УДК 343.1:343.98:004.056(477)

Сиза Наталія Петрівна – кандидатка юридичних наук, доцентка,
головна наукова співробітниця науково-організаційного центру
Національної академії Служби безпеки України
м. Київ, Україна
https://orcid.org/*0000-0001-5850-4023*
syzyy@ukr.net

DOI: *https://doi.org/10.17721/2413-5372.2025.1-2/103-122*

Використання цифрових доказів у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України

Стаття присвячена комплексному дослідженню теоретичних, нормативних та практичних аспектів використання цифрових доказів у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України. У контексті зростання гібридних загроз, активізації розвідувально-підривної діяльності та розширення використання захищених цифрових платформ, цифрові докази перетворюються на домінантне джерело фактичних даних. У роботі розкрито природу цифрової інформації, її відмінність від традиційних речових та документальних доказів, а також особливості її існування, пов'язані з нематеріальністю, мінливістю та залежністю від технічного середовища.

Проаналізовано доктринальні підходи до розуміння електронних доказів, зокрема позиції українських учених щодо критеріїв автентичності, цілісності, незмінності та простежуваності цифрових даних. Висвітлено роль оперативно-розшукової діяльності та негласних слідчих (розшукових) дій у формуванні цифрових доказів, з урахуванням особливостей їх використання у провадженнях із підвищеним рівнем секретності та ризиком протидії з боку суб'єктів злочинної діяльності. Значна увага приділена судовим і прокурорським механізмам контролю за законністю втручання у приватну сферу особи, аналізу відповідності процесуальних процедур стандартам ЄСПЛ, а також ролі захисника у забезпеченні доброчесності доказування й перевірці допустимості результатів НСРД.

На основі дослідження сформульовано висновки щодо потреби у вдосконаленні національного законодавства, стандартизації технічних процедур роботи з цифровими доказами та розробленні спеціальної моделі доказування у справах, що стосуються національної безпеки. Запропоновано напрями подальших наукових розвідок, пов'язані з підвищенням надійності цифрової криміналістики, забезпеченням балансу між таємністю та правом на захист, а також інтеграцією міжнародних стандартів у національний правопорядок.

Ключові слова: *цифрові докази; електронні докази; негласні слідчі (розшукові) дії; оперативно-розшукова діяльність; національна безпека; державна таємниця; автентичність; допустимість; судовий контроль; прокурорський нагляд; захисник; доказування.*

Вступ.

Стрімка цифровізація суспільства та зростання ролі інформаційно-комунікаційних технологій у всіх сферах життєдіяльності зумовили трансформацію способів підготовки, вчинення та маскування кримінальних правопорушень проти основ національної безпеки України. У сучасних умовах гібридних загроз, розвідувально-підривної діяльності,

кібератак, дистанційно координованих диверсій та використання закритих платформ електронної комунікації цифрова інформація стає основним масивом фактичних даних, що мають доказове значення (Крицька, 2016; Метелев, 2018). Розслідування кримінальних правопорушень цієї категорії неможливе без здатності органів правопорядку виявляти, фіксувати, вилучати та зберігати цифрові сліди, що формуються у мережевих середовищах, інформаційних системах, криптографічних каналах комунікації та інших прихованих цифрових екосистемах.

Попри очевидну актуальність цифрових доказів, чинне кримінальне процесуальне законодавство України не містить їх нормативного визначення, що спричиняє низку труднощів у правозастосуванні – від невизначеності процесуального статусу результатів оперативно-розшукової діяльності та негласних слідчих (розшукових) дій до проблем автентифікації, фіксації та оцінки цифрової інформації в суді (Гуцалюк, Антонюк, 2020; Гарасимів, Марко, Ряшко, 2023). Наявна судова практика лише окреслює окремі підходи до визнання цифрових документів оригіналами, визначення меж допустимості та перевірки цілісності цифрових файлів, проте не формує цілісної моделі їх використання у кримінальному провадженні (Об'єднана палата ККС ВС, 2021).

Проблематика набуває особливої ваги у провадженнях щодо кримінальних правопорушень проти основ національної безпеки України, де цифрові докази здобуваються переважно шляхом застосування спеціальних технічних засобів, ОРД та НСРД, нерідко у режимі державної таємниці та за умов підвищеного ризику технічної протидії з боку суб'єктів злочинної діяльності (Погорецький, 2008; Погорецький, 2009а). З огляду на це особливого значення набувають питання законності втручання, пропорційності застосованих засобів, судового та прокурорського контролю, а також ролі сторони захисту у забезпеченні доброчесності цифрових доказів (Погорецький, Іскендеров, 2021; Погорецький, Гриценко, 2012).

У науковій доктрині спостерігається суттєве зростання зацікавленості до цифрових доказів, проте багато аспектів їх використання у кримінальних провадженнях цієї категорії залишаються недостатньо дослідженими. Зокрема, не вироблено цілісної моделі взаємодії між інструментарієм НСРД, оперативною інформацією та процесуальними джерелами доказів; не визначено алгоритмів судової перевірки технічних процедур отримання цифрових даних; не врегульовано підходів до роботи з доказами, що становлять державну таємницю; відсутні стандарти доброчесності цифрових матеріалів та незалежної експертної верифікації (Погорецький, Сухачова, 2010; Погорецький, Старенький, 2018).

Підвищена актуальність теми зумовлена також необхідністю узгодження національних стандартів цифрового доказування зі стандартами ЄСПЛ щодо законності та пропорційності втручання у цифрову приватність, сформульованими у справах Roman Zakharov v. Russia та Big Brother Watch and Others v. the United Kingdom (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021).

З огляду на зазначене, виникає об'єктивна потреба у комплексному науковому осмисленні правової природи цифрових доказів, особливостей їх отримання у провадженнях щодо кримінальних правопорушень проти основ національної безпеки, визначенні гарантій їх допустимості та виробленні пропозицій щодо вдосконалення законодавства і практики. Саме тому метою цієї статті є формування науково обґрунтованого підходу до регламентації цифрових доказів у кримінальному процесі з урахуванням специфічних потреб національної безпеки, сучасних технологічних викликів та стандартів Європейського суду з прав людини.

Аналіз останніх досліджень і публікацій.

Питання правової природи, класифікації та процесуального режиму цифрових доказів уже тривалий час перебувають у центрі уваги сучасної кримінальної процесуальної науки. Одним із ключових напрямів цих досліджень є з'ясування співвідношення матеріальних носіїв, електронної інформації та процесуальних джерел доказів, а також вироблення критеріїв для їх відмежування. Вагомим внеском у цей напрям стала праця І. Крицької, яка запропонувала концептуальне розмежування цифрової інформації та речових доказів і визначила критерії їх належності до відповідних процесуальних категорій (Крицька, 2016).

Розвиток теорії цифрових доказів дістав продовження у роботах М. Гуцалюка та П. Антонюка, які обґрунтували необхідність нормативного закріплення поняття «електронна (цифрова) інформація» як окремого виду доказової інформації та наголосили на особливих вимогах до її фіксації, дослідження та процесуальної легалізації (Гуцалюк, Антонюк, 2020). Гносеологічні засади цифрових доказів та їхня принципова відмінність від матеріальних носіїв знайшли глибоке відображення у працях О. Метелева, який підкреслив нематеріальний характер цифрових артефактів, їх копійованість та залежність від програмно-технічної інфраструктури (Метелев, 2018).

Комплексний аналіз електронних джерел доказової інформації та проблем їх практичного використання здійснено у роботах О. Гарасиміва, С. Марка та О. Ряшка, які зосередили увагу на питаннях автентичності, несталій природі цифрових даних та труднощах їх подальшої оцінки в суді (Гарасимів, Марко, Ряшко, 2023). Практичний вимір ідентифікації, збору та збереження цифрових доказів відображено у Національному стандарті України щодо методів роботи з цифровими доказами (НСТУ, 2017), який визначає технічні вимоги до забезпечення цілісності, достовірності та простежуваності ланцюга збереження.

Закон України «Про електронні документи та електронний документообіг» створює нормативний фундамент для розуміння правового статусу електронних документів та принципів їх автентичності. Ці положення отримали подальший розвиток у практиці Верховного Суду, зокрема в постанові Об'єднаної палати Касаційного кримінального суду від 29 березня 2021 року, де Суд сформулював підхід до визнання електронних документів оригіналами й підкреслив неприпустимість обмеження їх доказової сили лише через цифрову форму (Об'єднана палата ККС ВС, 2021).

Міжнародні стандарти використання цифрової інформації у кримінальному провадженні, особливо у контексті втручання в приватне життя, були сформовані Європейським судом з прав людини у справах Roman Zakharov v. Russia та Big Brother Watch and Others v. the United Kingdom, де ЄСПЛ визначив обов'язкові критерії якості закону, необхідності, пропорційності, незалежного контролю та мінімізації збирання інформації (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021).

