збережені в первісному стані без жодних змін;

3) допустимість та релевантність (належність). Доказ повинен відповідати процесуальним вимогам для його прийняття в суді. Суд і сторони повинні мати доступ до обладнання та програмного забезпечення, необхідного для роботи з електронними доказами. Доказ має безпосередньо стосуватися справи та підтверджувати або спростовувати обставини, що розглядаються;

4) ланцюг збереження. Має бути забезпечено документування кожного етапу роботи з електронними доказами: хто, коли і за яких умов їх вилучив, зберігав і аналізував;

5) технологічна нейтральність. Принципи застосовуються до всіх типів електронних доказів, незалежно від платформи або технології, яка використовувалася.

Висновки і пропозиції. Таким чином, з аналізу міжнародного законодавства та практики можна запропонувати наступні шляхи впровадження електронних доказів у кримінальне процесуальне законодавство України:

1. Закріплення поняття електронних доказів у КПК України, встановивши його визначення та вказавши, що саме може відноситися до електронних доказів.

2. Створення окремого закону, який буде визначати процедуру дослідження, збирання, зберігання та аналізу електронних доказів. Встановлення чітких і зрозумілих процедур належності та допустимості електронних доказів у кримінальному провадженні.

Список використаної літератури

1. Kalat D. Nervous System #1: The Thief and the Scientist The Story of the First White Hat Hacker. Legaltech News, February 5. 2018. URL: https://media.thinkbrg.com/wp-content/uploads/2020/06/12122052/Kalat_Legaltech_Feb2018.pdf.
2. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543> (дата звернення: 03.02.2025).
3. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Strasbourg, 12.V.2022. URL: <https://rm.coe.int/1680a49dab>.
4. Кодекс адміністративного судочинства України : Закон України від 06 липня 2005 р. № 2747-IV. URL: <https://zakon.rada.gov.ua/laws/show/2747-15#Text> (дата звернення 03.02.2025).
5. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-IV. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення 03.02.2025).
6. Постанова колегії суддів Другої судової палати ККС ВС від 06.02.2024 р. у справі № 645/6247/16-к. URL: <https://reyestr.court.gov.ua/Review/116862907>.
7. Постанова Верховного Суду від 12 червня 2024 р. у справі № 569/190/23. URL: <https://reyestr.court.gov.ua/Review/119741340> (дата звернення 03.02.2025).
8. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : проєкт Закону від 01 вересня 2020 р. № 4004. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення 03.02.2025).
9. Про прийняття за основу проєкту Закону України про внесення змін до

Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : проект Постанови від 06 січня 2021 р. № 4004/П. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70797 (дата звернення 03.02.2025).

10. Criminal Procedure Law. URL: <https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law.com> (дата звернення 03.02.2025).
11. Törvény a büntetőeljárásról. URL: <https://net.jogtar.hu/jogszabaly?docid=a1700090.tv> (дата звернення 03.02.2025).
12. Evidence Act (1 July 1893). URL: <https://sso.agc.gov.sg/Act/EA1893> (дата звернення 03.02.2025).
13. Criminal Justice Act 2003. URL: <https://www.legislation.gov.uk/ukpga/2003/44/contents> (дата звернення 03.02.2025).
14. The Public Prosecution Service v William Elliott and Robert McKee [2013] UKSC 32. URL: https://en.wikipedia.org/wiki/The_Public_Prosecution_Service_v_William_Elliott,_Robert_McKee (дата звернення 03.02.2025).
15. Federal Rules of Evidence. URL: https://www.uscourts.gov/sites/default/files/evidence_federal_rules_pamphlet_dec_1_2023.pdf (дата звернення 03.02.2025).
16. Guidelines for digital forensics first responders. Best practices for search and seizure of electronic and digital evidence. URL: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf. (дата звернення 03.02.2025).
17. Sirius EU electronic evidence situation report 2024. 28 Nov 2024. URL: <https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2024> (дата звернення 03.02.2025).

