МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

КАЛАНЧА ІНГА ГЕОРГІЇВНА

УДК 343.14:004(477)

ДОКАЗИ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ: ТЕОРІЯ ТА ПРАКТИКА

12.00.09 – кримінальний процес та криміналістика;
судова експертиза; оперативно-розшукова діяльність

Реферат дисертації на здобуття наукового ступеня
доктора юридичних наук

Київ – 2025

Дисертацією є рукопис

Робота виконана в Національній академії внутрішніх справ,
Міністерство внутрішніх справ України

Офіційні опоненти:
доктор юридичних наук, професор
Гусєва Влада Олександрівна,
Харківський національний університет внутрішніх справ,
завідувач кафедри криміналістики та судової експертології
навчально-наукового інституту №1;

доктор юридичних наук, професор
Колесник Валерій Аркадійович,
Національна академія Служби безпеки України,
головний науковий співробітник науково-організаційного центру;

доктор юридичних наук, професор
Цехан Дмитро Миколайович,
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри
оперативно-розшукової та поліцейської діяльності

Захист відбудеться «19» грудня 2025 року о 09 год. на засіданні спеціалізованої вченої ради Д 26.007.03 у Національній академії внутрішніх справ за адресою: 03035, м. Київ, пл. Солом'янська, 1

З дисертацією можна ознайомитись у бібліотеці Національної академії внутрішніх справ за адресою: 03035, м. Київ, пл. Солом'янська, 1

Учений секретар
спеціалізованої вченої ради **Андрій АНТОЩУК**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Глибокі трансформації, що відбуваються під впливом цифровізації суспільних відносин, зумовлюють докорінне переосмислення доктрини кримінального процесуального доказування. Сьогодні чимало інформації, що може мати доказове значення у кримінальному провадженні, існує в електронній формі – у вигляді цифрових даних, записів комунікацій, інформації з технічних пристроїв, мережевих ресурсів та електронних систем. Зазначене об'єктивно висуває перед правовою наукою і практикою завдання формування нового концептуального підходу до розуміння, класифікації та використання доказів електронної форми під час кримінального провадження.

На відміну від традиційних матеріальних джерел доказової інформації, електронні дані характеризуються нестабільністю, можливістю несанкціонованої модифікації, складністю перевірки їх автентичності та цілісності, ризиком випадкової втрати. Вони водночас є носіями як змістовної, так і технічної інформації, що спричиняє необхідність поєднання правових, криміналістичних та інформаційно-технологічних підходів до їх аналізу. Ось чому проблеми визначення процесуальної природи доказів електронної форми, порядку їх фіксації, зберігання, перевірки та процесуальної оцінки набувають стратегічного значення для забезпечення законності й ефективності кримінального провадження.

У чинному кримінальному процесуальному законодавстві України досі бракує чіткої регламентації процедури обігу доказів електронної форми, а це породжує неоднакове їх розуміння та застосування в практиці органів досудового розслідування, прокуратури й суду.

Теоретичною базою дисертаційного дослідження є праці у сфері доказів та доказування таких вітчизняних науковців як О. В. Баганець, В. В. Вапнярчук, В. П. Гмирко, Ю. М. Грошевий, О. В. Капліна, Є. Г. Коваленко, С. О. Ковальчук, Г. Р. Крет, М. М. Михеєнко, В. Т. Нор, М. А. Погорецький, Д. Б. Сергєєва, В. А. Смирнов, О. С. Старенький С. М. Стахівський, В. Я. Тацій, О. Г. Шило, М. Є. Шумило, О. Г. Яновська а також роботи інших вчених-процесуалістів.

У сфері вітчизняного кримінального процесу загальнотеоретичні питання доказів електронної форми досліджували Д. О. Алєксєєва-Процюк, М. В. Багрій, О. М. Брисковська, Г. П. Власова, С. І. Гонгало, М. І. Демура, О. В. Капліна, А. В. Коваленко, С. О. Ковальчук, О. Г. Козицька, Д. І. Клепка, В. В. Мурадов, М. А. Погорецький, Д. Б. Сергєєва, О. В. Сіренко, А. В. Скрипник, І. А. Смаль, О. С. Старенький, А. В. Столітній, В. М. Тертишник, Л. Д. Удалова, Т. Г. Фоміна, В. Г. Хахановський, Є. С. Хижняк та інші. Відомі прикладні розробки таких науковців, як А. О. Антощук, Н. М. Ахтирська, І. В. Гловюк, І. В. Гора, А. В. Гутник (Ратнова), В. А. Колесник, І. О. Крицька, О. П. Метелев, Д. І. Овсянюк, Ю. Ю. Орлов, М. І. Пашковський, І. А. Тітко, О. О. Торбас, Д. М. Цехан, С. С. Чернявський та інші.

Особливу актуальність тема набуває у контексті імплементації міжнародних стандартів у сферу доказів електронної форми. Конвенція про кіберзлочинність та Другий додатковий протокол до неї закріплюють основи міжнародного

співробітництва у сфері збирання й передання доказів електронної форми. Європейський Союз у 2023 році ухвалив низку нормативно-правових актів, що визначають уніфіковані підходи до надання, збереження та збору доказів електронної форми під час кримінального провадження. Для України, яка прагне інтегруватися у єдиний європейський простір, адаптація цих положень є не лише науково, а й політично важливою.

Сучасні виклики – зокрема, воєнний стан, зростання кіберзлочинності, масове використання інформаційно-комунікаційних технологій у публічній і приватній сферах – вимагають побудови цілісної системи правового регулювання доказів електронної форми у кримінальному процесі України. У цьому контексті наукове осмислення правової природи таких доказів, формулювання їх доктринального обґрунтування, визначення критеріїв автентичності та цілісності, а також розроблення ефективних процесуальних і технічних механізмів роботи з ними набуває першорядного значення для подальшого розвитку кримінальної процесуальної науки та вдосконалення національного законодавства.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до абз. 11, 13, 15 розділу «Протидія злочинності» Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року, схваленої розпорядженням Кабінету Міністрів України від 15 листопада 2017 р. № 1023-р; § 4 Розділу 4 Національної стратегії у сфері прав людини, затвердженої Указом Президента України від 24 березня 2021 р. № 119/2021; п. 4.1.4 Розділу I Стратегії розвитку системи правосуддя та конституційного судочинства на 2021–2023 рр., затвердженої Указом Президента України від 11 червня 2021 р. № 231/2021; цілей С. 2 та С. 3 розділів 5 та 6 Стратегії кібербезпеки України, схваленої рішенням Ради національної безпеки і оборони України від 14 травня 2021 р. та уведеної в дію Указом Президента України від 26 серпня 2021 р. № 447/2021; п.п. 10, 16, 26 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 р. та уведеного в дію Указом Президента України від 1 лютого 2022 р. № 37/2022; п.п. 5.1–5.9 Розділу II Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 рр., схваленого Указом Президента України від 11 травня 2023 р. № 273/2023; розділу «Інформаційні та комунікаційні технології» Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затвердженого постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476; п.п. 2.7, 3.1.1, 3.1.2, 3.2, 3.3, 3.3.1–3.3.4, 4.5, 4.6 Стратегії розвитку прокуратури на 2025–2028 рр., затвердженої наказом Генерального прокурора № 322 від 8 жовтня 2025 р.

Тему дисертації затверджено рішенням Вченої ради Національної академії внутрішніх справ 24 червня 2025 року (протокол № 16/4-3).

Мета і задачі дослідження. *Метою* дисертації є теоретико-правове узагальнення та розв'язання комплексної наукової і прикладної проблеми формування цілісної концепції доказів електронної форми у кримінальному процесі України.

Для досягнення зазначеної мети поставлено такі *задачі*:

– дослідити вітчизняні доктринальні підходи до розуміння доказів та їх властивостей у кримінальному процесі України в контексті формування науково-теоретичної основи для доказів електронної форми;

– сформулювати теоретико-методологічні засади дослідження доказів електронної форми як складової кримінального процесу України;

– дослідити історичний розвиток теоретичних підходів до доказів електронної форми у кримінальному процесі України;

– визначити місце доказів електронної форми в системі процесуальних джерел доказів у кримінальних провадженнях, охарактеризувати їх процесуальну та технічну природу;

– запропонувати алгоритми пошуку та фіксації доказів електронної форми в кримінальному процесі України;

– розробити методику підтвердження автентичності та цілісності доказів електронної форми в кримінальному процесі України;

– систематизувати підходи до організації роботи з доказами електронної форми в системі органів кримінальної юстиції України;

– визначити й деталізувати повноваження слідчого як суб’єкта роботи з доказами електронної форми у кримінальному провадженні;

– охарактеризувати особливості процесуальної діяльності прокурора щодо збирання та оцінки доказів електронної форми у кримінальному провадженні;

– охарактеризувати специфіку діяльності захисника при роботі з доказами електронної форми у кримінальному провадженні;

– установити процесуальні повноваження судді та слідчого судді при дослідженні доказів електронної форми у кримінальному провадженні;

– охарактеризувати особливості участі інших учасників кримінального провадження при роботі з доказами електронної форми: експерта, спеціаліста в сфері цифрової криміналістики, спеціаліста в сфері OSINT;

– сформулювати пропозиції щодо використання Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations) як методологічної основи фіксації інформації з відкритих джерел під час кримінального провадження;

– визначити особливості процесуальних механізмів, визначених Конвенцією про кіберзлочинність щодо роботи з доказами електронної форми у кримінальному провадженні;

– розкрити специфіку ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» як методологічної складової щодо роботи з доказами електронної форми під час кримінального провадження;

– узагальнити зарубіжний досвід роботи з доказами електронної форми та міжнародну практику використання електронних інформаційних систем для міжнародного обміну доказами під час кримінального провадження;

– виокремити засади організації роботи з доказами електронної форми у кримінальному процесі України;

– розкрити процесуальні аспекти роботи з доказами електронної форми у

кримінальному процесі України;

– підготувати пропозиції щодо вдосконалення технічних аспектів роботи з доказами електронної форми у кримінальному процесі України;

– сформулювати концептуальне бачення щодо подальшого удосконалення інституту доказів електронної форми у кримінальному процесі України.

Об'єкт дослідження – суспільні відносини, що виникають у процесі кримінального провадження під час пошуку, фіксації, перевірки, оцінки та використання доказів електронної форми, а також механізми їх процесуального обігу в системі кримінальної юстиції України.

Предмет дослідження – докази електронної форми у кримінальному процесі України.

Методи дослідження. Для досягнення поставленої мети та вирішення обумовлених нею задач використовувались такі методи:

– *діалектичний* – для з'ясування сутності, змісту та закономірностей розвитку доказів електронної форми у кримінальному процесі в динаміці становлення інформаційного суспільства та цифровізації кримінальної юстиції (розділи 1, 2, 5); його застосування дозволило визначити внутрішні суперечності між технічною природою електронних даних і традиційними процесуальними механізмами доказування;

– *системний аналіз* – сприяв аналізу взаємодії процесуальних, організаційних та технічних складників механізму роботи з доказами електронної форми, що дозволило сформувати концептуальну модель їх процесуального статусу та обігу (розділи 1–5);

– *структурно-функціональний* – для виявлення взаємозв'язку елементів системи процесуального регулювання доказів електронної форми, їх місця у системі процесуальних джерел доказів, а також для розмежування понять і категорій (розділи 1–3);

– *історико-правовий* – для дослідження етапів формування уявлень про докази електронної форми (підрозділ 1.1 та 1.3), ґенези становлення та розвитку нормативних підходів до їх використання у кримінальному процесі, починаючи від перших спроб легалізації цифрових даних до сучасного етапу впровадження електронних систем правосуддя (розділи 1, 2);

– *компаративістський* – дав змогу здійснити порівняльний аналіз зарубіжного досвіду регламентації доказів електронної форми, насамперед у контексті імплементації положень Конвенції про кіберзлочинність, Другого додаткового протоколу до неї та законодавства Європейського Союзу в національну правову систему (розділ 4);

– *логіко-юридичний* – для формулювання авторських дефініцій ключових понять і для обґрунтування пропозицій щодо вдосконалення їх процесуального регулювання (розділи 1–3, 5);

– *формально-юридичний* – для аналізу норм чинного КПК України, законів України та підзаконних нормативно-правових актів, практики їх застосування органами досудового розслідування, прокуратури та суду (розділи 2–5);

– *моделювання* – дозволив розробити пропозиції щодо вдосконалення роботи з доказами електронної форми у кримінальному процесі України

(розділ 5);

– *статистичний* – під час аналізу результатів емпіричного дослідження, що включало узагальнення практики органів досудового розслідування, судів, прокуратури та адвокатури щодо роботи з доказами електронної форми (розділи 2–3);

– *соціологічний* – для отримання емпіричних даних про стан застосування доказів електронної форми у кримінальному провадженні, рівень цифрової компетентності слідчих, прокурорів, суддів і адвокатів, а також для виявлення проблем правозастосування (розділи 2-4).

Дослідження ґрунтується на інтеграції кримінальної процесуальної теорії доказів з положеннями цифрової криміналістики, правової інформатики та кібербезпеки. Це забезпечило комплексне розкриття правової природи доказів електронної форми з формуванням нових теоретико-методологічних положень щодо їх ідентифікації, збирання, зберігання, перевірки та оцінки в умовах цифровізації правосуддя.

Емпіричну базу дослідження становлять: зведені дані вивчення 350 кримінальних проваджень упродовж 2018–2025 рр.; 450 ухвал, постанов та вироків судів України усіх регіонів; 30 рішень Європейського суду з прав людини; результати опитування 1301 респондента, серед яких: 128 суддів, 574 прокурори, 100 адвокатів, 146 слідчих та детективів, 174 співробітники оперативних підрозділів, 59 судових експертів та ІТ-фахівців, що виконують функції спеціалістів під час кримінального провадження, 120 науковців; статистичні та аналітичні звіти й узагальнення Верховного Суду, Національної поліції України, Офісу Генерального прокурора, Ради Європи.

