МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

СОЦІАЛЬНО-ПОЛІТИЧНА ТА ПРАВОВА СИСТЕМА УКРАЇНИ В ЦИФРОВУ ЕПОХУ: СУЧАСНІ ВИКЛИКИ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 22 квітня 2026 року

Том 1

Одеса
2026

УДК 34:004:316.4(477)
С 70

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 23.04.2026 р.)

За загальною редакцією академіка ***С. В. Ківалова***

С70 **Соціально-політична та правова система України в цифрову епоху**: сучасні виклики : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 22 квітня 2026 р.) / заг. ред. С. Ківалова ; НУ «Одес. юрид. академія». – Одеса : Фенікс, 2026. – Т. 1. – 704 с.

ISBN 978-617-8763-15-2

Матеріали конференції узагальнюють результати наукових досліджень і практичних напрацювань учених, фахівців та представників професійних спільнот, виконаних в умовах воєнного часу та глибоких суспільних трансформацій.

У збірнику представлено широкий спектр наукових розвідок і практико-орієнтованих досліджень, що охоплюють актуальні проблеми публічного та приватного права, функціонування держави, судової та правоохоронної системи, а також трансформації суспільних процесів у цифрову епоху. Значну увагу приділено питанням адміністративного, фінансового, конституційного, міжнародного, морського та митного права, а також сучасним викликам у сфері кримінального права, кримінального процесу, криміналістики та оперативно-розшукової діяльності.

Окремі наукові секції присвячені проблемам удосконалення судоустрою, діяльності прокуратури, адвокатури та інших правоохоронних органів, розвитку трудового права і права соціального забезпечення, а також реформуванню цивільного, господарського, земельного, екологічного та енергетичного права. Збірник відображає також міждисциплінарний характер сучасних досліджень, охоплюючи питання філософії права, світових соціально-політичних процесів, соціології та психології, економіки та підприємництва в умовах війни і повоєнного відновлення. Важливе місце посідають дослідження у сфері інформаційних технологій, кібербезпеки, штучного інтелекту та математичного моделювання як ключових чинників забезпечення національної безпеки.

Крім того, у збірнику висвітлено проблематику педагогіки, лінгвістики права, перекладознавства, журналістики, фізичної та військової підготовки здобувачів вищої освіти.

Збірник розрахований на науковців, викладачів, здобувачів вищої освіти та практиків у галузях права, економіки, соціології, психології, політології, інформаційних технологій і суміжних дисциплін.

УДК 34:004:316.4(477)

Відповідальний за випуск професор ***М. Р. Аракелян***

Матеріали видано в авторській редакції.

ISBN 978-617-8763-15-2

Колодіна Анна Сергіївна
Національний університет «Одеська юридична академія»,
доцент кафедри криміналістики, судових експертиз та поліграфології,
кандидат юридичних наук, доцент

МОЖЛИВОСТІ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ ПРИ ДОСЛІДЖЕННІ ЦИФРОВИХ ДОКАЗІВ

У зв'язку з цифровізацією суспільства, можна помітити як зростає кількість кримінальних правопорушень пов'язаних з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, ускладняються злочинні технології, що зумовлює необхідність удосконалення засобів розслідування такого виду кримінальних правопорушень. Кіберзлочини на сьогоднішній день є найдинамічнішою формою злочинних проявів.

За останній час інформаційні технології все більше впроваджуються в різні сфери суспільної діяльності та мають свої як переваги так і недоліки, не виключенням в цьому є і наука криміналістика, де стрімкий розвиток та динамічність нових видів кримінальних правопорушень вивів її на новий етап розвитку, завдяки якому з'явилась нова її галузь – цифрова криміналістика (digital forensics). Тому, з наведеного випливає, що переосмислення потребують ні тільки застарілі методи, способи та технології діяльності розслідування, а й система наукових знань, де з'являються нові теорії, які мають бути обґрунтованими та бути корисними за потреби практики.

З приводу питання місця цифрової криміналістики в системі знань класичної традиційної криміналістики, досі тривають конструктивні наукові дискусії. Одні вчені вважають, що цифрова криміналістика є галуззю криміналістичної техніки (Черемнова А. І.); інші вчені відносять її до галузі судових наук (більшість зарубіжних фахівців, Степанюк Р. Л., Перлін С. І.); як новий напрям у криміналістичній науці вважають такі вчені як: (В. М. Шевчук, В. В. Тіщенко, В. Ю. Шепітько та М. В. Шепітько, І. І. Когутич). Тому, це питання остаточно не вирішено і потребує подальших наукових пошуків.