References

1. Kalat, D. (2018). Nervous System #1: The thief and the scientist: The story of the first white hat hacker. Legaltech News. URL: https://media.thinkbrg.com/wp-content/uploads/2020/06/12122052/Kalat_Legaltech_Feb2018.pdf
2. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543> (accessed February 3, 2025).
3. Council of Europe (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Strasbourg. URL: <https://rm.coe.int/1680a49dab>
4. Code of Administrative Procedure of Ukraine: Law of Ukraine dated July 6, 2005 No. 2747-IV. URL: <https://zakon.rada.gov.ua/laws/show/2747-15#Text> (accessed February 3, 2025) [in Ukrainian].
5. Criminal Procedure Code of Ukraine: Law of Ukraine dated April 13, 2012 No. 4651-IV. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (accessed February 3, 2025) [in Ukrainian].
6. Ruling of the Panel of Judges of the Second Judicial Chamber of the Supreme Court of Ukraine dated February 6, 2024, in case No. 645/6247/16-k. URL: <https://reyestr.court.gov.ua/Review/116862907> [in Ukrainian].
7. Ruling of the Supreme Court of Ukraine dated June 12, 2024, in case No. 569/190/23. URL: <https://reyestr.court.gov.ua/Review/119741340> (accessed February 3, 2025) [in Ukrainian].
8. On amendments to the Criminal Procedure Code of Ukraine to improve the efficiency of combating cybercrime and the use of electronic evidence: Draft Law dated September 1, 2020 No. 4004. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (accessed February 3, 2025) [in Ukrainian].
9. On adoption as a basis of the draft Law of Ukraine on amendments to the Criminal Procedure Code of Ukraine to improve the efficiency of combating cybercrime and the use of electronic evidence: Draft Resolution dated January 6, 2021 No. 4004/P. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70797 (accessed February 3, 2025)

[in Ukrainian].

10. Criminal Procedure Law. URL: <https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law.com> (accessed February 3, 2025).
11. Criminal Procedure Law. URL: <https://net.jogtar.hu/jogszabaly?docid=a1700090.tv> (accessed February 3, 2025) [in Hungarian].
12. Evidence Act (1893, July 1). URL: <https://sso.agc.gov.sg/Act/EA1893> (accessed February 3, 2025).
13. Criminal Justice Act 2003. URL: <https://www.legislation.gov.uk/ukpga/2003/44/contents> (accessed February 3, 2025).
14. The Public Prosecution Service v William Elliott and Robert McKee [2013] UKSC 32. URL: https://en.wikipedia.org/wiki/The_Public_Prosecution_Service_v_William_Elliott,_Robert_McKee (accessed February 3, 2025).
15. Federal Rules of Evidence. URL: https://www.uscourts.gov/sites/default/files/evidence_federal_rules_pamphlet_dec_1_2023.pdf (accessed February 3, 2025).
16. Guidelines for digital forensics first responders: Best practices for search and seizure of electronic and digital evidence. URL: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf (accessed February 3, 2025).
17. Sirius EU electronic evidence situation report 2024 (2024, November 28). URL: <https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2024> (accessed February 3, 2025).

Стаття надійшла 17.02.2025 р.

Y. V. Nedilko, PhD, Assistant Professor
Taras Shevchenko National University of Kyiv
Educational and Scientific Institute of Law
the Department of Criminal Procedure and Forensics
60 Volodymyrska St, Kyiv, 01033, Ukraine
e-mail: yaroslavnedilko@knu.ua
ORCID iD: <https://orcid.org/0000-0003-1483-3479>

DOCTRINE OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: NATIONAL FEATURES AND WORLD TRENDS

Summary

The article is devoted to the study of the place and photographs of electronic evidence in criminal proceedings. It is noted that with the advent of information and computer technology (smartphones, tablets, laptops, etc.), which criminals began to use for their illegal purposes, a new type of evidence began to appear – electronic evidence. Among domestic scientists there is no unity of opinion on the definition of the concept, place and electronic evidence in criminal proceedings. This is due not only to the lack of regulatory consolidation of electronic evidence in the Criminal Procedure Code of Ukraine (CPC of Ukraine), but also to the specification of their organization, research, seizure, storage and evaluation.

It is emphasized that the CPC of Ukraine does not contain a definition of the concept of “electronic evidence”, but it is given in the Code of Administrative Procedure of Ukraine (CAP of Ukraine), the Commercial Procedure Code (CPC of Ukraine) and the Civil Procedure Codes of Ukraine (CPC of Ukraine)

The article uses the concept of “electronic evidence after”, in international regulatory acts, in particular in acts of the European Union, the term electronic evidence (electronic evidence) is mainly used.

A comparative analysis of approaches to consolidation and regulation of electronic evidence in the legislation of foreign countries, in particular Latvia, Hungary, Singapore,

Great Britain and the USA, is presented. Both national and foreign judicial practice are given in detail.

Proposals have been made regarding the possible consolidation of electronic evidence in the criminal procedural legislation of Ukraine in two ways, namely: consolidation of the concept of electronic evidence in the Code of Criminal Procedure of Ukraine, establishing its definition and indicating what exactly can be attributed to electronic evidence and creating a separate law that will determine the procedure for research, collection, storage and analysis of electronic evidence. Establishment of clear and understandable procedures for the admissibility and admissibility of electronic evidence in criminal proceedings.

Keywords: electronic evidence, digital evidence, criminal proceedings, judicial investigation, admissibility of evidence, international experience, criminal process, judicial practice.