Наукова новизна одержаних результатів полягає в тому, що дисертація є першим в Україні комплексним дисертаційним дослідженням, в якому реалізовано доктринальний підхід до формування цілісної концепції доказів електронної форми у кримінальному процесі України з визначенням шляхів розв’язання низки фундаментальних і праксеологічних проблем удосконалення правових, організаційних, процедурних і технічних засад їх формування, перевірки, оцінювання та використання. Найсуттєвішими з них є такі положення:

вперше:

– запропоновано цілісне бачення електронної складової кримінального процесу України, що містить п’ять елементів: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми; електронні інструменти доказування; електронні інструменти реалізації повноважень суб’єктів правозастосування. Обґрунтовано інституційну самостійність доказів електронної форми у кримінальному процесі України, що обумовлює формування їх належної теоретичної та нормативної основи. У цьому напрямі розмежовано понятійний апарат в межах ключових для практики правозастосування категорій: «джерело доказів», «документ», «електронний документ», «носії інформації», «комп’ютерні дані» тощо. Дано визначення понять «електронні докази», «докази електронної форми» та «цифрові докази» і обґрунтовано підхід до використання термінів, за якого «цифровий доказ» відповідає змісту доказу, «електронний доказ» –

технічному способу його реалізації, а «доказ електронної форми» – процесуальній формі подання;

– сформульовано комплекс алгоритмів пошуку та фіксації доказів електронної форми, що об'єднаний за трьома функціонально-структурними категоріями і виступає як три самостійні стратегії фіксації доказів електронної форми у кримінальному процесі України: 1) фізичне вилучення електронних носіїв інформації або комп'ютерних систем; 2) огляд та копіювання комп'ютерних даних; 3) огляд та фіксація інформації з відкритих джерел. Запропонований підхід (у межах перших двох стратегій) визначає пріоритет огляду та копіювання комп'ютерних даних, здійснених з дотриманням вимог ч. 4 ст. 99 КПК України (за участю спеціаліста) та норм ДСТУ ISO/IEC 27037:2017, процесуально та технологічно допустимою альтернативою фізичному вилученню технічних пристроїв, здатною забезпечити завдання доказування. Запропоновано алгоритм здобуття високоінформативних доказів електронної форми, що поєднує національні та міжнародні процедури й передбачає: 1) фіксацію відомостей з відкритих джерел у порядку ч. 4 ст. 99, ст. 237 або ст. 240 КПК України (фіксація публічно доступних даних); 2) скерування запиту про термінове збереження комп'ютерних даних в порядку ст.ст. 16, 29 або 17, 30 Конвенції про кіберзлочинність (зберігання даних та отримання оперативної інформації щодо публічно недоступного сегменту відомостей); 3) скерування запиту про міжнародну правову допомогу в порядку ст. 551 КПК України для отримання даних, збережених відповідно до механізмів Конвенції про кіберзлочинність (отримання повних відомостей від держателя даних, що є процесуально допустимими доказами);

– обґрунтовано методику підтвердження автентичності та цілісності доказів електронної форми в кримінальному процесі України, засновану на техніко-криміналістичних (ДСТУ ISO/IEC 27037:2017) інструментах ідентифікації комп'ютерних даних і процесуальних (абз. 3 п. 3 ч. 3 ст. 104 КПК України) вимогах послідовної фіксації й перевірки таких ідентифікаторів, контролю доступу та забезпечення безпеки доказів. У межах відповідної методики запропоновано багаторівневу систему, диференційовану за ступенем зростання рівня надійності методів, що включає: 1) упакування та маркування електронних носіїв інформації; 2) фіксацію загальних та унікальних апаратних ідентифікаторів; 3) опис структури і змісту комп'ютерних даних та їх метаданих; 4) гешування комп'ютерних даних і послідовної фіксації контрольних сум комп'ютерних даних у процесуальних документах; 5) фіксацію стану доказу електронної форми у визначений часовий період за допомогою КЕП з електронною позначкою часу; 6) фіксацію ланцюга збереження доказів (chain of custody) в порядку ДСТУ ISO/IEC 27037:2017. Обґрунтовано необхідність розроблення та впровадження стандартних операційних процедур (СОП) щодо роботи з доказами електронної форми, заснованих на ДСТУ ISO/IEC 27037:2017, ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27002:2023, закріплення практики фіксації ланцюга збереження доказів (chain of custody);

– сформульовано наукове бачення місця та ролі ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови

для ідентифікації, збирання, здобуття та збереження цифрових доказів» як методологічної основи технічного аспекту роботи з доказами електронної форми під час кримінального провадження на етапах їх ідентифікації, збирання, здобуття та збереження. Обґрунтовано необхідність його системного вивчення суб'єктами кримінального провадження, що здійснюють збирання та здобуття доказів електронної форми (впровадження процесуальної ролі Digital Evidence First Responder з релевантними вимогами до кваліфікації), впровадження в практику правозастосування та нормативну інституціоналізацію у відомчих нормативно-правових актах та стандартних операційних процедурах (СОП);

– сформульовано процесуальні аспекти вдосконалення роботи з доказами електронної форми у кримінальному процесі України: вдосконалення правового регулювання та імплементації положень Конвенції про кіберзлочинність; ДСТУ ISO/IEC 27037:2017 та Протоколу Берклі, що передбачає внесення системних змін до КПК України; зміни до законів України щодо зберігання інформації операторами телекомунікації, вимог до спеціалізації представників органів досудового розслідування, прокурорів та суддів, їх спеціалізації; прийняття міжвідомчого підзаконного нормативно-правового акту щодо взаємодії органів досудового розслідування та органів прокуратури з національним контактним пунктом 24/7; прийняття суб'єктами кримінального провадження відомчих актів щодо організації роботи з доказами досліджуваної категорії – стандартних операційних процедур (СОП);

– розроблено концептуальні підходи до вдосконалення інституту доказів електронної форми у кримінальному процесі України, що включають: 1. Загальні положення. 2. Нормативний напрям: оновлення термінології КПК України; автентичність і цілісність; розмежування збирання та здобуття; OSINT; термінове збереження й аналіз даних про рух інформації; захист приватності та обмеження втручання. 3. Організаційний напрям: ефективна взаємодія між суб'єктами кримінального провадження; системні рішення щодо посилення кадрового потенціалу; створення сталого каналу міжвідомчої співпраці з провайдерами телекомунікації. 4. Інфраструктурний напрям: створення інтегрованої системи управління доказами; побудова цифрової інфраструктури для обміну даними між органами досудового розслідування, прокуратури та провайдерами телекомунікації, налагодження цифрової форми виконання ухвал про тимчасовий доступ до речей і документів. 5. Техніко-криміналістичний напрям: належне матеріально-технічне забезпечення органів досудового розслідування, прокуратури та суду; стандартизація форматів зберігання доказів електронної форми, методів ідентифікації, запровадження практики резервного копіювання, використання надійних електронних носіїв інформації, здатних забезпечити довготривале зберігання даних; криптографічне шифрування даних. 6. Освітній напрям: впровадження у вищих навчальних закладах юридичного та правоохоронного профілів компетентностей щодо роботи з доказами електронної форми; підвищення кваліфікації суб'єктів кримінального провадження; формування вимог щодо обов'язкових міждисциплінарних цифрових компетентностей. 7. Науково-аналітичний напрям: розширення та інституційна підтримка наукових досліджень за відповідною тематикою щодо вирішення

актуальних практичних завдань та вдосконалення практики правозастосування; здійснення прикладних наукових досліджень; забезпечення систематичного моніторингу практики. 8. Очікувані результати та строки реалізації;

удосконалено:

– положення щодо місця доказів електронної форми в системі процесуальних джерел доказів у кримінальному процесі України, що полягає у можливості їх потенційної належності до всіх процесуальних джерел доказів, визначених ст. 84 КПК України. Обґрунтовано, що факт належності доказу досліджуваної категорії до певного процесуального джерела визначає процесуальний порядок поводження з ними під час кримінального провадження та, як наслідок, критерії оцінки його допустимості. Електронна форма фіксації показань, у контексті ст. 225, ч. 11 ст. 615 КПК України, висуває додаткові вимоги до автентифікації допитуваної особи, збереження результатів технічної фіксації, підтвердження автентичності та цілісності. Обґрунтовано, що документами докази досліджуваної категорії визначаються через призму п. 1 та п. 3 ч. 2 ст. 99 КПК України, а також через призму електронних документів **(**у розумінні профільного закону), тоді як речові докази репрезентовані фізичними об'єктами, наділення яких відповідним статусом обумовлене потребою встановлення належного правового режиму при їх вилученні та подальшим арештом. Висновок експерта електронної форми потребує обов'язкового підписання кваліфікованим електронним підписом, забезпечення належного процесуального способу отримання, підтвердження автентичності та відтворюваності змісту. Доказ електронної форми варто розглядати як чотирирівневу структуру, що містить контент, метадані, системну оболонку та електронний носій інформації, який має матеріальне вираження. Запропоновано класифікацію електронних носіїв інформації та обґрунтовано вплив відповідних характеристик на прийняття процесуальних рішень щодо пріоритизації фіксації нестабільних даних, вилучення технічних пристроїв, арешту майна тощо. Доведено, що гешування забезпечує відтворювану ідентифікацію цифрового об'єкта та виявлення будь-яких змін, слугуючи технічною основою для підтвердження цілісності та незмінності доказів електронної форми. Технічні характеристики доказів електронної форми, що здатні підтвердити автентичність та цілісність зафіксованих цифрових даних, в сукупності з застосовуваними належними кримінальними процесуальними процедурами, становлять дуалістичну основу процесуальної допустимості доказів електронної форми у кримінальному провадженні;

– процесуальні та організаційні повноваження слідчого як суб'єкта роботи з доказами електронної форми у кримінальному провадженні, що вимагають поєднання правових навичок із базовою цифровою грамотністю. Відповідні повноваження слідчого деталізовано в частині прийняття рішення щодо способу фіксації доказів електронної форми (здобуття – копіювання інформації чи збирання – вилучення носія інформації), вибору ідентифікаційних параметрів комп'ютерних даних та їх відображення у протоколах слідчих (розшукових) дій, залучення спеціаліста;

– процесуальні засади діяльності прокурора щодо роботи з доказами

електронної форми у кримінальному провадженні як ключового суб'єкта, що поєднує координацію дій оперативних підрозділів, дізнавача, слідчого, залучення спеціаліста, контроль за дотриманням критеріїв належності, допустимості й достовірності. Відповідні повноваження прокурора деталізовано в частині перевірки автентичності електронних документів і електронних підписів, організації відкриття матеріалів досудового розслідування стороні захисту відповідно до ст. 290 КПК України, використання механізмів міжнародної взаємодії, інтеграції доказів електронної форми у структуру обвинувачення, забезпечення підтвердження цілісності даних, джерела походження та зв'язку з юридично значущими обставинами. Запропоновано методологію оцінки процесуальних та технічних аспектів доказів електронної форми, на основі якої розроблено відповідні методичні документи;

– бачення процесуальної діяльності сторони захисту при роботі з доказами електронної форми у кримінальному провадженні як самостійного суб'єкта доказової діяльності щодо їх фіксації та представлення. Забезпечення ефективної реалізації останньої розглядається через поєднанням процесуальної активності з технічною спроможністю підтвердити автентичність і цілісність комп'ютерних даних, дотримуючись стандарту доказування. Відповідні повноваження захисника деталізовано в контексті реалізації під час обшуку й доступу до матеріалів досудового розслідування (ст. 290 КПК України), щодо яких пріоритизовано мінімізацію втручання у приватне життя, охорону адвокатської таємниці, отримання доступу до криміналістичних (побітових) копій електронних носіїв інформації та їх ідентифікаторів, а також ефективне реагування на процесуальні порушення;

– наукове обґрунтування процесуальних повноважень та компетентностей судді та слідчого судді при дослідженні доказів електронної форми у кримінальному провадженні, що вимагає з'ясування відповідними суб'єктами низки техніко-правових критеріїв, серед яких: наявність у процесуальних документах геш-ідентифікаторів комп'ютерних даних і їх збіг з ідентифікаторами досліджуваних доказів, перевірюваність метаданих, електронних підписів і електронних позначок часу, відповідність процедур ідентифікації, збирання, здобуття та зберігання стандартам ДСТУ ISO/IEC 27037:2017; перевірка автентичності матеріалів з відкритих джерел та процесуального порядку здобуття доказів електронної форми, одержаних в порядку міжнародної правової допомоги. Обґрунтовано необхідність надання переваги криміналістичним (побітовим) копіям як об'єктам аналізу, тоді як дослідження оригінального технічного пристрою допустиме лише за умов, що не створюють ризику цілісності доказу;

– наукові засади використання рекомендацій Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations) як методологічної основи фіксації інформації з відкритих джерел під час кримінального провадження. Встановлено співвідношення положень п. 155 Протоколу Берклі з вимогами КПК України і запропоновано підхід до відображення відповідних відомостей в протоколі огляду кіберпростору;

– теоретико-прикладні засади реалізації процесуальних механізмів,

визначених Конвенцією про кіберзлочинність щодо роботи з доказами електронної форми у кримінальному провадженні: 1) встановлення норм, що знайшли відображення в КПК України: поширення обшуку за межі комп'ютерної системи, яка є об'єктом первинного втручання (ч. 2 ст. 19 Конвенції) – абз. 2 ч. 6 ст. 236 КПК України; 2) норм, що не імплементовані, але які можуть бути реалізовані за допомогою існуючих процедур: термінове збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29), та порядок представлення (ст. 18) – частково через тимчасовий доступ до речей і документів (Глава 15 КПК України), перехоплення змісту даних, що передаються (ст. 21 Конвенції) – ст.ст. 263, 264 КПК України; 3) прогалин, що потребує внесення змін до КПК України: термінове збереження і часткове розкриття даних про рух інформації (ст.ст. 17, 30), збирання даних про рух інформації у режимі реального часу (ст. 20); добровільне надання інформації (ст. 26);

дістало подальший розвиток:

– дослідження вітчизняних доктринальних підходів до розуміння доказів та їх властивостей у кримінальному процесі України, реалізоване в контексті формування науково-теоретичної основи доказів електронної форми, де електронна форма визначається характеристикою існування й подання фактичних даних у межах існуючих чотирьох видів (процесуальних джерел) доказів. Технологічний елемент і технічні характеристики доказів електронної форми визначено релевантними характеристиками, що впливають на такі властивості доказів як допустимість та достовірність;

– дослідження історичного розвитку теоретичних підходів щодо доказів електронної форми у кримінальному процесі України, яке засвідчило, що: становлення відповідного інституту характеризується конкуренцією доктринальних підходів (від ототожнення з документами чи речовими доказами до пропозицій їх виокремлення як самостійного процесуального джерела доказів) та значною термінологічною варіативністю; зумовлене технологічним розвитком, що збільшив обсяг електронних даних у кримінальних провадженнях, та внутрішньою потребою кримінальної процесуальної науки висвітлити власне бачення нової цифрової реальності. Обґрунтовано доцільність стриманого підходу щодо нормативного регулювання доказів електронної форми (без визнання самостійним процесуальним джерелом) та потреби застосування комплексного та технологічно орієнтованого підходу, що не дестабілізує систему кримінальної юстиції;

– узгоджені підходи до організації роботи з доказами електронної форми в системі органів кримінальної юстиції України через призму організаційної готовності суб'єктів кримінального провадження як три взаємопов'язані компоненти: 1) матеріально-технічний – забезпечення цифровими криміналістичними інструментами та інфраструктурою, сумісною з ДСТУ ISO/IEC 27037:2017; 2) кадровий – функціонування в структурі органів досудового розслідування криміналістичних ІТ-лабораторій, міждисциплінарною компетентністю суб'єктів кримінального провадження, їх профільною спеціалізацією та системним підвищенням кваліфікації; 3) нормативний – використанням єдиних стандартів роботи з доказами досліджуваної категорії,