У контексті дослідження цифрової криміналістики, після використання інформаціоно-комунікаційних технологій (ІКТ), залишаються цифрові сліди. Зокрема, особа, яка використовує ІКТ, може залишити «цифрові відбитки». Дані, залишені користувачами ІКТ, можуть розкрити відомості про них, включаючи інформацію про вік, стать, расову та етнічну приналежність, громадянство, сексуальну орієнтацію, думки, уподобання, звички, хобі, історію хвороби і проблеми зі здоров'ям, психологічні розлади, статус, зайнятість, приналежність до будь-якої спільноти, особисті відносини, геолокацію, розпорядок дня та інші активності [1].

Цифрові сліди – це будь-які криміналістично значущі дані, що залишаються в електронному середовищі внаслідок діяльності користувачів або систем (про-

грам), а також в результаті взаємодії з цифровими пристроями, призначеними для отримання та оброблення інформації в цифровій формі [2, с. 388]. Класифікувати цифрові сліди можна за наступними критеріями:

- за джерелом походження: сліди, що зберігаються на *жорстких дисках, SSD, флешках*; *мережеві сліди* (трафік IP, журнали доступу до сайтів); *мобільні сліди* (дзвінки, повідомлення, GPS, використання додатків); *хмарні сліди* (дані, збережені в Google Drive, iCloud тощо); *залишкові сліди в RAM* (актуальні під час експрес-аналізу);
- за характером виникнення: *свідомо створені*: документи, повідомлення, пости; *автоматично сформовані*: логи, технічні метадані, тимчасові файли;
- за доступом: *публічні сліди:* пости, коментарі в соціальних мережах; *приватні сліди:* внутрішні бази даних, зашифровані файли.

Даний перелік класифікаційних ознак не є вичерпним та потребує подальшого уточнення. В сучасних умовах цифровізації всі сфери життєдіяльності дедалі частіше стикаються з необхідністю дослідження цифрової інформації у кримінальному провадженні. При цьому особливого значення набуває правильна побудова алгоритму переходу від виявлення та первинного дослідження цифрової інформації до призначення та проведення комп'ютерно-технічної експертизи як джерела допустимих доказів.

З цього приводу влучно зазначають А. І. Черемнова, Л. С. Бєлік розглядаючи цифрову інформацію як об'єкт експертного дослідження, що «під цифровою інформацією в контексті розслідування кримінальних проваджень слід розуміти дані, представлені в електронній (цифровій) формі, що містять відомості, які мають значення для справи, містять сліди вчиненого кримінального правопорушення, були знаряддям чи засобом його вчинення, які зберігаються на матеріальних носіях інформації: комп'ютерних, мобільних пристроях, цифрових камерах, роутерах тощо – або нематеріальних ресурсах, як-от мережа Інтернет, локальні мережі установ та організацій тощо, при цьому на зазначених носіях інформації можуть міститися: файли (з текстовою інформацією, аудіо чи відео); різноманітне програмне забезпечення, що використовується як «знаряддя» вчинення злочину чи для приховання слідів його вчинення; файли, що містять сліди підробки чи фальсифікації; бази даних, вільний доступ до яких заборонено чинним законодавством у сфері охорони державної таємниці, захисту персональних даних тощо; скановані копії, фотокопії документів, обмежених для обігу тощо» [5, с. 60].

Цифрова інформація є джерелом цифрових доказів, які відіграють важливу роль при розслідуванні. Д. М. Цехан під цифровими доказами пропонує розуміти «фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому обов'язковою ознакою цифрового доказу є конвергентність, під якою розуміється здатність одиничного доказу входити у сукупність інших доказів і набувати у зв'язку з цим доказового значення» [4, с. 257].

Тому, цифрові сліди є об'єктом дослідження в рамках комп'ютерно-технічної експертизи і мають високе доказове значення в кримінальному провадженні. Для дослідження цифрових слідів призначають судову комп'ютерно-технічну експертизу, у якій виокремлюють такі види: експертиза комп'ютерної техніки (апаратно-комп'ютерна), експертиза програмних продуктів (програмно-комп'ютерна), інформаційно-комп'ютерна експертиза, комп'ютерно-мережева експертиза [3, с. 34].

Комп'ютерно-технічна експертиза (КТЕ) – це різновид судової експертизи, що передбачає дослідження комп'ютерної техніки, програмного забезпечення, даних на цифрових носіях з метою встановлення фактичних даних, що мають значення для кримінального провадження. Основною метою КТЕ є отримання об'єктивної та достовірної інформації, яка має значення для кримінального провадження, шляхом застосування спеціальних знань у сфері комп'ютерних технологій.