У вітчизняній доктрині основу системного аналізу цифрових доказів, результатів оперативно-розшукових заходів (ОРД) та негласних слідчих (розшукових) дій (НСРД) становлять праці проф. М.А. Погорецького. Дослідник послідовно розкриває функціональне призначення ОРД та НСРД і обґрунтовує необхідність чіткої процесуальної регламентації їх результатів у доказуванні (Погорецький, 2003; Погорецький, 2011; Погорецький, 2013). Особливе значення мають його дослідження щодо легалізації оперативної інформації та меж її використання у кримінальному процесі (Погорецький, 2006; Шумило, Погорецький, 2001).

Водночас важливими для сучасного дослідження цифрових доказів є праці, присвячені питанням прокурорського

нагляду (Погорецький, Сухачова, 2010), ролі прокурора при проведенні НСРД (Погорецький, Іскендеров, 2021), а також співвідношенню мети та завдань ОРД і кримінального процесу (Погорецький, 2008). У дослідженнях, присвячених державній таємниці, окреслюються специфічні процесуальні обмеження та гарантії, характерні для проваджень щодо злочинів проти основ національної безпеки України, де цифрові докази можуть створювати підвищені ризики розголошення чутливої інформації (Погорецький, 2009а; Погорецький, 2009б).

Окремо слід відзначити роботи, що стосуються права на справедливий суд в контексті цифрових доказів (Погорецький, Гриценко, 2012), а також аналізу кіберпростору як середовища вчинення злочинів, що є безпосереднім підґрунтям для дослідження цифрових слідів та їхніх властивостей у кримінальному провадженні (Погорецький, Шеломенцев, 2009).

У новітніх працях проф. М.А. Погорецький аналізує використання сучасних технологій у доказуванні, включно з OSINT, супутниковими знімками, цифровою трасологією та алгоритмами обробки великих масивів даних, що формує сучасну методологічну основу для роботи з технологічно складними видами цифрових доказів (Погорецький, 2023).

Попри значний масив напрацювань, низка аспектів використання цифрових доказів у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України залишається недостатньо дослідженою. Зокрема, відсутнім є системний аналіз: специфіки формування та використання цифрової інформації в середовищах підвищеної секретності; особливостей доказової релевантності цифрових слідів, отриманих у закритих комунікаційних мережах та захищених сервісах; механізмів забезпечення незмінності цифрових даних під час НСРД у процесах протидії розвідувально-підривній діяльності; алгоритмів судової перевірки допустимості цифрових доказів, отриманих шляхом спеціальних технічних заходів органів безпеки.

Саме брак комплексного підходу до використання цифрових доказів у провадженнях щодо кримінальних правопорушень проти основ національної безпеки обумовив актуальність і необхідність дослідження цієї проблематики. Зростання ролі цифрової інформації у структурі доказової бази, поєднання технічної складності таких даних із підвищеним режимом секретності та недостатня нормативна деталізація створюють ризики для забезпечення стандартів справедливого суду, дотримання прав людини та ефективного кримінального переслідування. Саме тому авторка звертається до зазначеної проблематики з метою формування науково обґрунтованої моделі використання цифрових доказів, узгодженої зі стандартами Верховного Суду, ЄСПЛ та сучасної криміналістичної теорії.

Мета і завдання дослідження.

З огляду на виявлені прогалини у теоретичному осмисленні та нормативному регулюванні використання цифрових доказів у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України, ***метою*** статті є формування науково обґрунтованої концепції їх отримання, фіксації, збереження та процесуальної оцінки з урахуванням особливостей таких проваджень, а також узгодження національної моделі з актуальними стандартами Верховного Суду та Європейського суду з прав людини.

Завданням дослідження є: з'ясування теоретичної природи цифрових доказів та визначення їх місця у системі процесуальних джерел доказів; аналіз сучасного стану наукової розробки проблеми у вітчизняній і зарубіжній доктрині з виокремленням аспектів, що залишаються недостатньо дослідженими; характеристика особливостей отримання цифрових доказів, зокрема у ході негласних слідчих (розшукових) дій, із наголосом на вимогах автентичності,

цілісності та простежуваності ланцюга збереження; дослідження нормативних засад використання цифрових доказів за КПК України, Законом України «Про електронні документи та електронний документообіг» і Національним стандартом щодо роботи з цифровими доказами; аналіз релевантної судової практики Верховного Суду та ЄСПЛ з метою виявлення критеріїв законності й пропорційності втручання в приватне життя під час отримання цифрових даних; встановлення ключових проблем і ризиків, властивих процесу їх збирання, оброблення та оцінки у провадженнях щодо злочинів проти основ національної безпеки; формулювання науково обґрунтованих пропозицій щодо вдосконалення законодавства та практики, спрямованих на підвищення доказової спроможності та процесуальної захищеності цифрових доказів.

Матеріали та методи.

Матеріальну основу дослідження становлять норми Кримінального процесуального кодексу України, Закон України «Про електронні документи та електронний документообіг», Національний стандарт України щодо методів роботи з цифровими доказами, а також акти практичного застосування законодавства: постанови Верховного Суду, зокрема постанова Об'єднаної палати Касаційного кримінального суду щодо статусу електронних документів та допустимості цифрових доказів; рішення Європейського суду з прав людини у справах Roman Zakharov v. Russia та Big Brother Watch and Others v. the United Kingdom, які встановлюють стандарти законності, пропорційності та незалежного контролю при втручанні у сферу приватного життя. У межах дослідження також використано сучасні наукові праці, присвячені природі цифрових доказів, результатам оперативно-розшукових заходів і негласних слідчих (розшукових) дій, доказуванню у справах щодо кримінальних правопорушень проти основ національної безпеки, а також роботам, що висвітлюють роль прокурора, питання державної таємниці та специфіку збору цифрової інформації в умовах підвищеного режиму секретності.

Методологічну основу дослідження складає комплекс загальнонаукових та спеціально-правових методів, застосованих у взаємозв'язку і взаємодоповненні. Формально-логічний метод використано для з'ясування змісту цифрових доказів, їх ознак та структури, а також для аналізу юридичної техніки норм, що регламентують їх отримання та використання у кримінальному провадженні. Системно-структурний метод дав змогу розглянути цифрові докази як елемент цілісної процесуальної системи, що взаємодіє з інститутами НСРД, ОРД, судового контролю та прокурорського нагляду.

Нормативно-правовий метод застосовано для аналізу положень КПК України, закону про електронні документи та підзаконних актів, що регламентують порядок фіксації, оброблення та збереження цифрової інформації. Порівняльно-правовий метод використано для зіставлення національного регулювання зі стандартами ЄСПЛ, а також для аналізу особливостей роботи з цифровими доказами у провадженнях, пов'язаних із національною безпекою, з урахуванням специфіки доступу до даних та обмежень, пов'язаних із державною таємницею.

Історико-правовий метод дозволив дослідити еволюцію підходів до електронних доказів та результатів НСРД, простежити поступовий перехід від матеріальних носіїв до цифрових форматів, а також оцінити зміни у правозастосовній практиці щодо їх допустимості. Метод аналізу й синтезу забезпечив виокремлення ключових проблем, пов'язаних із автентичністю, збереженням та судовою оцінкою цифрових даних, та сформував підґрунтя для подальших висновків і пропозицій.

Практико-орієнтований підхід, властивий дослідженням у сфері кримінального процесу, застосовано для ін-

терпретації матеріалів судової практики та визначення типових проблем використання цифрових доказів у провадженнях щодо кримінальних правопорушень проти основ національної безпеки. Використання цього підходу дозволило поєднати теоретичні положення з реальними потребами органів досудового розслідування і суду, а також з вимогами забезпечення прав людини та охорони державної таємниці.

У сукупності застосовані матеріали та методи забезпечили всебічне, комплексне й об'єктивне дослідження особливостей отримання, збереження та використання цифрових доказів у кримінальних провадженнях, що стосуються посягань на основи національної безпеки України.

Виклад основного матеріалу.

Передусім зазначимо, що у 2024 році обліковано 33 636 кримінальних правопорушень у провадженнях, досудове розслідування у яких здійснюється органами безпеки. З них – щодо 3 188 кримінальних правопорушень особам вручено повідомлення про підозру; щодо 318 кримінальних правопорушень досудове розслідування зупинено відповідно до ст. 280 Кримінального процесуального кодексу України (КПК України); 2 340 кримінальні правопорушення, за якими провадження направлені до суду (п. п. 2, 3 ст. 283 КПК України); щодо 169 кримінальних правопорушень провадження закрито; щодо 30 975 кримінальних правопорушень на кінець звітного періоду рішення про закінчення або зупинення провадження не прийнято (Єдиний звіт про кримінальні правопорушення за січень-грудень 2024 року).