забезпечення їх надійного зберігання та контролю доступу;

– обґрунтування підстав та алгоритмів залучення під час кримінального провадження спеціаліста в сфері цифрової криміналістики в ролі Digital Evidence First Responder з метою ідентифікації, збирання, здобуття, збереження відповідно до ДСТУ ISO/IEC 27037:2017 із процесуальною цифрових слідів без проведення експертного дослідження. Водночас процесуальну роль експерта пропонується зосереджувати на комплексних дослідженнях, що оптимізує навантаження експертних установ і скоротить строки проведення експертних досліджень;

– підходи до впровадження зарубіжного досвіду роботи з доказами електронної форми, результатами аналізу якого встановлено такі загальні тенденції: інституціоналізація правового режиму доказів електронної форми у межах кримінального процесуального законодавства; утвердження технологічно нейтрального підходу до їх оцінки та допустимості (відсутність вимог визначених технічних засобів чи форматів); посилення вимог до автентичності, цілісності й простежуваності; запровадження спеціальних процесуальних механізмів для їх збирання, збереження та перевірки; уніфікація національних підходів із міжнародними стандартами. У зв’язку з цим у сфері міжнародного обміну доказами електронної форми пропонується: 1) створення комплексної та надійної системи їх захисту; 2) зокрема, розроблення й уніфікація стандартних протоколів та процедур для гармонізації правових аспектів обміну доказами електронної форми між різними юрисдикціями; впровадження сучасних систем управління доказами, що забезпечують автоматизовану фіксацію, відстеження та аналіз усіх взаємодій з ними;

– пропозиції щодо вдосконалення організаційних засад роботи з доказами електронної форми у кримінальному процесі України, що передбачає, зокрема уніфікацію підходів до підготовки юридичних та правоохоронних кадрів на рівні вищих навчальних закладів юридичного та правоохоронного профілів; створення криміналістичних ІТ-лабораторій у структурі правоохоронних органів; результативне професійне навчання суб’єктів кримінального провадження (підвищення кваліфікації), зокрема запровадження міжвідомчих програм підвищення кваліфікації; посилення взаємодії між суб’єктами кримінального провадження – узгодженість у процесуальних діях, обмін знаннями та ресурсами, залучення спеціалістів і створення сталих каналів комунікації між слідчими, прокурорами, спеціалістами, експертами та судом, модернізацію процедури здійснення тимчасового доступу до речей і документів;

– підходи до вдосконалення технічних аспектів роботи з доказами електронної форми у кримінальному процесі України, що передбачає створення комплексної системи забезпечення цілісності, конфіденційності та збережуваності доказів електронної форми: запровадження гешування як механізму підтвердження цілісності доказів електронної форми; врегулювання практики використання електронних процесуальних документів; впровадження практики резервного копіювання доказів досліджуваної категорії, використання надійних електронних носіїв інформації під час фіксації, здатних забезпечити довготривале зберігання даних; криптографічне шифрування цифрових даних, що є доказами; створення відомчих віртуальних сховищ (цифрових архівів) для

зберігання резервних копій доказів електронної форми.

Практичне значення одержаних результатів. Обґрунтовані в дисертації положення впроваджені й можуть бути використані у:

науково-дослідній роботі – для подальших наукових досліджень проблем доказів електронної форми у кримінальному процесі України (акти Національної академії внутрішніх справ від 10.07.2025, Київського столичного університету імені Бориса Грінченка від 16.10.2025, ПВНЗ «Європейський Університет» від 20.10.2025);

законотворчій діяльності – шляхом внесення проєктів змін та доповнень до Кримінального процесуального кодексу України та інших законодавчих актів на основі розроблених автором законопроєктів (лист Комітету Верховної Ради України з питань правоохоронної діяльності від 13.11.2025);

діяльності органів кримінальної юстиції – для розроблення та удосконалення відомчих (міжвідомчих) нормативно-правових актів, підготовки методичних рекомендацій з питань доказів електронної форми у кримінальному процесі (акт Департаменту кіберполіції Національної поліції України від 13.11.2025, лист Офісу Генерального прокурора від 21.11.2025);

освітньому процесі – для підготовки наукових, навчальних та науково-практичних тестових завдань і дидактичних матеріалів з курсів кримінального процесуального права та в системі підвищення кваліфікації прокурорів (акти Тренінгового центру прокурорів України від 01.10.2025, Національної академії внутрішніх справ від 10.07.2025, Київського столичного університету імені Бориса Грінченка від 16.10.2025, ПВНЗ «Європейський Університет» від 20.10.2025, листи проєкту «HELP (Human Rights Education for Legal Professionals) for Ukraine including during wartime» Ради Європи від 16.10.2024), проєкту «CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine» Ради Європи від 30.10.2025.

Особистий внесок здобувача. Дисертація виконана автором самостійно. Усі сформульовані положення та висновки є результатом особистих досліджень автора. Власні теоретичні розробки здобувача після захисту кандидатської дисертації (2018 р.) та в опублікованих у співавторстві основних наукових працях становлять понад 85 %. Наукові доробки співавторів за темою дисертації не використовувались.

Апробація результатів дисертації. Основні положення та висновки дослідження оприлюднені автором у виступах на всеукраїнських і міжнародних науково-практичних конференціях, круглих столах, зокрема: «Актуальні питання судової експертології, криміналістики та кримінального процесу» (м. Київ, 5 листопада 2019 р.); «Інноваційні рішення в сучасній науці, освіті та практиці» (м. Київ, 17-18 листопада 2020 р.); «Кримінальна юстиція в Україні: реалії та перспективи» (м. Львів, 11 червня 2021 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 29 жовтня 2021 р.); «Наукові читання пам’яті Ганса Гросса» (м. Чернівці, 9 грудня 2021 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 21 жовтня 2022 р.); «ІІІ Наукові читання пам’яті Ганса Гросса» (м. Чернівці, 8 грудня 2023 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці,

27 жовтня 2023 р.); «Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини» (м. Київ, 7 грудня 2023 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 31 жовтня 2024 р.); «Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини» (м. Київ, 10 грудня 2024 р.); «Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій» (м. Чернівці, 20 грудня 2024 р.); «Актуальні проблеми національного законодавства» (м. Кропивницький, 17 квітня 2025 р.); «Пріоритетні шляхи розвитку науки і освіти» (м. Львів, 9–10 травня 2025 р.); «Актуальні питання реформування правової системи» (м. Луцьк, 13–15 червня 2025 р.).

Публікації. Основні положення дисертації опубліковано в 44 наукових працях, серед яких монографія, 19 статей – у виданнях включених МОН України до переліку наукових фахових з юридичних наук, 3 статті – у періодичних виданнях іноземних країн, 3 статті – у виданнях, що індексуються у наукометричних базах даних Scopus і Web of Science, 15 у збірниках тез доповідей, оприлюднених на науково-практичних конференціях та круглих столах.

Структура та обсяг дисертації. Робота складається з анотації, переліку умовних позначень, вступу, п’яти розділів, що містять 20 підрозділів, висновків, списку використаних джерел (540 найменувань на 67 сторінках) та 25 додатків на 117 сторінках. Повний обсяг дисертації становить 617 сторінок, з них основний текст дисертації – 407 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, висвітлено зв’язок роботи з науковими програмами, планами, темами; визначено мету й задачі, об’єкт і предмет та охарактеризовано методи дослідження; окреслено наукову новизну, практичне значення одержаних результатів, особистий внесок здобувачки; подано відомості про апробацію та публікації результатів дослідження, структуру й обсяг дисертації.

Розділ 1 «Теоретичні основи доказів електронної форми у кримінальному процесі України» складається з чотирьох підрозділів.

У *підрозділі 1.1 « Вітчизняні доктринальні підходи до розуміння доказів та їх властивостей у кримінальному процесі України »* досліджено категорію доказів у кримінальному процесі України, яка є результатом тривалої еволюції наукової думки та має багатовимірну правову природу, яка не може бути пояснена в межах будь-якої одновимірної теоретичної моделі. Сучасне доктринальне осмислення доказів ґрунтується на інтеграції інформаційного, логічного, процесуального, матеріально-правового та конституційно-ціннісного вимірів і знаходить своє найбільш послідовне відображення в комплексно-системному підході, відповідно до якого доказ розглядається як єдність фактичних даних, їх джерел і процесуальної форми, що набувають доказового значення внаслідок реалізації уповноваженими суб’єктами кримінального провадження передбачених законом процесуальних повноважень. Властивості доказів утворюють внутрішньо

впорядковану систему, в якій належність і допустимість виступають базовими юридично значущими властивостями окремого доказу, достовірність має оцінний характер і встановлюється в контексті всієї доказової сукупності, а достатність відображає інтегративну якість системи доказів загалом.

Технологічний елемент і технічні характеристики доказів електронної форми не розглядаються як підстава для виокремлення самостійного виду доказів, а оцінюються як релевантні чинники, що опосередковано впливають передусім на допустимість та достовірність доказів. Така позиція забезпечує спадкоємність із загальною теорією кримінального процесуального доказування, унеможливлює технократичну редукцію доказу до цифрового об'єкта чи його параметрів і водночас створює чіткі методологічні межі для коректного аналізу цифрової трансформації доказування.

У *підрозділі 1.2 «Концептуальні підходи до доказів електронної форми у кримінальному процесі України»* обґрунтовано необхідність системного підходу до вивчення електронної складової кримінального процесу України загалом та доказів електронної форми зокрема. Запропоновано п'ятиелементну модель електронної складової кримінального процесу України, що включає: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми; електронні інструменти доказування; електронні інструменти реалізації повноважень суб'єктів правозастосування; доведено необхідність чіткого розмежування зазначених елементів.

Встановлено, що чинне кримінальне процесуальне законодавство України не містить кодифікованого інституту доказів електронної форми, а наявна нормативна база є фрагментарною. Аргументовано, що положення Цивільного процесуального кодексу України, Господарського процесуального кодексу України та Кодексу адміністративного судочинства України щодо електронних доказів не можуть бути за аналогією застосовані у кримінальному процесі, з огляду на відсутність в КПК України відповідних бланкетних норм та автономну процесуальну модель доказування кримінального провадження.

Обґрунтовано, що термін «цифровий доказ» відповідає змісту доказу, «електронний доказ» – технічному способу його реалізації й відтворення, а «доказ електронної форми» – процесуальній формі подання доказу під час кримінального провадження. Доведено доцільність застосування у дисертації терміна «докази електронної форми» як найбільш академічно релевантного.

У *підрозділі 1.3 «Ретроспектива формування інституту електронних (цифрових) доказів у кримінальному процесі України»* проілюстровано еволюцію наукових уявлень про докази електронної форми у кримінальному процесі України як результату адаптації практики правозастосування до цифрової трансформації світу. Встановлено, що історичний розвиток наукових поглядів не є лінійним з огляду на паралельне існування конкуруючих підходів, що по-різному окреслювали місце таких доказів у системі процесуальних джерел.

Проведено огляд основних наукових концепцій, що склалися у вітчизняній кримінальній процесуальній доктрині щодо місця доказів електронної форми в системі процесуальних джерел доказів, їх класифікації. Висвітлено проблему

термінологічної невизначеності, що властива сучасній доктрині та відображає відсутність усталеного підходу до правової категоризації доказів електронної форми. Встановлено, що у вітчизняному дискурсі паралельно функціонують десятки дефініцій, що значною мірою схожі за змістом, але мають різні акценти залежно від наукового підходу, технічної площини дослідження або спеціалізації науковця.

Визначено передумови формування інституту електронних (цифрових) доказів у кримінальному процесі України. Відсутність кодифікованого інституту електронних доказів у КПК України є усвідомленим стриманим рішенням законодавця, продиктованим браком комплексного розуміння досліджуваного питання, ризиками правової невизначеності та ретроспективних спорів щодо допустимості вже зібраних матеріалів, потенційними колізіями перехідного періоду. Формальне розширення переліку процесуальних джерел доказів не здатне вирішити існуючі системні виклики, позаяк необхідне запровадження комплексної, доктринально вивіреної та технологічно релевантної системи процесуальних стандартів з виявлення, фіксації, верифікації, зберігання та дослідження доказів електронної форми в кримінальному процесі.

У *підрозділі 1.4 «Процесуальна та технічна природа доказів електронної форми у кримінальному процесі України»* доведено, що цифрова інформація як нематеріальна категорія існує у вигляді бітової послідовності, віддільної від матеріального носія інформації, і набуває статусу доказу виключно через належне процесуальне оформлення: протоколювання і оформлення результатів слідчих (розшукових) із застосуванням засобів технічних фіксації. Однак сучасний рівень технологічного розвитку та чинні правові норми усувають формальну прив’язаність доказу до паперового носія, що уможливлює існування у електронній формі всіх видів процесуальних джерел доказів.

Досліджено процесуальні особливості документів та речових доказів як процесуальних джерел доказів, їх співвідношення та розмежування в контексті досліджуваних об’єктів. Показано процесуальну природу комп’ютерних даних (як документа), носіїв інформації (як документа або як речового доказу – залежно від процесуальної ситуації) та фізичної оболонки пристрою (як речового доказу).

Охарактеризовано специфіку показань, що фіксуються в електронній формі. Під час відеофіксації допитів і реалізації дистанційних процесуальних процедур має бути забезпечено належну ідентифікацію допитуваної особи та фіксацію параметрів технічного середовища. Наголошено на необхідності нормативної деталізації механізмів підтвердження автентичності та цілісності відеозапису, стандартів зберігання, забезпечення доступу для сторін, методики дослідження під час судового розгляду (36,4% опитаних суб’єктів кримінального провадження цілісність доказів не перевіряють).

Висновок експерта як процесуальне джерело доказів існує в електронній формі у вигляді електронного документа, підписаного кваліфікованим електронним підписом (далі – КЕП). Обґрунтовано необхідність його долучення до кримінального провадження в електронній формі разом із файлами верифікації підпису.

Висвітлено технічну природу доказів електронної форми та роль технічного компоненту в процесі підтвердження їх автентичності, цілісності й відтворюваності у кримінальному провадженні. Запропоновано 4-рівневу внутрішню структуру доказу електронної форми: контент, метадані, системна оболонка, носій інформації.

Залежно від особливостей цифрового середовища електронні носії інформації доцільно класифікувати: I. За доступністю: 1) локальні; 2) віддалені; 3) динамічні; II. За середовищем зберігання: 1) фізичні; 2) віртуальні; III. За типом пам'яті: 1) постійна пам'ять; 2) тимчасова пам'ять; 3) розподілена пам'ять. Залежно від технічної конструкції: I. За ступенем інтеграції електронного носія інформації з інформаційною системою (далі – ІС): 1) відокремлені від ІС; 2) вбудовані в ІС, що: а) можуть бути відокремлені від ІС без втрати властивостей; б) можуть бути відокремлені від ІС лише шляхом фізичного знищення стійких структурних елементів та порушення цілісності ІС; II. За типом запам'ятовуючого пристрою: 1) оперативний запам'ятовуючий пристрій; 2) енергонезалежний запам'ятовуючий пристрій. Доведено значення пропонованої класифікації при обґрунтуванні необхідності прийняття окремих процесуальних рішень (підтвердження позиції сторони обвинувачення при вирішенні питання про арешт майна, скасування рішення про арешт майна, його повернення власнику, тощо).