Ключовими завданнями такої експертизи є: 1) *ідентифікаційні завдання:* встановлення типу, моделі та технічних характеристик пристрою (комп'ютера, смартфона, флеш-накопичувача, тощо); визначення належності файлів до певного пристрою або користувача. 2) *діагностичні завдання:* встановлення структури збереженої інформації на носії; виявлення та відновлення видалених, зашифрованих або прихованих даних; аналіз логів (журналів подій), історії дій користувача, автозавантаження програм, мережевих підключень. 3) *Класифікаційні завдання:* визначення характеру, призначення та функціоналу виявленого програмного забезпечення; встановлення ознак використання пристрою для протиправної діяльності (фішинг, несанкціонований доступ, поширення забороненого контенту, тощо). 4) *Реконструктивні завдання:* відтворення послідовності подій на пристрої; визначення часу утворення змін, відкриття або видалення файлів; встановлення фактів копіювання, пересилання або завантаження даних. 5) *Аналітичні завдання:* порівняння виявлених об'єктів з еталонними зразками; встановлення взаємозв'язку між різними пристроями, обліковими записами або користувачами.

Отже, перспективи розвитку в даному аспекті дослідження є масштабні, а саме: динамічний розвиток технологій, які швидко розвиваються, шифрування даних і захист від несанкціонованого доступу, інтеграція штучного інтелекту, автоматизація процесів аналізу, співпраця з міжнародними цифровими лабораторіями, уніфікація стандартів цифрової експертизи та ін., тому має бути високий рівень технічного забезпечення експертних установ в даному напрямку.

Список використаних джерел:

1. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. № 1. С. 176–180. URL: https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/151/139

2. Криміналістика : підручник / В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін. ; за ред. В. М. Шевчука ; Нац. Юрид. ун-т ім. Ярослава Мудруго. Харків: Право, 2024. 1008 с.

3. Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні: навч. посіб. Львів : держ. Ун-т внутр. Справ, 2022. С. 34–45.

4. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2013. № 5. С. 256–260.

5. Черемнова А. І., Бєлік Л. С. Цифрова інформація як об'єкт експертного дослідження в умовах діджиталізації: проблеми та перспективи розвитку. *Криміналістика і судова експертиза*. 2023. Вип. 68. С. 57–65.

Ключові слова: цифрова криміналістика, цифрові докази, спеціальні знання, комп'ютерно-технічна експертиза, кіберзлочинність, цифрові сліди, цифрова інформація.

Key words: digital forensics, digital evidence, specialized knowledge, computer forensics, cybercrime, digital traces, digital information.

Чернов Олександр Віталійович

Національний університет «Одеська юридична академія», доцент кафедри криміналістики, судових експертиз та поліграфології, доктор філософії з галузі знань 08 «Право»

ВИКОРИСТАННЯ ДАНИХ СУДОВОЇ ЕНТОМОЛОГІЇ У КРИМІНАЛІСТИЧНІЙ ПРАКТИЦІ ДЛЯ ВСТАНОВЛЕННЯ ЧАСУ НАСТАННЯ СМЕРТІ

Використання даних судової ентомології у криміналістичній практиці для встановлення часу настання смерті є одним із найбільш науково обґрунтованих та перспективних напрямів розвитку сучасної судово-медичної та криміналістичної науки, що ґрунтується на інтеграції біологічних, екологічних, медичних і правових знань. У сучасних умовах ускладнення криміногенної ситуації, підвищення рівня організованості злочинних груп, а також застосування злочинцями різноманітних способів маскування злочинів, питання точного встановлення часу настання смерті набуває особливого значення. Традиційні методи судово-медичної діагностики давності смерті, такі як аналіз трупних плям, трупного задубіння, ступеня розкладання тканин, температури тіла, мають обмежену ефективність, особливо у випадках значного постмортального інтервалу або впливу зовнішніх факторів. У таких умовах судова ентомологія виступає як альтернативне та водночас високоточне джерело криміналістично значущої інформації.

Сутність судової ентомології полягає у вивченні закономірностей заселення трупа комахами, їх видового складу, динаміки розвитку та взаємодії з середовищем. Біологічною основою цього напряму є те, що після настання смерті організм людини стає специфічним екологічним субстратом, який приваблює різні види комах, передусім некрофагів. Найбільш важливими у криміналістично-