Серед кримінальних правопорушень, у провадженнях щодо яких досудове розслідування здійснюється органами безпеки, у 2024 році кримінальні правопорушення проти основ національної безпеки України становили 14,4%. Так, у 2024 році обліковано 4 854 кримінальні правопорушення проти основ національної безпеки України. З них – щодо 1 939 кримінальних правопорушень особам вручено повідомлення про підозру; щодо 184 кримінальних правопорушень досудове розслідування зупинено відповідно до ст. 280 КПК України; 1 427 кримінальних правопорушень, за якими провадження направлені до суду (п. п. 2, 3 ст. 283 КПК України); щодо 78 кримінальних правопорушень провадження закрито; щодо 3 240 кримінальних правопорушень на кінець звітного періоду рішення про закінчення або зупинення провадження не прийнято (Єдиний звіт про кримінальні правопорушення за січень-грудень 2024 року).

У структурі кримінальних проваджень (справ), які були розглянуті місцевими загальними судами за 2024 рік з ухваленням вироку, справи про злочини проти основ національної безпеки України (статті 109–114[1] КК України) становили 2,3% або 2,4 тис. Кількість осіб, засуджених за вчинення злочинів проти основ національної безпеки України (за вироками, що набрали законної сили), становила 1 434 або 2,3% від усієї кількості засуджених у 2024 році за вироками, що набрали законної сили (Стан здійснення правосуддя у кримінальних провадженнях та справах про адміністративні правопорушення судами загальної юрисдикції у 2024 році; Аналіз стану здійснення правосуддя у кримінальних провадженнях та справах про адміністративні правопорушення у 2024 році).

Теорія доказів у кримінальному процесі формує базові методологічні параметри, які визначають зміст, місце та функціональне призначення цифрових доказів у структурі доказування. Розширення цифрового середовища, поява нових інформаційних платформ, мережевих сервісів і технічних засобів суттєво трансформували традиційне уявлення про джерела фактичних даних і способи їх отримання. Якщо класична теорія доказів виходила з матеріальної природи носія, то сучасний етап розвитку характеризується поступовим переходом до електронних, динамічних та мінли-

вих інформаційних структур, що потребує якісно інших критеріїв належності, допустимості, достовірності та достатності доказів (Метелев, 2018; Погорецький, 2023).

У цьому контексті цифрові докази наділяються специфічними властивостями – нематеріальністю, залежністю від програмно-технічного середовища, багатокопійністю та можливістю існувати паралельно в різних місцях без втрати автентичності, що вже було відзначено в ранніх дослідженнях українських авторів (Крицька, 2016; Гуцалюк, Антонюк, 2020). Зміна природи носія актуалізує потребу у переосмисленні традиційних категорій «джерело доказів» і «фактичні дані» та переходу від матеріально орієнтованого до інформаційно орієнтованого підходу, у центрі якого – властивості цифрової інформації як такої.

Вагомий внесок у формування методологічних засад використання цифрових доказів зроблено науковою школою проф. М.А. Погорецького. Використовуючи системний підхід, учений розглядає доказування як функціонально впорядкований процес трансформації фактичних даних у доказову інформацію, наголошуючи, що цифрові дані мають бути не лише отримані законним шляхом, а й належним чином легалізовані та інтегровані у процесуальну форму (Погорецький, 2006; Погорецький, 2011; Погорецький, 2013). У його працях окреслено чітке розмежування між оперативною інформацією, результатами ОРД і результатами НСРД, які лише після виконання встановлених законодавством процедур набувають доказового статусу (Шумило, Погорецький, 2001).

Теорія доказів у контексті кримінальних правопорушень проти основ національної безпеки характеризується підвищеним значенням таких категорій, як пропорційність втручання, баланс між інтересами держави та правами людини, стандарти контролю за втручанням у приватне життя. У цьому сенсі ключового значення набувають стандарти Європейського суду з прав людини, які визначають межі допустимості втручання у сферу приватного життя при перехопленні електронних комунікацій. Зокрема, у справах Roman Zakharov v. Russia та Big Brother Watch and Others v. the United Kingdom Суд вказав на обов'язковість чіткої законодавчої бази, ефективного попереднього контролю, незалежності органу, який ухвалює рішення про втручання, та мінімізації обсягу зібраних даних (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021). Ці положення мають безпосереднє значення для використання цифрових доказів у справах, пов'язаних з національною безпекою, де ризики зловживання є особливо високими.

Оскільки цифрова інформація у провадженнях цієї категорії нерідко перетинається з матеріалами, що становлять державну таємницю, теорія доказів повинна враховувати й специфіку процесуальних обмежень, спрямованих на захист секретної інформації. Питання взаємодії доказування з режимом державної таємниці детально проаналізовано в роботах М.А. Погорецького, де підкреслено необхідність забезпечення подвійного балансу – захисту інформації, що має значення для обороноздатності держави, та гарантування права на справедливий суд (Погорецький, 2009а; Погорецький, 2009б; Погорецький, Гриценко, 2012). Саме тут проявляється методологічний принцип поєднання процесуальних гарантій і вимог національної безпеки.

Сучасна теорія доказів також передбачає обов'язковість перевірки цифрової інформації на автентичність, цілісність і незмінність, що особливо підкреслено у практиці Верховного Суду. Постанова Об'єднаної палати Касаційного кримінального суду від 29 березня 2021 року закріплює підхід до електронних документів як до таких, що можуть існувати у множинних автентичних копіях, визнаючи при цьому кожну з них оригіналом за умови підтвердження цілісності (Об'єднана палата ККС ВС, 2021). Цей

підхід збігається з міжнародними стандартами роботи з цифровими доказами.

Таким чином, теорія доказів створює методологічне підґрунтя для дослідження цифрових доказів у кримінальних провадженнях про злочини проти основ національної безпеки, визначаючи принципи їх отримання, легалізації, автентифікації, процесуальної перевірки та інтеграції у доказову систему. Саме ця теоретична рамка дозволяє поєднати вимоги національного законодавства, доктринальні підходи та стандарти ЄСПЛ, що є необхідним для формування цілісного й ефективного механізму використання цифрових доказів у національній безпековій юрисдикції.

Отримання цифрових доказів у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України тісно пов'язане зі застосуванням оперативно-розшукової діяльності та системи негласних слідчих (розшукових) дій. Саме ці інструменти дозволяють виявляти, фіксувати та документувати цифрову інформацію, що перебуває у прихованому інформаційному середовищі, у захищених комунікаційних сервісах або у формах, недоступних під час проведення відкритих слідчих дій. Особливості правового режиму таких проваджень, пов'язані зі специфікою розвідувально-підривної діяльності, конспіративними методами взаємодії суб'єктів злочину та високим рівнем секретності, зумовлюють необхідність переважного використання саме спеціальних технічних форм отримання інформації (Погорецький, 2008).

До основних форм отримання цифрової інформації у межах ОРД та НСРД належить зняття інформації з електронних інформаційних систем, аудіо- та відеоконтроль, перехоплення комунікацій, а також доступ до закритих та захищених інформаційних платформ. Такі дані, як правило, наповнені цифровими слідами: метаданими, журналами активності, геолокаційною інформацією, мережевими логами, історіями комунікацій, файлами та їх цифровими відбитками. Вони формуються у процесі застосування спеціальних технічних засобів, у тому числі сучасних цифрових рішень для обробки великих масивів даних, що дозволяє встановити структуру комунікацій, маршрути передачі інформації та дії учасників відповідних мереж (Гарасимів, Марко, Ряшко, 2023).

Методологічні основи використання таких технічних засобів визначено у Національному стандарті щодо збирання та збереження цифрових доказів, який встановлює вимоги до забезпечення незмінності цифрових артефактів, їх документування та фіксації (НСТУ, 2017). Ці вимоги корелюють з положеннями Закону України «Про електронні документи та електронний документообіг», який визначає критерії автентичності та цілісності електронних документів як доказів (Закон України, 2003). Практика Верховного Суду підтверджує, що електронні документи можуть мати множинні автентичні копії, а тому збереження технічного сліду та контроль над ланцюгом доступу стають ключовими умовами доказової спроможності (Об'єднана палата ККС ВС, 2021).

У сфері протидії кримінальним правопорушенням проти основ національної безпеки оперативно-розшукова діяльність має особливий зміст, зумовлений необхідністю виявлення розвідувально-підривної діяльності, колабораціонізму, шпигунства, диверсій та інших форм діяльності, які реалізуються через складні цифрові екосистеми. Такі кримінальні правопорушення сутнісно пов'язані з використанням закритих каналів комунікації, криптографічного захисту, анонімізованих сервісів та платформ, що об'єктивно унеможливлює отримання доказів відкритими процесуальними засобами.