Аргументовано розмежування логічного копіюванням цифрових файлів і криміналістичного (побітового) копіюванням електронного носія інформації. Сформульовано підхід до підтвердження цілісності доказів електронної форми у кримінальному процесі за допомогою гешування як стандартної процедури підтвердження цілісності та незмінності цифрового об'єкта на всіх стадіях кримінального провадження. Розкрито техніко-юридичний механізм використання електронного підпису та електронної позначки часу для засвідчення авторства, походження і моменту створення електронного документа, взаємозв'язок цих інструментів із вимогами до допустимості та достовірності доказів. Виокремлено категорію об'єктів виключно цифрової природи, що існують лише у віртуальному середовищі та для збережуваності яких як доказів критичною є своєчасна фіксація.

Розділ 2 «Практика роботи з доказами електронної форми у кримінальному процесі України» складається з трьох підрозділів.

У *підрозділі 2.1 «Практика пошуку та фіксації доказів електронної форми у кримінальному процесі України»* доведено, що практичні рішення у цій сфері визначаються місцем розташування даних (кіберпростір чи фізичні носії), їх юридичним статусом, технічним вираженням, а також оперативною обстановкою на місці проведення слідчих (розшукових) дій. На цій основі обґрунтовано три стратегії фіксації доказів електронної форми в кримінальному процесі України: 1) фізичне вилучення носія або ІС, до якої він входить; 2) огляд та копіювання інформації, що зберігається на електронному носії інформації; 3) огляд та фіксація інформації з відкритих джерел (кіберпростору)).

Розкрито особливості пошуку доказів електронної форми у фізичному середовищі з урахуванням мініатюризації та маскування електронних носіїв інформації, що ускладнює їх виявлення без спеціальних знань і засобів. Фізичне

вилучення електронних ІС, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку суворо обмежене в КПК України, однак навіть за формальної процесуальної можливості для такого вилучення цей спосіб не завжди є ефективним через ризики блокування бізнес-процесів, шифрування даних чи структурну складність систем. Альтернативним і менш інвазивним способом збору доказів електронної форми є копіювання інформації. За результатами аналізу норм КПК України визначено закріплену в ч. 4 ст. 99 КПК України процесуальну формулу копіювання інформації як спосіб здобуття доказів електронної форми: «копія інформації × (слідчий або прокурор + спеціаліст) = оригінал документа». Визначено двокомпонентну природу належного копіювання інформації, процесуальний аспект якого полягає в обов'язковому залученні компетентного спеціаліста (ст. 71 КПК України) та належному документуванні, технічний — у дотриманні вимог ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» (далі – ДСТУ ISO/IEC 27037:2017) щодо недопущення змін первинних даних і верифікації копії шляхом гешування комп'ютерних даних з фіксацією контрольних значень (геш-сум) у протоколі слідчої (розшукової) дії.

Розглянуто підхід до роботи в умовах відсутності фізичного доступу до електронних носіїв інформації та комп'ютерних систем, коли джерелом відомостей є хмарні платформи, онлайн-сервіси чи інші елементи кіберпростору. Стратегією фіксації відомостей кіберпростору є огляд комп'ютерних даних у порядку ст. 237 КПК України із дотриманням вимог ч. 4 ст. 99 КПК України, фіксацією технічних параметрів доступу і відтворенням дій користувача (протокол наведено як додаток до дисертації). Для отримання недоступних публічно даних запропоновано покрокове використання механізмів Конвенції про кіберзлочинність: термінове збереження комп'ютерних даних компетентними органами іноземної держави з подальшим зверненням по міжнародну правову допомогу. Наголошено на необхідності вузького тлумачення «розширеного» доступу до даних під час обшуку в порядку абз. 2 ч. 6 ст. 236 КПК України з огляду на норми ч. 2 ст. 19 Конвенції – виключно в межах території України, що узгоджується з принципом державного суверенітету. Неодмінною є детальна фіксація технічних параметрів середовища доступу, збереження вихідного коду сторінок, артефактів завантаження, мережевої активності тощо.

Сформовано цілісну модель практики пошуку й фіксації доказів електронної форми, де копіювання цифрової інформації згідно з процесуальних вимог КПК України та дотриманням ДСТУ ISO/IEC 27037:2017 постає як пріоритетна та технологічно вивірена альтернатива фізичному вилученню, а робота з кіберпростором – як самостійний вектор доказування з опорою на процедури міжнародної взаємодії.

У *підрозділі 2.2 «Механізми підтвердження цілісності та автентичності доказів електронної форми в кримінальному провадженні»* обґрунтовано, що у вітчизняній моделі визначальним інструментом фіксації ходу і результатів процесуальних дій є протокол, вимоги до якого встановлені статтями 104–106 КПК України. Підкреслено значення змін, внесених до КПК України в 2022 році,

якими, зокрема, уточнено обов'язок відображати у прикінцевій частині протоколу виготовлені дублікати, копії комп'ютерних даних і спосіб їх ідентифікації, а також конкретизовано процесуальний режим огляду комп'ютерних даних.

Розкрито зміст і мету ідентифікації комп'ютерних даних як процесу, покликаного забезпечити встановлення тотожності об'єкта на різних стадіях кримінального провадження з первинно зафіксованим станом, тобто підтвердження його цілісності та автентичності. Систематизовано механізми, що застосовуються для досягнення цієї мети: документальне упакування та маркування носіїв; фіксація загальних та унікальних апаратних ідентифікаторів; опис структур і вмісту даних та їх метаданих; застосування гешування і фіксації контрольних сум на рівні файлів і криміналістичних образів. Цифрова природа об'єктів зумовлює потребу у верифікації з вищим рівнем упевненості, ніж це забезпечують традиційні засоби ідентифікації матеріальних об'єктів.

Досліджені емпіричні дані демонструють фрагментарність правозастосування: стандартизовану інструкцію для фіксації джерела надходження доказу електронної форми (протоколювання та долучення до матеріалів кримінального провадження) використовують у своїй роботі 58% опитаних респондентів, не використовують 38%, іншу відповідь вказали 4% опитаних; стандартизовану інструкцію для перевірки цілісності доказу електронної форми – 38% опитаних респондентів, не використовують 59%, іншу відповідь вказали 3% опитаних. Тривожною є тенденція щодо використання відповідних процедур лише 43% слідчих, детективів та 36% прокурорів, значна частка учасників провадження взагалі не здійснює такої перевірки, що ставить під ризик підтверджуваність цілісності значного масиву зібраних доказів. Окреслено поширені практики зберігання і долучення доказів електронної форми, що поєднують фізичні носії та хмарні сервіси, що, з одного боку, розширює інструментарій обігу доказів, а з іншого – ускладнює контроль за доступом до них.

Аргументовано доцільність використання ДСТУ ISO/IEC 27037:2017 як технічного орієнтиру для ідентифікації, збирання, здобуття та збереження, із наголосом на необхідності хронологічного документування процесу роботи з доказами електронної форми. Показано відмінність терміна «ідентифікація» у розумінні стандарту (як пошук і первинне виявлення) від його процесуального змісту для цілей протоколу (як засіб підтвердження цілісності та автентичності). Розкрито сутність концепції chain of custody як системи забезпечення прозорості та простежуваності кожної зміни місцезнаходження, форми та володільця доказу протягом усього життєвого циклу – від ідентифікації та збирання до представлення в суді й архівації. Висвітлено ключові реквізити chain of custody, вимоги до невідворотності і фіксації змін, а також багатосуб'єктний характер взаємодії з доказом, що обумовлює підвищені вимоги до автентифікації осіб та фіксації їх дій.

Проведено огляд сучасних організаційно-технічних моделей ведення chain of custody: від традиційного паперового документування до системно орієнтованих рішень управління доказами з інтегрованими журналами подій, ідентифікацією за штрих-кодами, цифровими підписами та побудовою криміналістичних образів, а також інфраструктурно керованих підходів із

використанням хмарних сервісів і блокчейну, спрямованих на гарантування незмінності та перевірюваності записів.

Обґрунтовано необхідність інституціоналізації chain of custody у національній практиці шляхом запровадження стандартних операційних процедур (далі – СОП) для всіх суб'єктів кримінального провадження, що працюють із доказами електронної форми, із вбудованими вимогами до ідентифікації, гешування, побітового копіювання, журналювання доступу та аудиту. Слід гармонізувати такі процедури із ДСТУ ISO/IEC 27037:2017 та суміжними стандартами інформаційної безпеки; закріпити у відомчих актах принципи прозорості й простежуваності, а також правові наслідки порушення хронологічного документування.

У *підрозділі 2.3 «Організаційні аспекти роботи з доказами електронної форми у кримінальному процесі України»* доведено, що результативність роботи з доказами електронної форми визначається не лише процесуальними приписами, а передусім організаційною спроможністю суб'єктів кримінального провадження. Емпіричні дані засвідчили домінування організаційних бар'єрів над суто нормативними, найчастіші проблеми – це технічні аспекти зберігання доказів електронної форми, недостатня технічна й процесуальна компетентність персоналу, труднощі використання цифрових матеріалів у суді, питання безпеки передачі та зберігання; додатково виокремлено типові ускладнення під час підтвердження цілісності та незмінності даних, пошуку й фіксації інформації, а також дефіцит спеціалістів (ст. 71 КПК України) у сфері цифрової криміналістики.

Організаційна готовність суб'єктів кримінального провадження до роботи з доказами електронної форми реалізується через три взаємопов'язані компоненти: матеріально-технічний, кадровий та організаційний. Матеріально-технічний компонент охоплює забезпечення органів досудового розслідування цифровими криміналістичними інструментами та інфраструктурою, сумісною зі стандартом ДСТУ ISO/IEC 27037:2017, з урахуванням динамічного характеру цифрових слідів і потреби технологій негайного реагування. Кадровий компонент пов'язаний із міждисциплінарною компетентністю слідчих, детективів, прокурорів, спеціалістів, експертів і суддів. Вказано на дефіцит базових технічних знань (структура цифрового сліду, механізми гешування, значення побітової копії, метадані, доступ до хмарних ресурсів), міжвідомчу й регіональну нерівномірність підготовки та потребу у стандартизованих програмах навчання, включно з OSINT-кваліфікаціями й внутрішньовідомчою сертифікацією. Нормативний компонент окреслює відсутність уніфікованого загальнообов'язкового стандарту дій для всіх органів досудового розслідування, адже аналіз чинних відомчих актів і методичних матеріалів свідчить про їхню фрагментарність, що обумовлює потребу у запровадженні СОП для ідентифікації, збирання, здобуття, збереження та використання доказів електронної форми.

Установлено доцільність створення централізованих відомчих віртуальних сховищ для доказів електронної форми із розділенням мереж та резервним копіюванням даних. Наголошено на ризиках фізичної й логічної деградації електронних носіїв інформації та необхідності запровадження системної політики резервного копіювання доказів електронної форми. Забезпечення їх автентичності

та цілісності вимагає процедурної фіксації засобів верифікації (геш-коди, електронний підпис) у процесуальних документах та впровадження повноцінного chain of custody з багаторівневим керуванням доступом, двофакторною автентифікацією, журналюванням дій і фіксацією метаданих. Порушено етичний аспект обмеження доступу до персональної інформації, що не має доказового значення, під час відкриття матеріалів за ст. 290 КПК України та окреслено потребу уточнення процесуальних механізмів захисту приватності.

Розділ 3 «Процесуальні повноваження та функціональні ролі суб'єктів кримінального провадження у взаємодії з доказами електронної форми» складається з п'яти підрозділів.

У *підрозділі 3.1 «Слідчий як суб'єкт роботи з доказами електронної форми в кримінальному провадженні»* висвітлено процесуальну, організаційну та технічну роль слідчого як основного суб'єкта роботи з доказами електронної форми під час досудового розслідування. Ефективність доказової діяльності залежить від первинних дій слідчого під час виявлення й фіксації цифрових слідів, його здатності самостійно ініціювати та проводити слідчі (розшукові) дії, а також базової технічної обізнаності. Обґрунтовано потребу системного залучення спеціаліста (ст. 71 КПК України) для забезпечення вимог ч. 4 ст. 99 КПК України та у випадках, коли реалізація технічних процедур перевищує межі компетентності слідчого.

Наголошено на необхідності точної фіксації в протоколах слідчих (розшукових) дій технічних характеристик досліджуваних ІС і електронних носіїв інформації, фіксації застосованих методів ідентифікації та способів доступу до комп'ютерних даних, вказано на значення ДСТУ ISO/IEC 27037:2017 як орієнтира для практики.

Проаналізовано алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку, огляду, застосування якого є ефективним інструментом аналізу оперативної обстановки на місці проведення обшуку, огляду в складних процесуальних обставинах та в умовах процесуальної протидії сторони захисту. Здійснено огляд ефективних стратегій та технічних засобів подолання систем логічного захисту доступу до сучасних комп'ютерних систем під час кримінального провадження. Навіть за наявності криптографічного захисту можливо забезпечити здобуття інформації за умови належного процесуального й технічного супроводу.

Розглянуто процесуальний режим вилученої під час обшуку копії інформації, носія, на якому вона зберігається, а також забезпечення збереження їх цілісності. Підкреслено, що виготовлена копія інформації, що міститься в ІС, у разі дотримання вимог ч. 4 ст. 99 КПК України, визнається судом як оригінал документа, що відкриває широкі можливості застосування доказів електронної форми без вилучення слідчим технічних пристроїв.

Окреслено можливості та межі використання OSINT як інструмента виявлення, перевірки та фіксації відомостей із відкритих джерел. Такі матеріали набувають процесуальної форми документа, однак їх допустимість залежить від належної верифікації джерела, забезпечення автентичності контексту та його

належної фіксації згідно з Протоколом Берклі з ведення розслідувань з використанням відкритих цифрових даних (далі – Протокол Берклі).

У *підрозділі 3.2 «Прокурор як суб'єкт роботи з доказами електронної форми в кримінальному провадженні»* висвітлено роль прокурора як центрального суб'єкта роботи з доказами електронної форми. Проаналізовано норми КПК України щодо обов'язкового відображення відомостей про дублікати і копії комп'ютерних даних у прикінцевій частині протоколу, що посилює позицію прокурора в суді для доведення автентичності та цілісності доказів електронної форми. Висвітлено підхід до електронного документа як різновиду документа у розумінні КПК України та спеціальних законів.

