DOI: 10.33270/05257004.3
УДК 343.14:343.985

ВАСИЛИНЧУК Віктор*
доктор юридичних наук, професор, професор кафедри оперативно-розшукової діяльності та національної безпеки Національної академії внутрішніх справ
м. Київ, Україна
ORCID: https://orcid.org/0000-0001-5415-8450;
ПОПТАНИЧ Юрій
аспірант Національної академії внутрішніх справ
м. Київ, Україна
ORCID: https://orcid.org/0009-0000-1680-5987

Використання цифрових доказів, отриманих під час оперативно-розшукової діяльності

Анотація. У статті розглянуто проблематику використання цифрових доказів у кримінальному процесі й оперативно-розшуковій діяльності. Визначено актуальність цифровізації для розвитку держави, а також її вплив на сферу протидії злочинності. Зосереджено увагу на автентичності, ланцюзі збереження та допустимості цифрових доказів у судовій практиці. Проаналізовано національні й міжнародні підходи, а також запропоновано рекомендації з удосконалення законодавства та практичного використання цифрових доказів в Україні. Дослідження присвячено вдосконаленню законодавства та формуванню рекомендацій для практичних підрозділів щодо виявлення та використання цифрових доказів, отриманих під час оперативно-розшукової діяльності. Визначено коло джерел отримання цифрових доказів від відкритих джерел (OSINT, протокол Берклі) до спеціальних технічних заходів під час проведення негласних слідчих (розшукових) дій та оперативно-розшукових заходів. Виокремлено основні проблеми під час виявлення, фіксації та використання цифрових доказів, отриманих у процесі оперативно-розшукової діяльності. Запропоновано низку змін до чинного законодавства, що можуть сприяти покращенню результатів використання відповідних матеріалів у кримінальному судочинстві. Акцентовано, що ефективне використання цифрових доказів у діяльності оперативних підрозділів підвищує результативність документування злочинів, сприяє зміцненню доказової бази в кримінальному судочинстві та розвитку принципу невідворотності покарання. Зазначено, що цифрові докази стають невіддільною складовою сучасного кримінального процесу й оперативно-розшукової діяльності. Упровадження міжнародних стандартів, нормативне закріплення процедури збирання, перевірки й оцінки цифрових доказів забезпечить підвищення ефективності розслідувань, прозорість судового розгляду та довіру суспільства до системи правосуддя.

Ключові слова: докази; кримінальне провадження; оперативно-розшукова діяльність; правове регулювання; удосконалення; цифровізація.

Історія статті:
Отримано: 26.08.2025
Переглянуто: 22.09.2025
Прийнято: 24.10.2025

Рекомендоване посилання:
Василинчук В., Поптанич Ю. Використання цифрових доказів, отриманих під час оперативно-розшукової діяльності. *Наука і правоохорона.* 2025. Вип. 4 (70). С. 24–37. DOI: 10.33270/05257004.3

*Відповідальний автор

Вступ

Цифровізація в Україні надзвичайно важлива для створення ефективної держави, розвитку економіки, підвищення конкурентоспроможності та покращення якості життя громадян. Вона сприяє спрощенню та доступності державних послуг, зменшенню бюрократії, створенню нових робочих місць, підвищенню продуктивності праці та відкриває широкі можливості для інновацій у різних сферах, включно з освітою, охороною здоров'я та промисловістю. В умовах війни цифровізація також є критично важливою для забезпечення стійкості держави та ефективного реагування на виклики.

3 березня 2021 року Кабінет Міністрів України своїм розпорядженням схвалив Концепцію розвитку цифрових компетентностей і затвердив план заходів щодо її реалізації.

Стратегічна ціль Мінцифри – навчити 6 млн українців цифрової грамотності, що дасть змогу громадянам підвищити конкурентоспроможність на ринку праці, надасть можливості для безперервного навчання, подарує комфорт проживання в цифровій країні, підвищить рівень доступності до державних послуг, зменшить ризики небезпек під час користування інтернетом.

Крім того, серед завдань цифровізації в Україні є: переведення 100 % усіх публічних послуг для громадян та бізнесу онлайн, забезпечити 95 % транспортної інфраструктури, населених пунктів та їхні соціальні об'єкти доступом до високошвидкісного інтернету; підвищити частку IT у ВВП країни до 10 % та ін.