Особливе значення має робота з інформацією, що становить державну таємницю. У цьому контексті вимоги щодо збереження конфіденційності, режимності та мінімізації кола ознайомлення визначають не лише порядок проведення

ОРД та НСРД, а й специфіку документування цифрових слідів. Як слушно зазначає М.А. Погорецький, у провадженнях цієї категорії цифрові дані часто набувають «подвійного режиму» – доказового та секретного, що потребує особливих процедур легалізації (Погорецький, 2009а; Погорецький, 2009б). Крім того, взаємозв'язок мети та завдань ОРД і кримінального процесу, як підкреслює вчений, формує комплексну модель використання оперативної інформації як потенційного джерела для подальшого її процесуального перетворення (Погорецький, 2008).

Негласні слідчі (розшукові) дії є центральним процесуальним інструментом формування цифрових доказів у справах про кримінальні правопорушення проти основ національної безпеки. Їх застосування підпорядковується принципам необхідності, пропорційності та неможливості здобуття фактичних даних відкритими способами. Саме НСРД забезпечують можливість доступу до інформації, яку неможливо виявити інакше: комунікації через зашифровані канали, приховані мережеві взаємодії, дані з серверів, до яких особа має дистанційний доступ, а також інформацію, що передається у режимі реального часу.

Методологічний підхід до НСРД, розроблений проф. М.А. Погорецьким, передбачає, що результати таких дій повинні бути не лише отримані відповідно до закону, а й документовані у спосіб, який гарантує можливість подальшої перевірки їх походження, автентичності та незмінності. При цьому важливо враховувати роль прокурора як суб'єкта контролю за законністю проведення НСРД (Погорецький, Іскендеров, 2021) та роль суду як первинного фільтра втручання у приватне життя згідно зі стандартами ЄСПЛ (ECtHR Zakharov, 2015).

У підсумку, цифрові докази, отримані внаслідок ОРД і НСРД, становлять ключову доказову основу проваджень щодо кримінальних правопорушень проти основ національної безпеки, а їх використання є можливим лише за умов дотримання підвищених стандартів законності, пропорційності та технологічної достовірності, що забезпечують справедливість і ефективність кримінального процесу.

Визнання результатів оперативно-розшукової діяльності та негласних слідчих (розшукових) дій цифровими доказами можливе лише за умови дотримання комплексу нормативних, судових та доктринальних вимог, які забезпечують їх автентичність, належність і допустимість. Ці вимоги формують основу процесуальної «доказової якості» цифрової інформації, яка завжди є вразливою до модифікації, знищення або спотворення і потребує посилених гарантій фіксації та збереження.

Кримінальний процесуальний кодекс України встановлює загальні вимоги до доказів, які повною мірою поширюються і на цифрові дані. Такі дані визнаються допустимими лише за умови дотримання принципів автентичності, цілісності, незмінності та простежуваності. Автентичність передбачає підтвердження того, що цифрова інформація походить саме з того джерела, яке зазначене у процесуальному документі, та не була змінена сторонніми впливами (Закон України «Про електронні документи та електронний документообіг», 2003).

Цілісність та незмінність забезпечуються шляхом дотримання вимог до технічної фіксації й збереження цифрових файлів, застосуванням хеш-ідентифікаторів, протоколюванням кожної дії з цифровим носієм та використанням сертифікованих технічних засобів. Ці положення докладно конкретизовані у Національному стандарті України щодо методів ідентифікації, збирання, здобуття та збереження цифрових доказів, який встановлює необхідність документування кожного етапу роботи з цифровими даними, що забезпечує їх простежуваність (НСТУ, 2017).

Таким чином, тільки за наявності підтвердженої автентичності, незмінно-

сті та контрольованого ланцюга доступу *(chain of custody*) цифрова інформація, отримана у результаті ОРД або НСРД, може претендувати на статус процесуального доказу.

Практика Верховного Суду має принципове значення для визначення вимог до цифрових доказів. Постанова Об'єднаної палати Касаційного кримінального суду від 29 березня 2021 року сформулювала ключовий підхід до електронних документів: цифровий документ не може визнаватися недопустимим лише через форму його існування; усі ідентичні електронні копії визнаються оригіналами за умови підтвердження їхньої цілісності та незмінності (Об'єднана палата ККС ВС, 2021). Це остаточно закріпило рівність електронних і паперових носіїв у доказовому процесі та підкреслило значення технічних процедур верифікації.

Європейський суд з прав людини визначає додаткові критерії, які особливо важливі для ОРД та НСРД у справах щодо національної безпеки. У рішеннях Roman Zakharov v. Russia та Big Brother Watch and Others v. the United Kingdom ЄСПЛ окреслив чотири ключові стандарти: якість закону, незалежний попередній контроль (насамперед судовий), мінімізація обсягу зібраних даних та обов'язковість забезпечення ефективних процедур перевірки законності втручання (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021). Вони прямо кореспондують до необхідності забезпечення прозорого та контрольованого процесу отримання цифрових доказів у межах НСРД.

Проф. М. А. Погорецький сформулював системну доктрину допустимості результатів ОРД та НСРД, яка має ключове значення для визначення статусу цифрових доказів. На думку вченого, передумовою їх використання є належна легалізація оперативної інформації, що включає її процесуальне оформлення, відмежування від фактичних даних, отриманих у ході слідчих дій, та недопущення підміни оперативного матеріалу доказами без належної трансформації (Погорецький, 2024, 2006, 2007, 2013 2023).

Важливим елементом є розмежування фактичних даних і джерела доказів: цифрова інформація сама по собі не є доказом, доки не буде оформлена відповідно до вимог КПК України, що повністю узгоджується з науковою позицією Погорецького щодо процесуального значення форми (Шумило, Погорецький, 2001; Погорецький, 2023).

Окрема група вимог стосується оформлення результатів НСРД. Воно має відбуватися із забезпеченням технічної фіксації, незмінності цифрових слідів, участі спеціаліста та документуванням усього обсягу операцій з інформацією, що гарантує можливість подальшої судової перевірки її достовірності та походження. Питання належного оформлення та процесуальної легалізації, як підкреслює Погорецький, набувають особливої ваги у провадженнях щодо злочинів проти основ національної безпеки, де цифрові докази часто формуються у режимах підвищеної секретності та обмеженого доступу (Погорецький, 2009а; Погорецький, 2009б).

Тактика отримання цифрових доказів у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України має свою специфіку, обумовлену як природою цифрової інформації, так і підвищеними вимогами до законності, непомітності та безпеки оперативних і процесуальних дій. На відміну від традиційних об'єктів доказування, цифрові сліди формуються в інформаційних системах, можуть бути швидко змінені або знищені, а їх збирання нерідко вимагає доступу до захищених мереж або прихованих каналів комунікації. Це зумовлює необхідність адаптації класичної криміналістичної тактики до умов цифрового середовища, що підкреслюється у вітчизняній доктрині (Метелев, 2018; Гарасимів, Марко, Ряшко, 2023).

У цифровому середовищі тактичні операції орієнтуються не лише на фізич-

не виявлення слідів злочину, а й на реконструкцію інформаційних процесів, що відбуваються у мережевих і електронних системах. Сучасна криміналістична тактика передбачає виявлення, фіксацію і збереження метаданих, логів доступу, мережевої активності, цифрових відбитків, історій комунікацій, геолокаційних слідів та інших артефактів, що відображають поведінку суб'єктів у цифровому просторі. Тактичні прийоми включають швидке блокування каналів передачі даних, фіксацію інформаційних потоків у реальному часі, роботу із зашифрованими форматами та відновлення видалених файлів (НСТУ, 2017).

Наукові підходи останнього десятиліття демонструють, що цифрова інформація має властивість самовідтворюваності і залежності від технічного середовища, що вимагає обов'язкового використання спеціаліста для забезпечення достовірності процесу фіксації (Гуцалюк, Антонюк, 2020). Відтак тактика роботи з цифровими доказами включає одночасне застосування технічних, організаційних та процесуальних засобів, що гарантують отримання даних із дотриманням принципів автентичності, цілісності, простежуваності та незмінності.

У провадженнях щодо кримінальних правопорушень проти основ національної безпеки тактика отримання цифрових доказів ускладнюється додатковими факторами. По-перше, значна частина інформації перебуває у сфері, що становить державну таємницю, або може бути пов'язана з діяльністю органів, які виконують спеціальні завдання у контррозвідувальній чи оперативній площині. Це потребує суворого дотримання режимних вимог, мінімізації кола ознайомлених осіб та використання спеціальних інструментів доступу до закритих ресурсів (Погорецький, 2009а).

По-друге, високий ризик контрдій з боку суб'єктів розвідувально-підривної діяльності зумовлює необхідність посилення прихованості тактичних прийомів, маскування оперативних операцій, застосування багаторівневих схем проникнення до цифрових середовищ, а також безперервного моніторингу кіберповедінки підозрюваних (Погорецький, 2008). Особливої ваги у таких провадженнях набуває тактика упередження – своєчасне фіксування цифрової інформації до її видалення або перетворення, швидке реагування на зміну поведінки суб'єкта, фіксація взаємодій у реальному часі.