Мінімізувати ризики існування доказу електронної форми в єдиному екземплярі варто шляхом його резервного копіювання – проведення огляду відповідного електронного носія інформації з дотриманням вимог ч. 4 ст. 99 КПК України та виготовлення його криміналістичної (побітової) копії, належною ідентифікацією комп'ютерних даних та фіксацією їх геш-значень у протоколі огляду.

Запропоновано практичний інструмент (бланк наведено як додаток до дисертації) для оцінки прокурором доказу електронної форми, який структуровано охоплює оцінку дотримання процесуальних і технічних аспектів та уніфікує відповідну діяльність прокурора під час прийняття ключових процесуальних рішень – повідомлення особі про підозру, затвердження обвинувального акта тощо.

Прокурор вправі відкривати матеріали досудового розслідуванні у частині доказів електронної форми згідно з ч. 3 ст. 290 КПК України як «документи або копії з них», забезпечуючи автентичність і цілісність даних (шляхом створення криміналістичних копій електронних носіїв інформації із фіксацією геш-ідентифікаторів), а також організовуючи стороні захисту доступ і можливість копіювання даних без покладання на сторону обвинувачення не передбачених законом обов'язків з технічного обслуговування. Вказано на необхідність інкорпорації цифрових слідів у зміст обвинувального акта та запропоновано підхід до їх представлення під час судового розгляду.

Проаналізовано результати опитування понад 700 прокурорів, ідентифіковано системні проблеми практики роботи з доказами електронної форми та сформульовано пропозиції, що включають нормативну уніфікацію процедур роботи з доказами електронної форми на рівні Офісу Генерального прокурора, розвиток спеціалізації й навчання, а також створення внутрішньої інфраструктури технічного супроводу та залучення фахівців у сфері цифрової криміналістики.

У *підрозділі 3.3 «Захисник як суб'єкт роботи з доказами електронної форми в кримінальному провадженні»* висвітлено процесуальні можливості захисника при роботі з доказами електронної форми у кримінальному провадженні. Сформульовано практичні стратегії роботи сторони захисту з електронною інформацією, акцентовано на доказовому потенціалі резервних копій комп'ютерних даних, журналів з'єднань, даних геолокації, листування у месенджерах і метаданих, зокрема для встановлення алібі чи спростування позиції

сторони обвинувачення. Ефективність використання таких відомостей поставлено в пряму залежність від дотримання стороною захисту вимог ДСТУ ISO/IEC 27037:2017 під час їх фіксації. Окремо розкрито тактику захисника під час обшуку, що пов'язаний із виявленням, фіксацією та вилученням електронної інформації. Запропоновано алгоритм фіксації порушень і формування зауважень до протоколу, з акцентом на індивідуалізацію електронних носіїв інформації, відображення геш-сум.

Проаналізовано особливості відкриття захиснику матеріалів досудового розслідуванні за ст. 290 КПК України та ефективні сценарії процесуальної взаємодії захисника зі стороною обвинувачення. Аргументовано, що належний доступ сторони захисту має включати не лише ознайомлення зі змістом доказів електронної форми, а й можливість перевірки їх автентичності та цілісності, за потреби – доступу до криміналістичної (побітової) копії електронних носів інформації. Зазначено про можливість реалізації стороною захисту самостійного технічного аналізу доказів електронної форми, у тому числі шляхом залучення спеціаліста. Підкреслено значення стандартів захисту приватності й персональних даних у роботі з великими масивами комп'ютерних даних, вилучених у підозрюваного, обвинуваченого. Розкрито потребу обґрунтування мінімізації втручання у приватне життя, анонімізації або псевдонімізації надлишкових відомостей і процесуального документування випадків необґрунтованого втручання, з урахуванням гарантій ст. 8 Конвенції про захист прав людини та основоположних свобод.

Указано на комплексний характер діяльності захисника при роботі з доказами електронної форми. Запропоновано вектор удосконалення відповідної практики щодо стандартизації форматів надання стороні захисту комп'ютерних даних в загальнодоступному технічному форматі, обов'язкове супроводження комп'ютерних даних ідентифікаторами (геш-суми) й технічною довідковою інформацією, а також інституційне зменшення технічної асиметрії між стороною обвинувачення і стороною захисту як передумова змагальності та рівності сторін кримінального провадження.

У *підрозділі 3.4 «Суддя та слідчий суддя як суб'єкти роботи з доказами електронної форми в кримінальному провадженні»* обґрунтовується, що слідчий суддя здійснює судовий контроль за правомірністю втручання органів досудового розслідування в цифрове середовище під час досудового розслідування, ухвалюючи рішення щодо тимчасового доступу до речей і документів, обшуку, арешту електронних носіїв інформації, обґрунтування не лише юридичну, а й технічну обґрунтованість втручання.

Обов'язок суду під час судового розгляду – забезпечити перевірку допустимості доказів електронної форми з урахуванням їх технічної природи. Така оцінка має здійснюватися з урахуванням автентичності та цілісності комп'ютерних даних, підтверджених журналюванням доступу, геш-сумами і можливістю відтворення в придатному для аналізу форматі. Обґрунтовано пріоритет дослідження під час судового розгляду саме криміналістичної (побітової) копії електронних носів інформації, оскільки робота з оригінальним

пристроєм спричиняє незворотні зміни його стану та неможливість повторного проведення експертного дослідження.

Розкрито специфіку перевірки судом інформації з відкритих джерел (результатів OSINT): ключовими критеріями є встановлення джерела інформації, відтворюваності та належного документування процесу фіксації. Запропоновано алгоритм дослідження доказів електронної форми під час судового розгляду як послідовності технічно обумовлених дій із безпечного підключення електронного носія інформації, точною навігацією до місця зберігання комп'ютерних даних та коректною презентацією змісту. Для підвищення ефективності доказування рекомендовано орієнтувати сторони кримінального провадження надавати структуровані навігаційні реквізити (шляхи, ідентифікатори, часові мітки, посилання на метадані). Висвітлено процесуальні механізми поглибленого дослідження судом доказів електронної форми під час судового розгляду, зокрема витребування додаткових даних, призначення комп'ютерно-технічної експертизи, допиту експерта та залучення спеціаліста.

Узагальнено підходи вітчизняної судової практики шляхом аналізу правових позицій Верховного Суду щодо електронних документів, електронних носіїв інформації та копій цифрових даних, водночас виявлено неоднорідність рішень, що зумовлює необхідність уніфікації підходів.

У *підрозділі 3.5 «Інші учасники кримінального провадження як суб'єкти роботи з доказами електронної форми в кримінальному провадженні»* висвітлено роль технічних фахівців при роботі з досліджуваними доказами. Базових технічних знань слідчого, прокурора чи судді зазвичай об'єктивно недостатньо для ефективної роботи з доказами електронної форми, тож слід залучати носіїв спеціальних знань. Теоретично розмежовано використання і застосування спеціальних знань, окреслено статус та межі процесуальних повноважень експерта і спеціаліста. Роль експерта визначено через положення КПК України та Закону України «Про судову експертизу», вказано на формалізованість підстав і порядку призначення експертизи, багаторівневу структуру компетенції та вимогах до методик, що підлягають державній реєстрації. Досліджено специфіку комп'ютерно-технічної та телекомунікаційної експертиз, їх предметні завдання та типові питання, а також методичні вимоги до формулювання завдань.

Головним ризиком існуючої практики є перевантаженість експертних установ і тривалі строки проведення експертних досліджень, що зумовлює процесуальні затримки та загрозу втрати релевантних цифрових даних. Запропоновано процесуальну оптимізацію через чітке розмежування функцій технічних фахівців, де спеціаліст забезпечує первинні технічні дії – ідентифікацію комп'ютерних даних, їх здобуття (створення криміналістичних (побітових) копій із фіксацією геш-сум), попередній технічний аналіз метаданих та логів тощо, тоді як експерт зосереджується на комплексних питаннях та глибинному технічному дослідженні. Робота з оригінальними носіями є недопустимою, а криміналістичні дослідження здійснюється виключно з використанням побітових копіях електронних носів інформації із забезпеченням відтворюваності процедур.

Описано процесуальний механізм залучення спеціаліста (ст. 71 КПК України), його права та обов'язки, а також форми фіксації участі, що

передбачає складання протоколів процесуальних дій, письмових пояснень, технічних довідок і журналу судового засідання. Наголошено на значенні галузевих стандартів, насамперед ДСТУ ISO/IEC 27037:2017, що визначає вимоги до роботи спеціаліста з доказами електронної форми і його роль як першого відповідального за цифровий доказ або ж Digital Evidence First Responder (далі – DEFR). Указано на можливість допиту експерта під час судового розгляду з метою роз'яснення, уточнення та доповнення висновку, а також брак спеціальної моделі допиту для спеціаліста, що уможливлює використання альтернативних процесуальних форм його залучення.

Обґрунтовано допустимі форми участі OSINT-фахівців як спеціалістів під час фіксації даних з відкритих джерел, необхідність належної фіксації їх участі у відповідному протоколі огляду та використання міжнародно визнаної методології.

Розділ 4 «Міжнародні процедури пошуку, фіксації та використання доказів електронної форми» складається з чотирьох підрозділів.

У *підрозділі 4.1 «Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних та застосування його вимог під час кримінального провадження»* установлено значення Протоколу Берклі як міжнародного стандарту роботи з інформацією з відкритих джерел, що може бути застосований під час кримінального провадження. Протокол Берклі визначено як орієнтир, що акцентує не на конкретних інструментах, а на принципах і методології, стійких до технологічних змін, із пріоритетом професійної відповідальності, компетентності, об'єктивності та безпеки учасників.

Систематизовано ключові положення Протоколу Берклі щодо нормативної основи, безпеки, підготовки, процесу розслідування та фіксації відшуканих даних. Наголошено на необхідності визначення застосовного права, забезпечення автентичності та документування ланцюга збереження доказів, управління ризиками на інфраструктурному й поведінковому рівнях. Описано цикл OSINT: від запитів і попередньої оцінки до збирання, збереження, перевірки та слідчого аналізу; підкреслено мінімальні стандарти фіксації (URL, HTML-код, повноекранне захоплення, метадані, контекст, дані збору, геш-значення) і вимоги до довготривалого зберігання. Вказано на значення верифікації інформації через аналіз джерела, технічний аналіз і аналіз контенту, а також роль структурованого слідчого аналізу. Окремо обґрунтовано вимоги до письмової, усної та візуальної звітності як форм фіксації відшуканих даних, необхідності забезпечення точності, повноти фіксації, нейтральності описової частини та прозорості застосовуваних методів.

Окреслено стан імплементації Протоколу Берклі в кримінальному процесі України, зокрема: рекомендації Офісу Генерального прокурора, відсилання до положень Протоколу Берклі у рішеннях Верховного Суду, та, водночас, відсутність у КПК України окремих правил роботи з інформацією з відкритих джерел. Сформульовано пропозиції щодо нормативного врегулювання огляду віртуального середовища як окремої слідчої (розшукової) дії. Обґрунтовано необхідність системної імплементації стандартів Протоколу Берклі до КПК України для підвищення ефективності розслідування кримінальних проваджень, особливо щодо кіберзлочинів та воєнних злочинів.

У *підрозділі 4.2 «Механізми Конвенції про кіберзлочинність та практика їх застосування в кримінальному процесі України»* доведено, що цей акт є базовим міжнародним стандартом для роботи з доказами електронної форми, адже поєднує уніфіковані дефініції, процесуальні повноваження зі збирання даних та механізми міжнародного співробітництва.

Термінове збереження комп'ютерних даних (ст.ст. 16, 29 Конвенції) виконує превентивну функцію «заморожування» інформації до отримання формального доступу, але не імплементоване в КПК України; на практиці його роль виконує тимчасовий доступ до речей і документів, що не забезпечує оперативності та конфіденційності; розкрито зміст процедур термінового збереження і часткового розкриття даних про рух інформації (ст.ст. 17, 30 Конвенції), яке дає змогу ідентифікувати повний маршрут передавання без розкриття змісту, також не імплементований в КПК України. Доцільно запровадити окрему норму (ст. 245-2 КПК України) для фіксації та термінового розкриття таких даних.

Обґрунтовано доцільність імплементації порядку представлення (ст. 18 Конвенції) з чітким охопленням усіх категорій комп'ютерних даних, адже чинні норми КПК України щодо тимчасового доступу до речей і документів не повністю відтворюють вимоги Конвенції. Щодо обшуку і арешту збережуваних комп'ютерних даних (ст. 19 Конвенції) вказано на часткову імплементацію, зокрема елемент «розширеного обшуку» в абз. 2 ч. 6 ст. 236 КПК України, однак є потреба впровадження спеціальних норм для захисту цілісності даних. Збирання даних про рух інформації у реальному часі (ст. 20 Конвенції) і перехоплення змісту, що передається (ст. 21 Конвенції), у КПК України опосередковано охоплені ст. 263, проте вимагають чіткого розмежування в частині доступу до трафіку і до контенту, підвищення гарантій пропорційності та судового контролю. Інститут добровільного надання інформації (ст. 26 Конвенції) потребує доктринальної та нормативної інтеграції у КПК України. Реалізація процедур Конвенції про кіберзлочинність відбувається через мережу національних контактних пунктів, що забезпечує цілодобову взаємодію України з іншими державами-підписантами (ст. 35 Конвенції), функцію якого в Україні виконує один з підрозділів Департаменту кіберполіції Національної поліції України. Проаналізовано положення Другого додаткового протоколу до Конвенції про кіберзлочинність та доцільність імплементації відповідних положень.

Зміни, внесені до КПК України в березні 2022 року, започаткували імплементацію норм Конвенції про кіберзлочинність, однак зберігаються системні прогалини у контексті оперативності, технологічної адекватності та дотриманням балансу між ефективністю кримінального переслідування і захистом прав людини.

У *підрозділі 4.3 «Практика впровадження стандарту ISO/IEC 27037:2012 в державах Європи та в Україні»* висвітлено практику впровадження міжнародного стандарту ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence» у державах Європи та в Україні, що має ключове значення для уніфікації процедур роботи з доказами електронної форми у кримінальному

провадженні. Відсутність у КПК України техніко-процесуальних норм щодо ідентифікації, збирання, здобуття та збереження таких доказів зумовлює необхідність орієнтації на положення ДСТУ ISO/IEC 27037:2017, який є ідентичним міжнародному ISO/IEC 27037:2012.

ДСТУ ISO/IEC 27037:2017 регламентує чотири ключові процеси роботи з доказами електронної форми: ідентифікацію, збирання, здобуття та збереження, що забезпечують підтвердження автентичності та цілісності доказів й обумовлюють їх допустимість. Стандарт містить рекомендації щодо функціональної діяльності спеціалістів — першого відповідального за цифровий доказ (DEFR) та спеціаліста з цифрових доказів (Digital Evidence Specialist, DES), визначає вимоги до технічних засобів і середовищ збереження доказів, підкреслюючи, що він не замінює законодавчих норм, а доповнює їх як практична інструкція. Підкреслено складність доступу до офіційного тексту стандарту через режим авторського права ISO та політику, що обмежує його вільне поширення. Вказане створює практичні труднощі для працівників правоохоронних органів і вимагає розроблення організаційних механізмів офіційного доступу до таких стандартів у службовій діяльності.