З огляду на зазначені стійкі та позитивні тенденції цифровізації держави динамічно та пропорційно зростає і використання цифрових інструментів у протиправній діяльності, які залишають в основному цифрові сліди.

Як приклад, за результатами аналізу вироків за ст. 436-2 КК України, у 83,1% справ «саме інтернет-простір став місцем вчинення кримінального правопорушення», оскільки глорифікатори збройної агресії рф проти України для вчинення кримінального правопорушення використовували найбільш популярні соціальні мережі (найчастіше в 61,7% «Одноклассники»).

Ключова роль у запобіганні аналізованим кримінальним правопорушенням у разі їх вчинення з використанням інструментів інтернет-простору має відводитися сфері високих технологій із забезпеченням відповідного нормативно-правового супроводу їх використання (Batyrhareieva, & Netesa, 2024).

Технологічний прогрес не стоїть на місці, навіть більше: він безперервно охоплює всі сфери нашого життя (включно з кримінальним судочинством), тому таким вкрай актуальним і необхідним є використання електронних доказів у встановленні істини та притягненні винних до кримінальної відповідальності (Harasymov, Marko, & Riashko, 2023).

Актуальність цифрових доказів у сучасному кримінальному процесі та оперативно-розшуковій діяльності зумовлена широким використанням цифрових технологій у суспільстві. Електронна інформація стає не лише додатковим, а й ключовим джерелом даних для розкриття злочинів. Збирання, збереження та допустимість цифрових доказів у суді набувають особливого значення, оскільки саме цифрові сліди часто є основним підтвердженням протиправної діяльності.

Запобігання та вчасне виявлення кримінальних правопорушень є життєво важливими, оскільки вони дають змогу запобігти матеріальним та моральним збиткам, зберегти життя, зменшити витрати на діяльність правоохоронної системи й сприяти позитивній суспільній атмосфері, реалізовуючи прогресивний принцип «краще попереджати, ніж карати».

Профілактика злочинності як діяльність держави та громадськості спрямована на усунення причин і умов, що породжують злочини, а також на формування законослухняної поведінки громадян.

За такої концепції ефективної протидії злочинності надзвичайної актуальності набуває пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, а також отримання інформації в інтересах безпеки громадян, суспільства і держави, що є основним завданням оперативно-розшукової діяльності.

Тому надзвичайно актуальним є дослідження виявлення цифрових слідів і цифрових доказів під час проведення оперативно-розшукової діяльності з метою документування протиправних діянь окремих осіб та груп.

Аналіз і дослідження проблематики, пов'язаної з виявленням і використанням цифрових доказів у правозастосовчій діяльності, привертали увагу низки вчених в Україні та за кордоном.

На міжнародному рівні важливим джерелом є Practical Guide for Requesting Electronic Evidence Across Borders, де детально описано процедури транскордонного отримання електронних доказів. Цей посібник є корисним інструментом для правоохоронців, оскільки містить рекомендації щодо ланцюга збереження даних і співпраці з іноземними органами.

У практичній площині важливу роль відіграють неурядові організації, такі як Bellingcat та Mnemonic. Bellingcat продемонстрував ефективність OSINT-методів у справі MH17, де цифрові докази з відкритих джерел стали ключовими в міжнародному розслідуванні. Організація Mnemonic забезпечує архівування цифрових свідчень воєнних злочинів, що дає змогу зберегти дані для подальших судових процесів.

Серед український вчених О. Метелев (2023) запропонував розгорнуту класифікацію цифрових доказів, що дає змогу відокремити їх від інших видів інформації. М. Гуцалюк (2020) наголошує

на складності уніфікації поняття «цифровий доказ» у законодавстві, оскільки воно охоплює широкий спектр інформаційних об'єктів. Дослідження М. Шумило (2019) акцентує на застосуванні цифрових доказів у кримінальному провадженні, де важливим є належне їхнє документування. О. Гарасимов (2023) зосереджується на проблемі автентичності та допустимості таких доказів у суді. О. Користін (2024) формує методологічні засади OSINT у системі кримінального аналізу Національної поліції України.

Основну увагу вчені присвятили дослідженню цифрових доказів суто в межах кримінального процесу без врахування особливостей, що виникають під час проведення оперативно-розшукової діяльності відповідними оперативними підрозділами.