По-третє, специфіка цифрових доказів у справах національної безпеки пов'язана з тим, що злочинці часто використовують захищені месенджери, VPN-сервіси, TOR, шифрування end-to-end, криптографічні контейнери, а збирання інформації вимагає особливої технічної тактики, включно з роботою з трафіком, логами серверів, цифровими ключами та обхідними технічними методами, що не порушують вимоги законності (Закон України, 2003; ECtHR Zakharov, 2015).

У працях М. Погорецького спільно з Д. Сергєєвою та О. Стареньким розроблено концепцію тактики проведення НСРД, яка має фундаментальне значення для отримання цифрових доказів. Автори підкреслюють, що тактика НСРД має бути побудована на поєднанні: оперативної інформації; технічних можливостей; процесуальних гарантій; алгоритмів взаємодії між підрозділами (Погорецький, Сергєєва, 2014; Погорецький, Старенький, 2018).

Науковці акцентують, що результат НСРД може бути визнаний доказом лише за умови, що тактичний задум був реалізований з дотриманням вимог законності, а технічні процедури – задокументовані так, щоб забезпечити можливість подальшої перевірки. Тактика проведення НСРД передбачає чітку структуровану послідовність дій: від отримання оперативної інформації до технічного вилучення цифрових даних, складання протоколу, експертної верифікації та збереження цифрових носіїв (Погорецький, 2013).

Важливим є також питання міжвідомчої взаємодії. У співавторстві з О. Стареньким М.А. Погорецький розглядає тактичну взаємодію підрозділів у процесі проведення НСРД, наголошуючи, що чіткий розподіл ролей та завдань між оперативними та слідчими підрозділами є ключовою умовою ефективного отримання цифрових доказів і запобігання їх спотворенню (Погорецький, Старенький, 2018).

Прокурорський нагляд і процесуальне керівництво займають ключове місце у забезпеченні законності та доброчесності здобуття цифрових доказів у провадженнях щодо кримінальних правопорушень проти основ національної безпеки України. Особливості цифрової інформації – її мінливість, вразливість до модифікації та залежність від технічних процедур – потребують посиленого контролю за дотриманням вимог закону під час проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій (Погорецький, Іскендеров, 2021). У провадженнях, що пов'язані з державними інтересами у сфері безпеки, прокурор виконує не лише функцію процесуального керівника, а й гаранта прав особи, щодо якої здійснюється втручання у приватне життя шляхом збору цифрової інформації.

Результати НСРД становлять основний масив цифрових доказів у справах про кримінальні правопорушення проти основ національної безпеки, а тому прокурор повинен забезпечити, щоб кожне втручання відповідало критеріям законності, необхідності та пропорційності. Саме прокурор перевіряє обґрунтованість клопотань про дозвіл на НСРД, їх фактичні підстави, співмірність очікуваного обсягу цифрових даних та неможливість здобуття інформації менш інвазивними засобами, що узгоджується зі стандартами ЄСПЛ (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021).

Прокурор також здійснює контроль за тим, щоб оперативні та слідчі підрозділи діяли в межах дозволеної мети, не виходили за рамки санкціонованого обсягу перехоплення інформації та дотримувалися режиму секретності, що особливо критично у справах, пов'язаних із державними секретами (Погорецький, 2009а). Таким чином прокурор виконує функцію первинного гаранта від неправомірного або надмірного втручання у цифрове середовище особи.

У межах оперативно-розшукової діяльності прокурорський нагляд спрямований на забезпечення належного юридичного оформлення результатів ОРД та їх подальшої трансформації у процесуальні документи. У науковій літературі підкреслено, що будь-які результати оперативно-розшукової діяльності не можуть автоматично набувати статусу доказів, і саме прокурор має контролювати їх легалізацію, відповідність встановленим процесуальним формам і вимогам допустимості (Погорецький, Сухачова, 2010).

Процесуальний контроль прокурора включає перевірку протоколів, носіїв інформації, цифрових файлів, наявність технічної фіксації, участі спеціаліста, даних щодо місця, часу, технічних параметрів збирання, а також відповідність процедури вимогам автентичності та цілісності цифрових даних (Закон України, 2003; НСТУ, 2017). Прокурор таким чином виступає «процесуальним фільтром», який запобігає використанню матеріалів, здобутих з порушенням закону, що особливо важливо у справах національної безпеки, де ризики зловживань є вищими, ніж у звичайних категоріях проваджень.

У межах оперативно-розшукової діяльності прокурорський нагляд спрямований на забезпечення належного юридичного оформлення результатів ОРД та їх подальшої трансформації у процесуальні документи. У науковій літературі підкреслено, що будь-які результати оперативно-розшукової діяльності не можуть автоматично набувати статусу доказів, і саме прокурор має контролювати їх легалізацію, відповідність встановленим процесуальним формам і вимогам допустимості (Погорецький, Сухачова, 2010).

Процесуальний контроль прокурора включає перевірку протоколів, носіїв інформації, цифрових файлів, наявність технічної фіксації, участі спеціаліста, даних щодо місця, часу, технічних параметрів збирання, а також відповідність процедури вимогам автентичності та цілісності цифрових даних (Закон України, 2003; НСТУ, 2017). Прокурор таким чином виступає «процесуальним фільтром», який запобігає використанню матеріалів, здобутих з порушенням закону, що особливо важливо у справах національної безпеки, де ризики зловживань є вищими, ніж у звичайних категоріях проваджень.

Захисник у кримінальному провадженні щодо кримінальних правопорушень проти основ національної безпеки України є самостійним та активним суб'єктом доказування, наділеним комплексом процесуальних прав, спрямованих на забезпечення законності отримання цифрових доказів, їх подальшої оцінки та запобігання порушенням прав людини. В умовах, коли значна частина цифрової інформації у таких провадженнях здобувається шляхом НСРД або оперативно-розшукових заходів, саме діяльність захисника виступає ключовим елементом процесуального балансу – «контрвагою» державним інструментам прихованого втручання у приватне життя (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021).

У провадженнях цієї категорії захисник відіграє критичну роль у перевірці дотримання стандартів прав людини під час втручання у сферу приватної комунікації особи. Після розкриття результатів НСРД захисник аналізує законність підстав проведення таких заходів, пропорційність втручання, відповідність ухвали слідчого судді фактичним обставинам справи, а також обсяг отриманої цифрової інформації, зокрема її релевантність і межі вторгнення (Погорецький, 2013).

Важливим завданням захисника є виявлення ознак необґрунтованого розширення предмета НСРД, отримання надмірного обсягу цифрових даних, відсутності технічної фіксації або порушень під час оброблення цифрових матеріалів. У такий спосіб він забезпечує виконання вимог законності, передбачених КПК України, та стандартів належного процесу, сформованих у практиці ЄСПЛ.

Захисник має право ставити під сумнів як законність отримання результатів НСРД та ОРД, так і допустимість цифрових доказів, які випливають із таких заходів. Це право є складовою гарантії «справедливого суду» у розумінні ст. 6 Конвенції про захист прав людини і основоположних свобод, що було докладно проаналізовано в роботах М. Погорецького та І. Гриценко (Погорецький, Гриценко, 2012).

Захисник може ініціювати визнання цифрових доказів недопустимими у випадках, коли: НСРД були санкціоновані без достатніх підстав; втручання було непропорційним; процедура отримання цифрової інформації не відповідала вимогам автентичності, цілісності або простежуваності (НСТУ, 2017); оперативні матеріали були використані як докази без належної легалізації (Шумило, Погорецький, 2001).

Таким чином, право на оскарження є ключовим інструментом захисника для забезпечення доброчесності цифрових доказів.

Окрім процесуального оскарження, захисник має суттєві тактичні можливості, спрямовані на перевірку достовірності та цілісності цифрових доказів. Він може ініціювати проведення експертних досліджень, технічних відтворень, аналізу цифрових відбитків, метаданих та хеш-сум для встановлення факту зміни або втручання в електронні файли.

У наукових роботах підкреслено, що участь захисника у технічній верифікації цифрових матеріалів є необхідною частиною реалізації права на захист, з огляду на високий ризик фальсифікації цифрових даних або технічних помилок під час їх вилучення та копіювання (Погорецький, 2009а, Погорецький, 2011; Погорецький, Старенький, 2018). Захисник

може також вимагати повторної технічної фіксації інформації, проведення альтернативної експертизи або витребування цифрових логів від провайдерів сервісів.

Тактичні прийоми захисника особливо важливі у справах, де цифрові дані пов'язані з державною таємницею. У таких випадках захисник діє у межах спеціального процедурного режиму, що передбачає обмежений доступ, проте дозволяє ставити питання про законність та пропорційність втручання, навіть якщо вся інформація не розкривається повністю.