У *підрозділі 4.4 «Зарубіжний досвід роботи з доказами електронної форми в кримінальному процесі»* здійснено порівняльний аналіз моделей роботи з доказами електронної форми у провідних юрисдикціях загального та континентального права й на наднаціональному рівні ЄС, із орієнтиром на процесуальні інструменти доступу до даних, стандарти допустимості та механізми транснаціональної взаємодії.

Досліджено та систематизовано досвід роботи з доказами електронної форми на рівні нормативних актів Європейського Союзу, а також правове регулювання та практику США, Великої Британії, Франції, Німеччини та цілої низки інших країн.

Визначено тенденції досвіду інших держав щодо роботи з доказами електронної форми під час кримінального провадження, зокрема: інституціоналізація правового режиму доказів електронної форми у межах кримінального процесуального законодавства; утвердження технологічно нейтрального підходу до їх оцінки та допустимості (відсутність вимог визначених технічних засобів чи форматів) тощо. Обґрунтовано потребу гармонізації національної практики з європейською процесуальною архітектурою, унормуванні прямих інструментів доступу до даних, запровадженні техніко-процесуальних стандартів роботи з доказами електронної форми та повноцінній інтеграції у багатосторонні механізми транскордонного обміну доказами електронної форми.

Використання електронної ІС як інструменту обміну доказами обумовлює набуття ними електронної форми незалежно від первинного носія, що висуває підвищені вимоги до підтвердження автентичності, цілісності та відтворюваності даних. Виокремлено критичні виклики — кібербезпека і захист персональних даних, неуніфікованість правових стандартів, колізії юрисдикцій у сфері передачі та використання цифрових даних, а також залежність результативності від людського фактора та рівня підготовки суб’єктів кримінального провадження.

Розділ 5 «Перспективи вдосконалення роботи з доказами електронної форми у кримінальному процесі України» складається з чотирьох підрозділів.

У *підрозділі 5.1 «Організаційні аспекти вдосконалення роботи з доказами електронної форми у кримінальному процесі України»* доведено, що ключовою передумовою належної роботи з доказами електронної форми є належне матеріально-технічне забезпечення органів досудового розслідування, прокуратури та суду, уніфіковані підходи до кадрової підготовки й підвищення кваліфікації суб'єктів кримінального провадження, а також ефективна міжвідомча координація. Підкреслено потребу стандартизації практики роботи з доказами електронної форми під час кримінального провадження шляхом розробки та впровадження СОП як міжвідомчих методичних документів, що синтезують вимоги КПК України, положення ДСТУ ISO/IEC 27037:2017 та Протоколу Берклі й формують передбачуваність оцінки допустимості й достовірності доказів та узгодженість процесуального й технічного компонентів.

Розкрито модель підвищення інституційної спроможності суб'єктів кримінального провадження шляхом поєднання спеціалізації та інституційної автономії. Запропоновано впровадити профільну спеціалізацію слідчих і поступово — прокурорів у сфері розслідування кіберзлочинів, що передбачає інтеграцію правових і технічних компетентностей (інформаційні технології, цифрова криміналістика, кібербезпека) для коректної ідентифікації, фіксації, зберігання та дослідження доказів електронної форми. Обґрунтовано доцільність створення криміналістичних ІТ-лабораторій у структурі правоохоронних органів із організаційною відокремленістю від органів досудового розслідування, щоб забезпечити інституційну незалежність та технологічну спроможність виконувати повний цикл робіт із доказами електронної форми.

Обґрунтовано потребу регламентованих каналів взаємодії з операторами телекомунікації і запропоновано електронну форму виконання ухвал слідчих суддів про тимчасовий доступ до речей і документів у частині даних операторів телекомунікацій через захищену платформу, інтегровану в ІС учасників, із використанням КЕП та процедур криптографічного захисту даних.

З'ясовано, що наявні диспропорції в технічному оснащенні та підготовці кадрів обумовлюють фрагментарність правозастосування. Запропоновано впровадження системного професійного навчання суб'єктів кримінального провадження, що здійснюватиметься професійними тренерами-практиками в тренінговому форматі у формі послідовного багаторівневого навчання за прогресивною шкалою, спільного навчання оперативних працівників, слідчих, прокурорів та суддів, з застосуванням регіонального або кущового формування груп, з можливістю обміну актуальним досвідом та формуванням уніфікованих стандартів роботи. Лише 22% опитаних суб'єктів кримінального провадження вважають свої знання щодо роботи з доказами електронної форми достатніми, 68% вважають їх недостатніми, ще 10% вказують на потребу покращення.

У *підрозділі 5.2 «Шляхи вдосконалення процесуального регулювання використання доказів електронної форми у кримінальному процесі України»* аргументовано потребу системного оновлення кримінального процесуального законодавства України щодо правової природи, статусу та процесуального

режиму роботи з доказами електронної форми. Доведено доцільність поетапної імплементації передових практик: підвищення цифрової компетентності суб'єктів провадження, формування усталеної практики вищих судів, розроблення та впровадження СОП, спеціалізації підрозділів і поступового внесення змін до КПК України.

Сформульовано першорядні напрями оновлення законодавства. Обґрунтовано зміни щодо представлення комп'ютерних даних і врахування технічних аспектів при оцінці доказів, редакційне усунення надлишкової згадки «матеріальний» у ст. 99, запровадження ст. 100-1 про зберігання доказів електронної форми із пріоритетом криміналістичного (побітового) копіювання над фізичним вилученням. Окреслено процесуальну регламентацію автентифікації та збереження, включно з гешуванням, криміналістичним (побітовим) копіюванням, фіксації геш-ідентифікаторів, процедурою реагування на втрату чи зміну даних, створенням відомчих цифрових архівів, електронною формою процесуальних документів із КЕП.

Підтримано гармонізацію КПК України з Конвенцією про кіберзлочинність: термінове збереження комп'ютерних даних і тимчасове розкриття даних про рух інформації; оновлення глави 15 для впровадження «ордера на представлення» відповідно до ст. 18 з акцентом на надання копій даних і реалізації процедури отримання відповідних даних у цифровому форматі; адаптація правил обшуку, огляду та арешту зі ст. 19 із пріоритетом копіювання перед вилученням. Розроблено процесуальні підвалини огляду віртуального середовища (кіберпростору), унормування OSINT як багатоетапної слідчої (розшукової) дії з фіксацією технічних параметрів, диференціацію доступу до змісту й даних про рух інформації, у тому числі запровадження ст. 264-1 для доступу до даних про рух трафіку в режимі реального часу.

Запропоновано вдосконалення технічного аспекту фіксації результатів негласних слідчих (розшукових) дій (гешування та КЕП); впровадження процедури транснаціонального онлайн-допиту свідка зі складанням за його результатами електронного протоколу (з відеододатком) підписаного КЕП; посилення захисту інформації про приватне життя учасників кримінального провадження; впровадження вимог щодо фіксації ланцюга збереження доказів із можливістю використання електронних систем обліку.

У *підрозділі 5.3 «Напрями технічного удосконалення використання доказів електронної форми у кримінальному процесі України»* умотивовано, що цифровізація кримінальної юстиції вимагає якісного оновлення технічної інфраструктури роботи з доказами електронної форми. Доцільно уніфікувати мінімальні стандарти обладнання й програмного забезпечення органів досудового розслідування, прокуратури та судів.

Вимоги до базового технічного оснащення: захищені електронні носії; засоби відеофіксації, інтегровані з цифровими сховищами даних; інструменти створення цифрових протоколів із використанням КЕП; засоби гешування та перевірки цілісності; модулі верифікації КЕП і електронної позначки часу тощо. Акцентовано на необхідності отримання органами досудового розслідування спеціалізованих програмних рішень, що дозволять здійснювати криміналістичне

копіювання з фіксацією геш-значень, аналіз метаданих і журналів подій, відновлення даних, захищені цифрові архіви з фіксацією ланцюга збереження доказу (chain of custody) тощо.

Запропоновано підхід до модернізації системи гарантування цілісності, конфіденційності та збережуваності доказів електронної форми через впровадження гешування як механізму підтвердження їх цілісності, використання електронних процесуальних документів, резервне копіювання, криптографічне шифрування, застосування надійних електронних носіїв та створення відомчих віртуальних сховищ із контрольованим доступом і журналюванням. Необхідно узгодити ці механізми зі стандартами національної системи криптографічного захисту, а також нормативно закріпити геш-значення комп'ютерних даних як обов'язковий реквізит протоколу слідчої (розшукової) дії.

Обґрунтовано концепцію повністю цифрового протоколу слідчої (розшукової) дії, підписаного КЕП усіх залучених суб'єктів, з обов'язковою відеофіксацією та гешуванням відеофайлів і потенційною інтеграцією до e-Case. Доведено необхідність запровадження обов'язкового резервного копіювання доказів електронної форми за уніфікованими стандартами, створення національних (або регіональних) центрів зберігання, інтегрованих з Єдиним реєстром досудових розслідувань і e-Case, із жорстким контролем доступу, багаторівневим шифруванням і географічним дублюванням та дотримання вимог інформаційної безпеки. Підкреслено потребу забезпечення інтероперабельності електронних ІС органів кримінальної юстиції.

У *підрозділі 5.4 «Концепція вдосконалення інституту доказів електронної форми у кримінальному процесі України»* сформульовано концепцію комплексного вдосконалення роботи з доказами електронної форми у кримінальному процесі України, що ґрунтується на системному поєднанні нормативних, організаційних, інфраструктурних, техніко-криміналістичних, освітніх та науково-аналітичних заходів. Її стратегічна мета – створення ефективного, цілісного та технологічно узгодженого механізму процесуального обігу доказів електронної форми, здатного забезпечити достовірність, автентичність і цілісність даних під час кримінального провадження відповідно до міжнародних стандартів.

Обґрунтовано необхідність внесення системних змін до КПК України, що визначатимуть правовий статус доказів електронної форми, механізми підтвердження їх цілісності та критерії допустимості, процедури їх здобуття а також закріплення механізмів Конвенції про кіберзлочинність. Організаційний напрям концепції спрямовано на створення єдиних процедур поводження з доказами електронної форми. Запропоновано розробити й затвердити СОП щодо роботи з доказами електронної форми, який має визначати порядок ідентифікації, фіксації, збирання, здобуття, передачі та зберігання таких доказів.. У межах інфраструктурного напряму необхідна побудова цифрової архітектури на основі існуючих електронних інформаційних систем органів кримінальної юстиції, що забезпечить зберігання та обмін доказами електронної форми; створення безпечного механізму електронного обміну ними між суб'єктами кримінального провадження – інтегрованої системи управління доказами, що має забезпечити

централізований облік, автоматизований контроль доступу, фіксацію дій уповноважених осіб і формування електронного досьє, синхронізованого з Єдиним реєстром досудових розслідувань та e-Case. У межах техніко-криміналістичного напряму варто стандартизувати формати зберігання доказів електронної форми, методи ідентифікації та застосовувані суб'єктами кримінального провадження інструменти цифрової криміналістики. Пропонується впровадження уніфікації та внутрішньої сертифікації програмних і апаратних засобів, що застосовуються для обробки доказів електронної форми. Освітній напрям передбачає підвищення рівня цифрової компетентності суб'єктів кримінального провадження. Науково-аналітично напрям спрямовано на розширення та інституційну підтримку наукових досліджень за відповідною тематикою, а також забезпечення постійного моніторингу суб'єктами кримінального провадження практики застосування доказів електронної форми.

ВИСНОВКИ

У **дисертації** на основі комплексного аналізу доктринальних положень вітчизняних і зарубіжних учених у галузі права та дотичних спеціальностей, актів національного законодавства, міжнародно-правових документів та сталої кримінальної процесуальної практики правозастосування вирішено важливу наукову проблему, що полягає у науковому обґрунтуванні концептуальних засад інституту доказів електронної форми у кримінальному процесі України, визначенні їх процесуально-правової природи, особливостей джерел походження, порядку ідентифікації, збирання, здобуття, процесуальної фіксації, зберігання і використання, а також у розробленні теоретико-методологічних та організаційно-практичних підходів до вдосконалення кримінального процесуального регулювання діяльності суб'єктів кримінального провадження щодо роботи з такими доказами в умовах глобальної цифровізації, а саме.

1. Категорія доказів у кримінальному процесі України є результатом тривалої еволюції наукової думки та має багатовимірну правову природу. Інтегративний підхід до розуміння доказів у кримінальному процесі України ґрунтується на узгодженні інформаційного, логічного та формально-процесуального вимірів доказування і відображає сучасний стан доктринального осмислення цієї категорії. У такому підході доказ сприймається не як абстрактна інформація чи ізольований факт, а як єдність фактичних даних, їх джерел і процесуальної форми, що набувають доказового значення внаслідок реалізації уповноваженими суб'єктами кримінального провадження передбачених законом процесуальних повноважень. Властивості доказів (належність, допустимість, достовірність і достатність) виступають загальними критеріями їх оцінки незалежно від способу фіксації чи виду матеріального носія. За такого розуміння електронна форма постає не як підстава для виокремлення самостійного виду доказів, а як характеристика способу існування й подання фактичних даних у межах усіх визначених в ст. 84 КПК України процесуальних джерел доказів, специфіка якої проявляється насамперед через розширення можливостей перевірки автентичності та цілісності відомостей як складової забезпечення їх допустимості та достовірності.

2. Електронна складова кримінального процесу України складається з п’яти елементів: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми; електронні інструменти доказування; електронні інструменти реалізації повноважень суб’єктів правозастосування. Розуміння правової природи вказаних елементів та їх неототожнення є передумовою коректного правозастосування.

«Цифровий доказ» відповідає змісту доказу, «електронний доказ» – технічному способу його реалізації, а «доказ електронної форми» – процесуальній формі подання. Нормативна уніфікація понятєвого апарату досліджуваної сфери є необхідною умовою побудови ефективної системи роботи з доказами електронної форми в кримінальному процесі України.

3. Передумови становлення інституту доказів електронної форми в кримінальному процесі України зумовлені як технологічним розвитком, що збільшив обсяг електронних даних у кримінальних провадженнях, так і внутрішньою потребою кримінальної процесуальної науки висвітлити власне бачення нової цифрової реальності. Становлення відповідного інституту характеризується конкуренцією доктринальних підходів (від ототожнення з документами чи речовими доказами до пропозицій їх виокремлення як самостійного процесуального джерела доказів) та значною термінологічною варіативністю. Потреба переосмислення доказів електронної форми у кримінальному процесі України як самостійного інституту вимагає уніфікованого, послідовного, комплексного та технологічно орієнтованого доктринального та нормативного супроводу, заснованого на концептуальному баченні поетапного формування спеціальних процесуальних режимів, уникаючи різких нормативних змін, здатних дестабілізувати систему доказування.

4. Процесуальна природа доказів електронної форми у кримінальному процесі полягає у можливості їх потенційної належності до всіх процесуальних джерел доказів, визначених ст. 84 КПК України. Факт належності доказу досліджуваної категорії до певного процесуального джерела визначає процесуальний порядок поводження з ними під час кримінального провадження та, як наслідок, критерії оцінки його допустимості. Електронна форма фіксації показань (шляхом застосування відеозапису) є допустимим у контексті ст. 225, ч. 11 ст. 615 КПК України способом здобуття релевантного для суду доказу, що не змінює їх особистісної сутності, але висуває додаткові вимоги до автентифікації допитуваної особи, збереження результатів фіксації та перевірки їх цілісності. Документами докази досліджуваної категорії визначаються через призму п. 1 та п. 3 ч. 2 ст. 99 КПК України, а також електронних документів, підписаних КЕП (у розумінні профільного закону). Речові докази репрезентовані фізичними об’єктами – електронними носіями інформації або технічними пристроями, щодо яких доказове значення має саме зафіксована на них інформація, тож їх визнання речовим доказом обумовлене потребою встановлення належного правового режиму при їх вилученні – арештом майна. При цьому слід чітко розмежовувати носій інформації, на якому за допомогою технічних засобів зафіксовано процесуальні дії – як документ (п. 3 ч. 2 ст. 99 КПК України), та матеріальний об’єкт, що охороняється у статусі майна, – як речовий доказ.

Висновок експерта дедалі частіше набуває електронної форми й потребує підписання кваліфікованим електронним підписом, що вимагає забезпечення його належного процесуального оформлення, підтвердження автентичності та відтворюваності.

Технічна природа доказів електронної форми визначається сукупністю характеристик інформаційного середовища, у якому вони створюються та зберігаються, а також властивостями електронних носіїв інформації, що досліджуються під час кримінального провадження. Доказ електронної форми функціонує як чотирирівнева структура: контент, метадані, системна оболонка та електронний носій інформації, що має матеріальне вираження. Запропонована у дослідженні класифікація електронних носіїв інформації (за доступністю, середовищем зберігання, типом пам'яті, ступенем інтеграції з ІС) безпосередньо впливає на вибір процесуальних рішень: підходи до виявлення й вилучення, обґрунтування арешту майна, пріоритизацію фіксації нестабільних даних тощо. Важливими для доказування під час кримінального провадження є технічні аспекти доказів досліджуваної категорії: метадані; розмежування логічного копіювання (окремих файлів) і побітового (криміналістичного) копіювання (створення образу електронного носія інформації); гешування; електронний підпис та електронна позначка часу. Гешування забезпечує відтворювану ідентифікацію цифрового об'єкта та виявлення будь-яких змін, слугуючи технічною основою для підтвердження цілісності та незмінності комп'ютерних даних. Відповідні технічні характеристики доказів електронної форми, що здатні підтвердити автентичність та цілісність цифрових даних, в сукупності з належними кримінальними процесуальними процедурами становлять дуалістичну основу процесуальної допустимості доказів електронної форми у кримінальному провадженні.

5. Комплекс алгоритмів пошуку та фіксації доказів електронної форми об'єднаний за трьома функціонально-структурними категоріями і розглядається як три стратегії фіксації доказів електронної форми у кримінальному процесі України: 1) фізичне вилучення електронних носіїв інформації або комп'ютерних систем; 2) огляд та копіювання комп'ютерних даних; 3) огляд та фіксація інформації з відкритих джерел. Пропонована модель визначає копіювання комп'ютерних даних, здійснене з дотриманням вимог ч. 4 ст. 99 КПК України (за участю спеціаліста) та норм ДСТУ ISO/IEC 27037:2017, пріоритетною та технологічно доцільною альтернативою фізичному вилученню технічних пристроїв. Фіксація інформації з відкритих джерел розглядається як самостійний напрям здобуття доказів електронної форми, що на практиці реалізується через призму огляду (ст. 237) або слідчого експерименту (ст. 240), ґрунтується на використанні методології Протоколу Берклі, програмних засобів OSINT, та, в окремих випадках, застосуванні механізмів Конвенції про кіберзлочинність та процедур міжнародної правової допомоги під час кримінального провадження.

6. Підтвердження цілісності та автентичності доказів електронної форми в кримінальному процесі ґрунтується на поєднанні техніко-криміналістичних інструментів ідентифікації комп'ютерних даних і процесуальних вимог послідовної фіксації й перевірки таких ідентифікаторів, контролю доступу та

забезпеченні безпеки доказів досліджуваної категорії, що вибудовують багаторівневу систему. Ідентифікація комп'ютерних даних під час кримінального провадження розглядається через призму абз. 3 п. 3 ч. 3 ст. 104 КПК України та п. 5.4.2 ДСТУ ISO/IEC 27037:2017 як процесу, покликаного забезпечити встановлення тотожності комп'ютерних даних на всіх стадіях кримінального провадження, підтвердження їх цілісності та автентичності. Практично значущі механізми, що застосовуються для досягнення цієї мети, доцільно систематизувати за ступенем зростання рівня надійності: упакування та маркування електронних носіїв інформації; фіксація загальних та унікальних апаратних ідентифікаторів; опис структури і змісту комп'ютерних даних та їх метаданих; гешування комп'ютерних даних і послідовної фіксації контрольних сум комп'ютерних даних в процесуальних документах; використання КЕП та електронної позначки часу. Системне дослідження концепції chain of custody, її організаційно-технічних моделей засвідчило необхідність її подальших системних досліджень та перспективу інституціоналізації у національній практиці.

7. Ефективність оперування доказами електронної форми у кримінальному процесі України визначається організаційною спроможністю інституцій кримінальної юстиції. Організаційну готовність суб'єктів кримінального провадження до роботи з доказами електронної форми доцільно розглядати через три взаємопов'язані компоненти: 1) матеріально-технічний – охоплює забезпечення органів досудового розслідування, прокуратури та суду цифровими криміналістичними інструментами та інфраструктурою, сумісною з ДСТУ ISO/IEC 27037:2017; 2) кадровий – пов'язаний зі створенням в структурі органів досудового розслідування криміналістичних ІТ-лабораторій для роботи з доказами електронної форми, міждисциплінарною компетентністю слідчих, детективів, прокурорів, спеціалістів, експертів і суддів, їх профільною спеціалізацією та системним підвищенням кваліфікації; 3) нормативний – окреслює необхідність запровадження єдиних стандартів роботи з доказами досліджуваної категорії для всіх суб'єктів кримінального провадження, забезпечення надійного зберігання таких доказів та контролю доступу до них.

8. Роль слідчого у роботі з доказами електронної форми є системоутворювальною: від його фаховості, своєчасних процесуальних рішень і технічно коректної взаємодії з цифровим середовищем залежить доказова спроможність отриманих даних. Ефективність такої діяльності передбачає поєднання правових навичок із базовою цифровою грамотністю: розуміння природи комп'ютерних даних і метаданих, механізмів логічного захисту та гешування, відмінностей між логічним і побітовим копіюванням, а також практичне володіння інструментами OSINT для оперативного виявлення релевантних слідів. Протоколи слідчих (розшукових) дій мають відтворювати технічний контекст одержання даних, характеристики електронних носіїв інформації і комп'ютерних систем, спосіб та параметри ідентифікації (геш-значення), а також фіксувати будь-які впливи на цифрове середовище. Процесуально значущим є виважений вибір слідчого між фізичним вилученням носія та копіюванням інформації, що повинен спиратися на сукупність

процесуальних і технічних умов.

9. Прокурор у кримінальному провадженні виступає ключовим суб'єктом забезпечення належного обігу доказів електронної форми, поєднуючи координацію дій слідчого, оперативних підрозділів, спеціаліста й експерта, контроль за дотриманням критеріїв належності, допустимості й достовірності. Його повноваження охоплюють (але не обмежуються): вибір способу одержання відомостей (копіювання інформації чи вилучення носія інформації), фіксацію ідентифікаційних параметрів комп'ютерних даних (зокрема геш-значень) у протоколах, перевірку автентичності електронних документів і електронних підписів, організацію відкриття матеріалів досудового розслідування стороні захисту відповідно до ст. 290 КПК України, а також використання механізмів міжнародної взаємодії. На стадії судового розгляду прокурору необхідно логічно інтегрувати докази електронної форми в структуру обвинувачення, забезпечуючи демонстрацію джерела походження, цілісності та зв'язку з юридично значущими обставинами, у разі потреби — із залученням спеціаліста. Технічні засади роботи мають відповідати вимогам ДСТУ ISO/IEC 27037:2017 та міжнародно визнаній методології належної фіксації даних з відкритих джерел.

10. Захисник у кримінальному провадженні виступає самостійним суб'єктом доказової діяльності щодо доказів електронної форми, реалізуючи гарантоване ч. 2 ст. 22 та ч. 3 ст. 93 КПК України право на їх використання. Ефективність цієї діяльності зумовлюється поєднанням процесуальної активності з технічною спроможністю забезпечити автентичність і цілісність цифрових даних (відповідно до ДСТУ ISO/IEC 27037:2017). На стадії обшуку й доступу до матеріалів (ст. 290 КПК України) пріоритетними є: мінімізація втручання у приватне життя, охорона адвокатської таємниці, вимога надання криміналістичних (побітових) копій і контрольних ідентифікаторів, а також своєчасного та ефективного реагування на процесуальні порушення.

11. Слідчий суддя та суд формують єдиний контур процесуального контролю за доказами електронної форми: перший – через попереднє санкціонування втручання у цифрове середовище і визначення обмежень щодо цифрових пристроїв, другий – через дослідження доказів електронної форми та перевірку їх належності, допустимості, достовірності та достатності. Ключовими орієнтирами є техніко-правові критерії: наявність у процесуальних документах і збіг геш-ідентифікаторів комп'ютерних даних, перевірюваність метаданих, відповідність процедур ідентифікації, збирання, здобуття та зберігання стандартам ДСТУ ISO/IEC 27037:2017. Перевага має надаватися криміналістичним (побітовим) копіям як об'єктам аналізу, тоді як дослідження оригінального пристрою допустиме лише за умов, що не створюють ризику цілісності доказу. Окремої уваги потребують електронні документи (включно з КЕП і позначкою часу), матеріали з відкритих джерел та докази, одержані за результатами міжнародної правової допомоги – перевірка їх походження та процесуальної легітимності.

12. У сучасному кримінальному процесі докази в електронній формі зумовлюють інституціалізацію спеціальних технічних знань і виокремлення автономних, але інтегрованих суб'єктів їх опрацювання — насамперед експертів,

спеціалістів (з цифрової криміналістики, цифрової безпеки, OSINT-аналітиків та інших). Процесуальна роль експерта фокусується на науково вивіреному дослідженні, використанні атестованих методик та формулюванні висновку експерта. Спеціаліст виконує технічну функцію «першої ланки» (DEFR): ідентифікація, фіксація, збереження та первинний аналіз цифрових слідів відповідно до ДСТУ ISO/IEC 27037:2017, із процесуальною фіксацією його участі й результатів. Чітке розмежування компетенцій цих суб'єктів оптимізує навантаження експертних установ і скорочує строки провадження; натомість їх змішування породжує процесуальні ризики перевантаження експертних установ та втрату релевантних цифрових даних. Залучення OSINT-аналітиків як спеціалістів для пошуку відомостей з відкритих джерел є доцільним за умови належної процесуальної фіксації та дотримання методології Протоколу Берклі.

13. Протокол Берклі забезпечує релевантну для кримінального процесу України методологію ведення розслідувань з використанням відкритих цифрових даних, поєднуючи організаційні, етичні й технічні стандарти. Їх впровадження покликане підвищити якість OSINT-матеріалів, знизити ризики визнання відповідних доказів недопустимими та посилити безпеку суб'єктів правозастосування. Для належної фіксації інформації з відкритого джерела під час кримінального провадження в протоколі огляду необхідно відобразити відомості, визначені в п. 155 Протоколу Берклі. Водночас варто зауважити розрив між практикою буквального використання терміна «Протокол Берклі» щодо таких протоколів огляду й реальним дотриманням його вимог, а також відсутність у КПК України уніфікованого процесуального порядку роботи з даними з відкритих джерел зумовлюють потребу нормативної деталізації. Судова рецепція Протоколу Берклі (2025) та рекомендації ОГП (2021) свідчать про позитивну динаміку, однак повноцінна інтеграція потребує поєднання нормативних змін, підготовки кадрів і матеріально-технічного забезпечення, що у підсумку сформує сталу технологію доказування в умовах цифровізації.

14. Конвенція про кіберзлочинність вибудовує цілісний процесуальний каркас міждержавної взаємодії у контексті роботи з доказами електронної форми. У КПК України відповідні інструменти частково імплементовано, однак зберігаються ключові прогалини: 1) знайшли відображення в КПК України: поширення обшуку за межі комп'ютерної системи, яка є об'єктом первинного втручання (ч. 2 ст. 19 Конвенції) – абз. 2 ч. 6 ст. 236 КПК України; 2) не імплементовано, але можуть бути реалізовані за допомогою існуючих процедур: термінове збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29), та порядок представлення (ст. 18) – частково через тимчасовий доступ до речей і документів (Глава 15 КПК України), перехоплення змісту даних, що передаються (ст. 21 Конвенції) – ст.ст. 263, 264 КПК України; 3) потребують імплементації в КПК України: термінове збереження і часткове розкриття даних про рух інформації (ст.ст. 17, 30), збирання даних про рух інформації у режимі реального часу (ст. 20); добровільне надання інформації (ст. 26). Другий додатковий протокол поглиблює співпрацю (прямі звернення до провайдерів, прискорені процедури, надзвичайні ситуації, стандарти захисту даних) і задає вектор подальшої гармонізації КПК України (після ратифікації).

Оптимальною вбачається комплексна імплементація: 1) кодифікація термінового збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29), термінового збереження і часткового розкриття даних про рух інформації (ст.ст. 17, 30), збирання даних про рух інформації у режимі реального часу (ст. 20); добровільного надання інформації (ст. 26); 2) процесуальна модель production order для комп'ютерних даних і відомостей про користувача; 3) чіткі гарантії пропорційності для збору трафіку в реальному часі та перехоплення контенту; 4) унормування взаємодії органів досудового розслідування з національним контактним пунктом 24/7. Системне впровадження цих механізмів забезпечить ефективність доказування з належним балансом прав людини й інтересів кримінального переслідування.