Отже, діяльність захисника забезпечує баланс між інтересами держави у сфері національної безпеки та правами особи, сприяє збереженню цілісності цифрових доказів і гарантує, що такі докази використовуються у кримінальному процесі лише за умови дотримання вимог законності, справедливості та належної процесуальної форми.

Суд у кримінальному провадженні щодо кримінальних правопорушень проти основ національної безпеки виконує ключову функцію гаранта законності, пропорційності та процесуальної справедливості у процесі отримання й подальшої оцінки цифрових доказів. В умовах, коли основна частина цифрової інформації здобувається шляхом негласних слідчих (розшукових) дій або оперативно-розшукових заходів, суд забезпечує баланс між інтересами держави у сфері національної безпеки та правами особи на повагу до приватного життя, ефективний захист і справедливий судовий розгляд. Саме судова влада виступає інституційним фільтром, який перешкоджає надмірному або необґрунтованому втручанню органів держави у цифрову сферу приватності (ECtHR Zakharov, 2015; ECtHR Big Brother Watch, 2021).

Кримінальний процесуальний кодекс України передбачає, що проведення НСРД можливе виключно на підставі ухвали слідчого судді, яка є конститутивною умовою будь-якого втручання у сферу приватного життя особи. Суд зобов'язаний оцінити обґрунтованість клопотання слідчого або прокурора, перевірити необхідність такого заходу, співмірність очікуваного втручання та неможливість отримати цифрову інформацію іншим, менш інвазивним способом. Ця функція узгоджується з вимогами «якості закону», сформульованими ЄСПЛ, які передбачають передбачуваність, доступність та чіткість процедур, а також наявність ефективного попереднього контролю (ECtHR Big Brother Watch, 2021).

У наукових працях підкреслюється, що роль суду як «первинного контролера вторгнення» є особливо значущою у провадженнях щодо злочинів проти основ національної безпеки, де інформація містить ознаки державної таємниці, а цифрові докази здобуваються за максимально високого рівня секретності (Погорецький, 2009а).

Процедура оцінки цифрових доказів судом включає три базові критерії: автентичність, допустимість та достатність. Автентичність означає, що суд повинен встановити, чи є цифровий файл саме тим, за який він видається, і чи не зазнав він змін, видалення, модифікації або технічного втручання (НСТУ, 2017). Допустимість ґрунтується на відповідності способу отримання цифрових даних вимогам КПК України, а також на дотриманні судового контролю при проведенні НСРД (Закон України, 2003).

Судова практика демонструє, що оцінка технічних цифрових матеріалів має свою специфіку. Суд повинен враховувати особливості цифрового середовища, зокрема можливість автоматичного створення окремих елементів цифрового сліду, залежність метаданих від технічних параметрів обладнання, а також відмінність між системною інформацією і змістовими даними. Саме на це звертають увагу як доктринальні дослідження, так і практика ЄСПЛ (ECtHR Zakharov, 2015).

Особливого значення набуває постанова Об'єднаної палати ККС ВС від 29 березня 2021 року, де Суд чітко зазначив, що електронні документи можуть існувати у множинних автентичних копі-

ях, і кожна з них є оригіналом за умови забезпечення незмінності та цілісності (Об'єднана палата ККС ВС, 2021). Це рішення є фундаментом для оцінки цифрових доказів у національній судовій практиці.

Процедура оцінки цифрових доказів судом включає три базові критерії: автентичність, допустимість та достатність. Автентичність означає, що суд повинен встановити, чи є цифровий файл саме тим, за який він видається, і чи не зазнав він змін, видалення, модифікації або технічного втручання (НСТУ, 2017). Допустимість ґрунтується на відповідності способу отримання цифрових даних вимогам КПК України, а також на дотриманні судового контролю при проведенні НСРД (Закон України, 2003).

Судова практика демонструє, що оцінка технічних цифрових матеріалів має свою специфіку. Суд повинен враховувати особливості цифрового середовища, зокрема можливість автоматичного створення окремих елементів цифрового сліду, залежність метаданих від технічних параметрів обладнання, а також відмінність між системною інформацією і змістовими даними. Саме на це звертають увагу як доктринальні дослідження, так і практика ЄСПЛ (ECtHR Zakharov, 2015).

Висновки і перспективи подальших досліджень.

На підставі проведеного дослідження можна стверджувати, що цифрові докази набули статусу центрального елементу доказової системи у кримінальних провадженнях щодо кримінальних правопорушень проти основ національної безпеки України. Їхня природа, способи формування, процесуальний режим та особливості судового використання сутнісно відрізняються від традиційних матеріальних носіїв інформації, що зумовлює необхідність переосмислення теоретичних і практичних засад кримінального процесуального доказування. Цифрові дані характеризуються мінливістю, залежністю від технічного середовища, вразливістю до модифікації та можливістю існування у множинних автентичних копіях, що потребує застосування підвищених стандартів автентичності, цілісності, незмінності та простежуваності. Саме ці властивості значною мірою формують нову конфігурацію доказового процесу, в якій ключову роль відіграють стандарти законності, пропорційності та незалежного контролю, визначені як національним законодавством, так і практикою ЄСПЛ.

Особливу складність становлять цифрові докази, отримані у результаті оперативно-розшукової діяльності та негласних слідчих (розшукових) дій. Застосування цих заходів у провадженнях щодо кримінальних правопорушень проти основ національної безпеки здійснюється у контексті підвищеного режиму секретності, що охоплює не лише зміст отриманої інформації, а й технічні процедури її здобуття та збереження. Наявність державної таємниці, обмеженого доступу до цифрових носіїв, а також імовірність протидії з боку суб'єктів розвідувально-підривної діяльності ускладнюють процес доказування та потребують особливої уваги до механізмів документування, легалізації та судової оцінки таких даних. Як випливає з доктринальних положень, належне оформлення результатів НСРД, чітке розмежування оперативної інформації та процесуальних доказів, а також дотримання вимог до технічної фіксації є необхідною умовою їх подальшої допустимості й доказової спроможності.

Роль прокурора у цьому процесі набуває подвійного значення: як гаранта законності втручання у сферу цифрової комунікації, так і контролера за дотриманням вимог незмінності та цілісності цифрових слідів. Суд, у свою чергу, виступає первинним фільтром законності та кінцевим арбітром допустимості, забезпечуючи баланс між інтересами національної безпеки та правами особи на приватність і справедливий суд. Діяльність сторони захисту також є ключовою, оскільки захисник забезпечує

перевірку законності та пропорційності НСРД, ініціює технічні перевірки цифрових матеріалів, ставить під сумнів їх автентичність і, таким чином, забезпечує реалізацію принципу змагальності й гарантій справедливого судового розгляду.

Разом із тим проведений аналіз дозволяє дійти висновку, що попри наявність суттєвих напрацювань, у науці й практиці залишаються невирішеними низка проблемних питань. Зокрема, потребують подальшої деталізації правові критерії допустимості цифрових доказів у провадженнях із підвищеним режимом секретності, механізми доступу сторони захисту до таких матеріалів із дотриманням режиму державної таємниці, а також алгоритми судового контролю за технічними процесами отримання і збереження цифрової інформації. Невирішеною залишається й проблема забезпечення незалежності експертної верифікації цифрових даних, особливо коли вони пов'язані з діяльністю органів безпеки.

Перспективними напрямами подальших досліджень видається розроблення моделі спеціального процесуального режиму для цифрових доказів у справах про кримінальні правопорушення проти основ національної безпеки; формування єдиних стандартів цифрової криміналістики для роботи з метаданими, цифровими слідами й системними журналами; вироблення механізмів адаптації кібертрасології, OSINT-технологій та штучного інтелекту до вимог кримінального процесу; удосконалення гарантій прокурорського нагляду та судового контролю з урахуванням технічних особливостей цифрових даних; розроблення процедур, що забезпечують баланс між режимом секретності та принципом змагальності. Особливої уваги потребує створення національного стандарту доказової автентифікації цифрових файлів, здатного забезпечити однаковість підходів правоохоронних органів, прокурорів, експертів та судів.

Отже, цифрові докази у провадженнях щодо кримінальних правопорушень проти основ національної безпеки становлять складну міждисциплінарну категорію, яка потребує подальшого теоретичного осмислення, нормативного вдосконалення та технологічної підтримки. Подальший розвиток цього напряму має значення не лише для ефективності кримінального переслідування, а й для забезпечення належного рівня прав людини та верховенства права в умовах сучасних безпекових викликів.

Подяки

Немає

Конфлікт інтересів

Немає

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Аналіз стану здійснення правосуддя у кримінальних провадженнях та справах про адміністративні правопорушення у 2024 році. Сайт Верховного Суду. URL: https://court.gov.ua/storage/portal/supreme/Analyz_zdijsnenna_pravosydda_2024.pdf

European Court of Human Rights. Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, Judgment of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001–203614

European Court of Human Rights. Roman Zakharov v. Russia, no. 47143/06, Judgment of 4 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001–159324

Гарасимів О.І., Марко С.І., Ряшко О.В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету. Серія Право.* 2023. Вип. 75. Т. 2. С. 158–162.

Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні. *Криміналістичний вісник.* 2020. № 1 (33). С. 37–49.

Закон України «Про електронні документи та електронний документообіг». URL: https://zakon.rada.gov.ua/laws/show/851–15

Крицька І.О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права.* 2016. № 1. С. 301–305.

Метелев О.П. Гносеологічна і правова природа цифрових доказів у кримінальному процесі. *Правова позиція.* 2018. № 1 (20). С. 75–86.

Національний стандарт України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів». URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=74978

Погорецький М.А. Актуальні питання теорії доказів. *Докази і доказування за новим КПК України…* Харків: Строков Д.В., 2013. С. 15–22.

Погорецький М.А. Докази у кримінальному процесі. *Вісник прокуратури.* 2003. № 2. С. 59–65.

Погорецький М.А. Докази у кримінальному процесі: проблемні питання. *Часопис Національного університету «Острозька академія». Серія «Право».* 2011. № 1 (3). URL: https://lj.oa.edu.ua/articles/2011/n1/11pmappp.pdf

Погорецький М.А. Доказування у кримінальному процесі: поняття, зміст, структура. *Актуальні проблеми доказування у кримінальному провадженні…* 2013. С. 17–21.

Погорецький М.А. Негласні слідчі (розшукові) дії: проблеми провадження та використання результатів у доказуванні. *Юридичний часопис НАВС.* 2013. № 1. С. 270–277.

Погорецький М.А. Новели проекту нового КПК України і проблеми їх реалізації у правозастосовній діяльності. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 1 (27). С. 208–216. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_25

Погорецький М.А. Порядок проведення НСРД та використання їх результатів у доказуванні. У: *Актуальні питання досудового розслідування…* Київ, 2013. С. 186–193.

Погорецький М.А. Сучасні концепції кримінального процесуального доказування. *Сучасні тенденції розвитку криміналістики та кримінального процесу…* Харків, 2017. С. 309–312. URL: https://ir.library.knu.ua/handle/15071834/8507

Погорецький М.А. Теоретичні і практичні проблеми використання матеріалів оперативно-розшукової діяльності в кримінальному процесі (за матеріалами СБУ). Автореф. дис. … д-ра юрид. наук. Київ: КНУВС, 2006. 36 с.

Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства.* 2023. № 3–4. С. 84–102. DOI: https://doi.org/10.17721/2413–5372.2023.3–4/84–102

Погорецький М.А., Сергєєва Д.Б. Криміналістична тактика: щодо визначення поняття. *Часопис НаУ «Острозька академія».* 2012. № 1 (5). URL: https://lj.oa.edu.ua/articles/2012/n1/12pmasvp.pdf

Погорецький М.А., Сергєєва Д.Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. *Боротьба з організованою злочинністю і корупцією.* 2014. № 2 (33). С. 137–141. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_34

Погорецький М.А., Сергєєва Д.Б. Тактика захисника: поняття, зміст та місце в системі криміналістичної тактики. *Вісник кримінального судочинства.* 2016. № 2. С. 113–123. URL: https://vkslaw.knu.ua/images/verstka/2_2016_Sergeeva.pdf

Погорецький М.А. Допуск адвоката як захисника до участі у кримінальних справах, матеріали яких становлять державну таємницю. *Вісник Акад. правових наук.* 2009. № 3 (59). С. 209–220.

Погорецький М.А. Кримінально-процесуальні гарантії державної таємниці у кримінальних справах проти основ національної безпеки України. Національні інтереси та проблеми забезпечення безпеки України: зб. матеріалів Всеукр. наук. – практ. конф., 5–6 листоп. 2009 р. Кіровоград: КірЮІ ХНУВС, 2009. С. 23–25.

Погорецький М.А., Іскендеров Е.Ф. Роль прокурора при проведенні негласних слідчих (розшукових) дій. *Вісник кримінального судочинства.* 2021. № 3–4. С. 47–58.

DOI: https://doi.org/10.17721/2413–5372.2021.3–4/47–58 URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3–4_21_230726_avt%20(3).pdf

Погорецький М.А. Взаємозв'язок мети та завдань ОРД і кримінального процесу: теоретико-правові проблеми. *Кримський юрид. вісник.* Сімферополь, 2008. Вип. 3 (4). С. 5–12.

Погорецький М.А., Сухачова І.О. Прокурорський нагляд за законністю використання матеріалів оперативно-розшукової діяльності на досудових стадіях кримінального процесу. *Вісник національної академії прокуратури України*. 2010. № 4. С. 64–70 URL: http://nbuv.gov.ua/UJRN/Vnapu_2010_4_14

Погорецький М.А., Гриценко І.С. Право на справедливий суд. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки.* 2012. № 91. С. 4–7. URL: http://nbuv.gov.ua/UJRN/VKNU_Yur_2012_91_3

Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчення злочину. *Інформаційна безпека людини, суспільства, держави:* наук. – практ. журнал. Київ: НАСБУ, 2009. № 2 (2). С. 77–81. URL: https://ir.library.knu.ua/handle/15071834/8415

Погорецький М.А. Проблеми використання матеріалів оперативно-розшукової діяльності для забезпечення безпеки учасників кримінального судочинства. *Вісник прокуратури.* 2007. № 2. С. 86–93.

Погорецький М.А., Старенький О.С. Негласні слідчі (розшукові) дії як засоби отримання доказів. *Право України.* 2018. № 8. С. 85–106. URL: http://nbuv.gov.ua/UJRN/prukr_2018_8_9

Посібник для підвищення кваліфікації працівників органів та підрозділів Національної поліції України / О.І. Безпалова та ін. Харків: ХНУВС, 2019. 132 с.

Постанова колегії суддів Третьої судової палати ККС ВС від 12.06.2024, справа № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340

Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29 березня 2021 року у справі № 554/5090/16-к. URL: https://reyestr.court.gov.ua/Review/

Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Єдиний звіт за 2024 рік. Сайт ОГП. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

Стан здійснення правосуддя у кримінальних провадженнях та справах про адміністративні правопорушення судами загальної юрисдикції у 2024 році. Сайт Верховного Суду. URL: https://court.gov.ua/storage/portal/supreme/Stan%20zdiisnenna%20pravosydda%20y%20kruminalnyh_provadgennah_admin_pravoporyshen_2024.pdf

Шумило М.Є., Погорецький М.А. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах. *Вісник Луганського інституту внутрішніх справ.* 2001. Вип. 3. С. 199–209.

Шумило М.Є., Погорецький М.А. Докази і доказування. У: *КПК України. Науково-практичний коментар.* Т. 1. Харків: Право, 2012. С. 247–308.

REFERENCES

Analysis of the State of Administration of Justice in Criminal Proceedings and Cases on Administrative Offenses in 2024. (2024). Supreme Court of Ukraine. URL: https://court.gov.ua/storage/portal/supreme/Analyz_zdijsnenna_pravosydda_2024.pdf

Berkeley Protocol on Digital Open Source Investigations. (2022). Practical Guide for Effective Use of Open-Source Digital Information in Investigating Violations of International Criminal, Humanitarian, and Human Rights Law. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

Bezpalova, O. I., Buhaichuk, K. L., Voitsikhovskyi, A. V., et al. (2019). *Professional Development Manual for Officers of the National Police of Ukraine*. Kharkiv: Kharkiv National University of Internal Affairs.

Big Brother Watch and Others v. the United Kingdom. (2021). European Court of Human Rights, Applications nos. 58170/13, 62322/14, 24960/15. URL: https://hudoc.echr.coe.int/eng?i=001–203614

Criminal Offenses Registered and Results of Their Pre-trial Investigation: Annual Report January–December 2024. (2024). Office of the Prosecutor General of Ukraine. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

Harasymiv, O. I., Marko, S. I., Riashko, O. V. (2023). Digital Evidence: Selected Problematic Issues of Its Concept and Use in Criminal Proceedings. *Scientific Bulletin of Uzhhorod National University. Law Series*, 75(2), 158–162.

Hutsaliuk, M. V., Antoniuk, P. Ye. (2020). On the Essence of Electronic (Digital) Information as a Source of Evidence in Criminal Proceedings. *Criminalistic Bulletin*, 1(33), 37–49.

Krytska, I. O. (2016). Physical Evidence and Digital Information: Concept and Correlation. *Journal of Kyiv University of Law*, 1, 301–305.

Law of Ukraine «On Electronic Documents and Electronic Document Workflow.» (2003). URL: https://zakon.rada.gov.ua/laws/show/851–15

Meteliev, O. P. (2018). Gnoseological and Legal Nature of Digital Evidence in Criminal Proceedings. *Legal Position*, 1(20), 75–86.