15. ISO/IEC 27037:2012, інтегрований у Європі як EN ISO/IEC 27037:2016 та імплементований в Україні через ДСТУ ISO/IEC 27037:2017, формує методологічне ядро поводження з доказами електронної форми: ідентифікація, збирання, здобуття (копіювання) та збереження із забезпеченням цілісності, відтворюваності й верифікованості. Українська правозастосовна практика, попри наявність указаного ДСТУ, стикається з нормативною лакуною КПК України щодо розмежування процесів ідентифікації, збирання та здобуття доказів електронної форми, процесуального закріплення ролей DEFR та DES, фіксації ланцюга збереження тощо. Необхідними заходами в цьому напрямі визначено таке: 1) процесуальна легітимація основних підходів ДСТУ ISO/IEC27037:2017 у КПК України; 2) відображення процедур ДСТУ ISO/IEC 27037:2017 в СОП; 3) інституціоналізація ролей DEFR та DES і вимог до їх компетентності; 4) системне навчання оперативних працівників, слідчих та прокурорів роботі з доказами електронної форми відповідно до вимог ДСТУ ISO/IEC 27037:2017 для можливості виконання функцій DEFR.

16. Порівняльний аналіз зарубіжного досвіду засвідчує, що докази електронної форми перетворилися на системоутворювальний елемент кримінального провадження, а ефективність їх використання зумовлюється поєднанням чітких процесуальних рамок, інституційної спроможності та транснаціональної взаємодії. ЄС запроваджує наднаціональну модель (пакет e-evidence) з прямою адресацією до провайдерів і вбудованими гарантіями прав людини, англо-американські юрисдикції забезпечують гнучкість через прецедент і професійні стандарти, натомість континентальні системи формують детальні механізми процесуального контролю. Основні виклики у цій сфері проявляються через колізії юрисдикцій, потребу підтвердження автентичності даних та фіксації ланцюга збереження доказів, загрози кібербезпеки і потребу стандартизації процесуальних процедур.

Варто визначити тенденції зарубіжного досвіду правового регулювання щодо досліджуваного предмета, серед яких: інституціоналізація правового режиму доказів електронної форми у межах кримінального процесуального законодавства; утвердження технологічно нейтрального підходу до їх оцінки та допустимості (відсутність вимог визначених технічних засобів чи форматів); посилення вимог до автентичності, цілісності й простежуваності; запровадження

спеціальних процесуальних механізмів для їх збирання, збереження та перевірки; уніфікація національних підходів із міжнародними стандартами.

У сфері міжнародного обміну доказами електронної форми перспективними напрямами розвитку є: 1) створення комплексної та надійної системи їх захисту; 2) розроблення й уніфікації стандартних протоколів та процедур для гармонізації правових аспектів обміну доказами електронної форми між різними юрисдикціями; 3) впровадження сучасних систем управління доказами, що забезпечують автоматизовану фіксацію, відстеження та аналіз усіх взаємодій з ними.

17. Удосконалення організаційних засад роботи з доказами електронної форми є важливим чинником адаптації кримінального процесу України до цифрової доби. Ефективність цього напряму визначається рівнем матеріально-технічного забезпечення суб'єктів кримінального провадження, наявністю кваліфікованих кадрів і спроможністю до міжвідомчої взаємодії. Підготовка спеціалізованих кадрів, створення криміналістичних ІТ-лабораторій, а також впровадження міждисциплінарних програм навчання формують основу інституційної спроможності системи кримінальної юстиції. Стандартизація діяльності суб'єктів кримінального провадження через розроблення СОП забезпечує єдність практики, передбачуваність дій і зменшує ризики втрати чи спотворення доказів. Водночас розбудова системи міжвідомчої координації, цифровізації процедур тимчасового доступу до речей і документів та створення захищених цифрових сховищ, підтвердження цілісності даних шляхом фіксації їх геш-ідентифікаторів, запровадження обов'язкового резервного копіювання та криптографічного захисту сприяють збереженню цілісності та конфіденційності доказів електронної форми.

18. Процесуальне вдосконалення роботи з доказами електронної форми передбачає розвиток нормативної бази зі збереженням балансу між правовою визначеністю та технічною адаптивністю, запобіганням надмірній формалізації процедур і, водночас, гарантуванням автентичності, цілісності і допустимості доказів цієї категорії. Запропоновані зміни до КПК України передбачають поетапне впровадження міжнародних стандартів Конвенції про кіберзлочинність та актів ЄС. Визначальним є закріплення базових дефініцій, унормування ідентифікації комп'ютерних даних на основі їх гешування, створення цифрових архівів, впровадження практики фіксації ланцюга збереження доказів (chain of custody), регламентації «віртуального огляду» та використання його результатів як доказів та інше. Поетапне запровадження відповідних положень має супроводжуватися навчанням суб'єктів кримінального провадження, розробленням СОП і створенням міжвідомчих механізмів координації.

19. Технічне вдосконалення роботи з доказами електронної форми спрямоване на ефективне їх використання і потребує створення інфраструктури, що охоплює сертифіковані системи ідентифікації та зберігання. Упровадження цифрових протоколів слідчих дій, резервного копіювання та централізованих сховищ із багаторівневим шифруванням забезпечує збереження й контрольованість електронних даних протягом усього процесуального циклу. Використання геш-ідентифікаторів комп'ютерних даних як процесуального

реквізиту протоколу слідчих (розшукових) дій, підкріпленого кваліфікованим електронним підписом, створює об'єктивний механізм перевірки автентичності та цілісності доказів електронної форми. Уніфікація технічних вимог, сертифікація програмних засобів і нормативне закріплення процедур цифрової обробки доказів електронної форми становлять основу для формування цілісної державної політики у відповідній сфері.

20. Концепція вдосконалення інституту доказів електронної форми у кримінальному процесі України спрямована на створення єдиного науково обґрунтованого та технологічно інтегрованого механізму їх процесуального обігу. Її сутність полягає у комплексному розвитку нормативних, організаційних, інфраструктурних, техніко-криміналістичних, освітніх та науково-аналітичних напрямів. Концепція передбачає законодавче унормування критеріїв їх допустимості, установлення уніфікованого порядку їх ідентифікації, фіксації та дослідження. Інфраструктурний та техніко-криміналістичний компоненти передбачають стандартизацію форматів зберігання, сертифікацію програмних засобів і створення інтегрованої системи управління доказами, синхронізованої з національними реєстрами. Освітній напрям орієнтований на фахову підготовку суб'єктів кримінального провадження, а науково-аналітичний – на запровадження постійного аналізу стану правозастосування й оновлення методичних стандартів. Реалізація цієї концепції забезпечить підвищення ефективності електронного сегменту доказування, зміцнить гарантії прав учасників процесу та гармонізує національну практику з міжнародними стандартами кримінальної юстиції.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Монографія

1. Каланча І. Г. Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект : монографія. Київ : Вид-во «SBA Print», 2025. 528 с.

Рецензія: Цимбал Г. П. Рецензія на монографію Каланчі Інги Георгіївни «Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект». *Європейський правничий часопис*. №10. С. 11–13.

Публікації у виданнях, які включено до наукометричних баз Scopus і Web of Science:

1. Patreliuk D., Svoboda I., Kalancha I., Filashkin V., Kachmar B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences.* 22(2). 2024. pp. 4811–4820. URL: https://www.scopus.com/pages/publications/85204286465.

2. Kozii V.; Kalancha I.; Vlasova H.; Orlean A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal.* no. 42. 2025. pp. 1-13. URL: https://www.scopus.com/pages/publications/85217974797.

3. Kalancha I., Bozhyk V., Muzychenko O., Vatsiyk V. Digital evidence in comparative criminal procedure: international experience and the practice of judicial review. *TPM – Testing, Psychometrics, Methodology in Applied Psychology*. Vol. 32, No. S2. 2025. pp. 34-46. URL: https://www.scopus.com/pages/publications/105013864919.

Публікації у фахових періодичних виданнях України (категорія «Б»):

1. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. № 59. 2019. С. 117–121. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2020/12/No.59-2.pdf.

2. Каланча І. Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*. № 3. 2019. С. 212–216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf.

3. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. Вип. 146. 2019. С. 179–191. URL: https://doi.org/10.21564/2414-990x.146.171218.

4. Каланча І. Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 4. 2019. С. 161–166. URL: https://doi.org/10.31733/2078-3566-2019-4-161-166.

5. Каланча І. Г. Роль правових актів Європейського суду з прав людини в кримінальному процесі України. *Проблеми законності*. Вип. 150. 2020. С. 233–243. URL: https://doi.org/10.21564/2414-990x.150.209071.

6. Каланча І. Г. Тенденції та динаміка застосування практики Європейського суду з прав людини під час кримінального провадження: статистичне та соціологічне дослідження. *Теорія і практика правознавства*. Вип. 2(18). 2020. С. 1–17. URL: https://doi.org/10.21564/2225-6555.2020.18.213676.

7. Каланча І. Г. Поняття практики Європейського суду з прав людини як джерела кримінального процесуального права України. *Вісник кримінального судочинства*. № 2. 2020. С. 8–21. URL: https://doi.org/10.17721/2413-5372.2020.3-4/8-21.

8. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91–95. URL: http://apnl.dnu.in.ua/1_2020/23.pdf.

9. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 1. 2020. С. 205–210. URL: https://visnik.dduvs.edu.ua/index.php/visnyk/issue/view/48/19.

10. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65. 2020. С. 90–100. URL: https://digest.kndise.gov.ua/wp-content/uploads/2025/07/2020_65.pdf.

11. Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. № 8. 2021. С. 336–339.

URL: https://doi.org/10.32782/2524-0374/2021-8/77.

12. Каланча І. Г., Орлеан А. М. Адаптація системи кримінальної юстиції до цифровізації світу: роль навчального компоненту. *Наукові перспективи*. № 11(53). 2024. С. 937–944. URL: https://doi.org/10.52058/2708-7530-2024-11(53)-937-944.

13. Каланча І. Г., Юрчишин Ю. В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6. 2024. С. 108–115. URL: https://doi.org/10.32782/TNU-2707-0581/2024.6/19.

14. Каланча І. Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*. Вип. 4. 2024. С. 69–74. URL: https://doi.org/10.32782/LST/2024-4-13.

15. Каланча І. Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження. *Успіхи і досягнення у науці*. № 1 (11). 2025. С. 76–93. URL: https://doi.org/10.52058/3041-1254-2025-1(11)-76-93.

16. Каланча І. Г., Стемковський Д. Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство*. № 2. 2025. С. 1001–1008. URL: https://doi.org/10.24144/2788-6018.2025.02.148.

17. Каланча І. Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. № 2. 2025. С. 84–92. URL: https://doi.org/10.32782/2311-8040/2025-2-12.

18. Каланча І. Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85–92. URL: https://doi.org/10.25313/2520-2308-2025-7-11208.

19. Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90. Ч. 4. 2025. С. 258–266. URL: https://doi.org/10.24144/2307-3322.2025.90.4.36.

Публікації у періодичних виданнях іноземних держав:

1. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. № 1 (41). 2020. С. 132–137. URL: http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf.

2. Каланча І. Г. Інтероперабельність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zborník vedeckých prác*. (Рочник Українсько-Словацький. Збірник наукових праць) 2020. С. 64–70. URL: https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf.

3. Каланча І. Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8 (51). 2025. С. 206–230. URL: https://doi.org/10.52058/2695-1592-2025-

8(51)-206-230.

Тези виступів на науково-практичних конференціях:

1. Каланча І. Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матер. міжнарод наук.-практ. конф. (м. Київ, 05.11.2019 р.). Київ, 2019. С. 209–213.

2. Каланча І. Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: матеріали І Міжнар. наук.-практ. інтернет-конференції (наукове видання), 17–18 листопада 2020 р.: у 2 ч. Київ : НТУ, 2020. Ч. 2. С. 209–212.

3. Гаркуша А. М., Каланча І. Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів : Львівський державний університет внутрішніх справ, 2021. С. 159–165.

4. Каланча І. Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: матер. V Міжнар. наук.-практ. конф. (29 жовтня 2021 р., Чернівці) / редкол.: О. В. Щербанюк та ін. Чернівці: 2021. С. 211–213.

5. Гаркуша А. М., Каланча І. Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез Міжнар. наук.-практ. конф. (м. Чернівці, 9 грудня 2021 р.). Чернівці : Технодрук, С. 72–75.

6. Каланча І. Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: матер. VI Міжнар. наук.-практ. конф. (21 жовтня 2022 р., Чернівці) / редкол.: О. В. Щербанюк та ін. Чернівці, 2022. С. 327–332.

7. Каланча І. Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *ІІІ Наукові читання пам'яті Ганса Гросса* : збірник тез міжнар. наук.-практ. конф. (м. Чернівці, 8 грудня 2023 р.). Чернівці: Чернівец. нац. у-нт ім. Ю.Федьковича, 2023. С. 71–75.

8. Каланча І. Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023 р., Чернівці) / редкол.: О. В. Щербанюк та ін. Чернівці: 2023. С. 253–258.

9. Каланча І. Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини* : зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А. Ю. Нашинець-Наумова, Г. П. Власова, С. В. Бобровник, Т. О. Дідич, Н. А. Сергієнко, А. П. Чернега. Київ : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115–119.

10. Каланча І. Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні* : матер. VIII Міжнар. наук.-практ. конф. (31 жовтня 2024 р., Чернівці) / редкол.: О. В. Щербанюк та ін. Чернівці: 2024. С. 229–233.

11. Каланча І. Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні*: X круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). *Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А. Ю. Нашинець-Наумова, Г. П. Цимбал, С. В. Бобровник, Т. О. Дідич, О. І. Чаплюк, А. П. Чернега. Київ : Київ. столич. ун-т імені Б. Грінченка, 2025. С. 63–67.

12. Каланча І. Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К. А. Возняковська. Том 1, Чернівці, 2024. С. 43–49.

13. Каланча І. Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства*: збірник матеріалів Міжнар. наук.-практ. конф., м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154–156.

14. Каланча І. Г. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти*: матер. XV Міжнар. наук.-практ. конф. (м. Львів, 9–10 травня 2025 року). Львів : Львівський науковий форум, 2025. С. 195–197.

15. Власова Г. П., Каланча І. Г. Захисник як суб’єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи* : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13–15 червня 2025 р. / Уклад. Джурак Л. М. Луцьк : Вежа-Друк, 2025. С. 113–115.

Праці, які додатково відображають результати дослідження:

1. Каланча І. Г. Організація навчання представників органів кримінальної юстиції сучасним процесуально-цифровим компетентностям. Training legal professionals following European standards: scientific and pedagogical internship, November 4 – December 15, 2024. Riga, the Republic of Latvia. p.p. 45-50.

2. Каланча І. Г., Щербанюк О. В. Досудовий процес. Навчально-методичний посібник. Чернівці: Рута. Чернівецький національний університет імені Юрія Федьковича, 2020. 200 с.

3. Шевчук П. В., Каланча І. Г. Кримінальний процес : навчально-методичний посібник для здобувачів вищої освіти першого (бакалаврського) рівня; галузь знань – 08 «Право»; спеціальність – 081 «Право». Чернівці, 2024. 184 с.