National Standard of Ukraine «Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.» (2017). URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=74978

Pohoretskyi, M. A. (2003). Evidence in Criminal Proceedings. *Bulletin of the Prosecutor's Office*, 2, 59–65.

Pohoretskyi, M. A. (2007). Problems of Using Operational Search Materials to Ensure the Safety of Participants in Criminal Proceedings. *Prosecutor's Office Bulletin*, 2, 86–93.

Pohoretskyi, M. A. (2008). Relationship Between the Purpose and Tasks of Operational-Search Activity and Criminal Procedure: Theoretical and Legal Problems. *Crimean Legal Bulletin*, 3(4), 5–12.

Pohoretskyi, M. A. (2009). Admission of a Defence Lawyer to Criminal Cases Involving State Secrets. *Bulletin of the Academy of Legal Sciences*, 3(59), 209–220.

Pohoretskyi, M. A. (2009). Criminal Procedure Guarantees of State Secrets in Criminal Cases Against the Fundamentals of National Security of Ukraine. In: *National Interests and Problems of Ensuring the Security of Ukraine* (pp. 23–25). Kirovohrad: Kirovohrad Institute of the Ministry of Internal Affairs.

Pohoretskyi, M. A., Hrytsenko, I. S. (2012). The Right to a Fair Trial. *Bulletin of Taras Shevchenko National University of Kyiv. Legal Studies*, 91, 4–7. URL: http://nbuv.gov.ua/UJRN/VKNU_Yur_2012_91_3

Pohoretskyi, M. A., Iskenderov, E. F. (2021). The Role of the Prosecutor in Conducting Covert Investigative (Search) Actions. *Bulletin of Criminal Justice*, 3–4, 47–58. DOI: https://doi.org/10.17721/2413–5372.2021.3–4/47–58 URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3–4_21_230726_avt%20(3).pdf

Pohoretskyi, M. A., Shelomentsev, V. P. (2009). The Concept of Cyberspace as an Environment for Committing Crimes. *Information Security of the Individual, Society and the State*, 2(2), 77–81. URL: https://ir.library.knu.ua/handle/15071834/8415

Pohoretskyi, M. A., Sukhachova, I. O. (2010). Prosecutorial Supervision over the Lawfulness of Using Materials of Operational-Search Activity at Pre-Trial Stages of Criminal Proceedings. *Bulletin of the National Academy of the Prosecutor's Office of Ukraine*, 4, 64–70. URL: http://nbuv.gov.ua/UJRN/Vnapu_2010_4_14

Pohoretskyi, M. A. (2006). *Theoretical and Practical Problems of Using Materials of Operational and Investigative Activities in Criminal Proceedings (Based on Materials of the Security Service of Ukraine).* Doctoral thesis abstract. Kyiv: KNUVS.

Pohoretskyi, M. A. (2011). Evidence in Criminal Proceedings: Problematic Issues. *Ostroh Academy Law Journal*, 1(3). URL: https://lj.oa.edu.ua/articles/2011/n1/11pmappp.pdf

Pohoretskyi, M. A. (2012). Novelties of the Draft CPC of Ukraine and Issues of Their Implementation. *Struggle Against Organized Crime and Corruption*, 1(27), 208–216. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_25

Pohoretskyi, M. A. (2013). Covert Investigative (Search) Actions: Procedure and Use in Evidence. In: *Contemporary Issues of Pre-trial Investigation* (pp. 186–193). Kyiv: Khli-Tek Press.

Pohoretskyi, M. A. (2013). Evidence and Proof in Criminal Proceedings: Concept, Content, Structure. In: *Topical Problems of Evidence in Criminal Proceedings* (pp. 17–21). Odesa: Legal Literature.

Pohoretskyi, M. A. (2017). Contemporary Concepts of Criminal Procedural Evidence. In: *Modern Trends in the Development of Criminalistics and Criminal Procedure* (pp. 309–312). Kharkiv: KhNUVS. URL: https://ir.library.knu.ua/handle/15071834/8507

Pohoretskyi, M. A. (2023). Application of Advanced Technologies in the Investigation and Proof of War Crimes: Problematic Issues. *Bulletin of Criminal Justice*, 3–4, 84–102. DOI: https://doi.org/10.17721/2413–5372.2023.3–4/84–102

Pohoretskyi, M. A., Sergeieva, D. B. (2012). Criminalistic Tactics: On the Definition of the Concept. *Ostroh Academy Law Journal*, 1(5). URL: https://lj.oa.edu.ua/articles/2012/n1/12pmasvp.pdf

Pohoretskyi, M. A., Sergeieva, D. B. (2014). Covert Investigative (Search) Actions and Operational Measures: Concept, Essence and Correlation. *Struggle Against Organized Crime and Corruption*, 2(33), 137–141. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_34

Pohoretskyi, M. A., Sergeieva, D. B. (2016). Defence Counsel's Tactics: Concept, Content and Place in the System of Criminalistic Tactics. *Bulletin of Criminal Justice*, 2, 113–123. URL: https://vkslaw.knu.ua/images/verstka/2_2016_Sergeeva.pdf

Pohoretskyi, M. A., Starenkyi, O. S. (2018). Covert Investigative (Search) Actions as Means of Obtaining Evidence: Selected Problematic Issues. *Law of Ukraine*, 8, 85–106. URL: http://nbuv.gov.ua/UJRN/prukr_2018_8_9

Roman Zakharov v. Russia. (2015). European Court of Human Rights, no. 47143/06. URL: https://hudoc.echr.coe.int/eng?i=001–159324

Shumylo, M. Ye., Pohoretskyi, M. A. (2001). Problems of Using Operational and Investigative Materials as Evidence in Criminal Cases. *Bulletin of the Luhansk Institute of Internal Affairs*, 3, 199–209.

Shumylo, M. Ye., Pohoretskyi, M. A. (2012). Evidence and Proof. In: *Criminal Procedure Code of Ukraine: Scientific and Practical Commentary*. Vol. 1, pp. 247–308. Kharkiv: Pravo.

Standard of Administration of Justice in Criminal and Administrative Cases by Courts of General Jurisdiction in 2024. (2024). Supreme Court of Ukraine. URL: https://court.gov.ua/storage/portal/supreme/Stan%20zdiisnenna%20pravosydda%20y%20kruminalnyh_provadgennah_admin_pravoporyshen_2024.pdf

Unified Report on Criminal Offenses for January–December 2024. (2024). Office of the Prosecutor General of Ukraine. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

Unified Chamber of the Criminal Cassation Court of the Supreme Court. (2021). Judgment of 29 March 2021 in Case No. 554/5090/16-k. URL: https://reyestr.court.gov.ua/Review/96074938

Supreme Court of Ukraine, Third Judicial Chamber of the Criminal Cassation Court. (2024). Judgment of 12 June 2024 in Case No. 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340

UDC 343.1:343.98:004.056(477)

Syza Nataliia Petrivna – PhD in Law, Associate Professor,
Chief Research Fellow,
Scientific and Organizational Center,
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0001-5850-4023
syzyy@ukr.net

Use of Digital Evidence in Criminal Proceedings Regarding Criminal Offenses Against the Fundamentals of National Security of Ukraine

The article provides a comprehensive study of the theoretical, regulatory, and practical aspects of the use of digital evidence in criminal proceedings concerning criminal offenses against the fundamentals of Ukraine's national security. In the context of escalating hybrid threats, intensified intelligence and subversive activities, and the growing use of secure digital platforms, digital evidence has become the dominant source of factual information. The study examines the nature of digital data, its differences from traditional physical and documentary evidence, as well as specific characteristics related to its immateriality, volatility, and dependence on technical environments.

Doctrinal approaches to the understanding of electronic evidence are analyzed, including the views of Ukrainian scholars concerning the criteria of authenticity, integrity, immutability, and traceability of digital data. The role of operational-search activity and covert investigative (search) actions in generating digital evidence is explored, taking into account the specificities of their use in proceedings involving elevated secrecy and risks of counteraction by subjects engaged in criminal or hostile activity. Considerable attention is devoted to judicial and prosecutorial mechanisms of controlling the legality of interference with an individual's private sphere, assessing the compliance of procedural practices with the standards of the European Court of Human Rights, as well as the role of the defence in ensuring the reliability of evidence and in verifying the admissibility of covertly obtained materials.

Based on the findings, the article outlines the need to improve national legislation, standardize technical procedures for handling digital evidence, and develop a specialized evidentiary model for cases related to national security. It identifies promising directions for further research, including enhancing the reliability of digital forensics, ensuring a balance between secrecy and the right to defence, and integrating international standards into national legal practice.

Keywords: *digital evidence; electronic evidence; covert investigative (search) actions; operational-search activity; national security; state secrecy; authenticity; admissibility; judicial control; prosecutorial oversight; defence counsel; criminal evidence.*