Отже, метою статті є вдосконалення кримінального процесуального законодавства України та Закону України «Про оперативно-розшукову діяльність», формування рекомендацій для практичних підрозділів щодо виявлення та використання цифрових доказів, отриманих під час оперативно-розшукової діяльності.

Досягнути цього можливо шляхом виокремлення та аналізу особливостей проблем сучасного правового регулювання, а також розроблення пропозицій вдосконалення з урахуванням досягнення національної та іноземної юридичної науки й реалій сучасної практики в Україні.

Матеріали та методи

Під час дослідження опрацьовано емпіричні, загальнологічні, евристичні й спеціально-юридичні методи. З емпіричних методів правових досліджень для аналізу цифрових доказів, отриманих під час оперативно-розшукової діяльності, використано метод спостереження, що дав змогу комплексно сприйняти системну діяльність уповноважених суб'єктів, регламентовану КПК України та Законом України «Про оперативно-розшукову діяльність». За допомогою порівняльно-правового методу виявили законодавчі недоліки правового регулювання, визначили можливість рецепіюання іноземного досвіду в українське законодавство та правозастосування. Серед загальнологічних методів у дослідженні найширше представлений метод аналізу, який дав змогу виокремити шляхи подальшого використання цифрових доказів, отриманих під час оперативно-розшукової діяльності. Застосовано ряд аналогій для ототожнення процесів отримання і використання цифрових доказів у межах кримінального процесу та оперативно-розшукової діяльності. Евристичний метод колективного стимулювання використано для визначення експертних оцінок українських та іноземних вчених, які стали у пригоді під час формування доктринального підґрунтя вдосконалення українського законодавства та реалізації принципу пропорційності. Формально-юридичний метод дав змогу визначити особливості законодавчого формування ст. 84 КПК України, допущені в ній недоліки реалізації принципу пропорційності як цілісної юридичної конструкції. Формально-логічний метод застосовано для визначення понять «цифрові докази» та інших пов'язаних термінів, а також для структурування аргументації та формування висновків. Метод системного підходу – для розгляду проблеми цифрових доказів у кримінальному процесі та оперативно-розшуковій діяльності як єдиної системи.

Результати й обговорення

Докази в кримінальному процесі є надзвичайно важливими, оскільки на їх основі встановлюють наявність чи відсутність злочину, винуватість особи та інші важливі обставини справи, а також формується внутрішнє переконання суду для ухвалення законного та обґрунтованого рішення. Без належних та допустимих доказів неможливо довести вину, забезпечити права учасників процесу та досягти справедливості.

Систему процесуальних доказів протягом кількох століть удосконалювали з кримінально-процесуальним законодавством. Вона доволі консервативна і змінювалася лише під впливом неминучості змін, які були спричинені соціальним і технічним прогресом під час розвитку суспільства.

XXI століття характеризується швидким розвитком цифровізації – впровадженням та використанням цифрових технологій в усіх сферах життя, включно з бізнесом, державним управлінням, освітою та побутом, що створює цифрову економіку та цифрове суспільство. Цей процес спрямований на покращення доступу до інформації та послуг, оптимізацію бізнес-процесів та досягнення суспільних цілей за допомогою інформаційно-комунікаційних технологій.

Інформаційні технології стрімко розвиваються, а разом з ними й методи злочинного використання цифрових технічних засобів, постійно зростає кількість злочинів, скоєних у кіберпросторі.

Чинне процесуальне законодавство пропонує не так класифікацію електронних доказів, як орієнтовний перелік цифрової інформації, на яку повинні звернути увагу суд та учасники справи і яку можна використати як доказ, зокрема в цивільному процесі (Pavlova, 2023).

Українські науковці А. В. Гутник, А. Я. Хитра (2022) також використовують термін «електронні докази» для позначення відповідного різновиду цифрових доказів у контексті чинного КПК України.

Небезпідставно дотримуються й наукової позиції Т. Г. Фоміна, О. О. Рачинський (2023) щодо доцільності застосування саме терміну «електрон-

ний (цифровий) доказ». Обґрунтовують це тим, що «електронний» вказує на вид пристрою, за допомогою якого створили й зберегли доказ, а «цифровий» – на тип запису інформації на відповідний пристрій. Проте треба зважати на швидкоплинність технологічного прогресу, адже вже через певний проміжок часу можуть з'явитися як нові види пристроїв, так і нові типи запису інформації.

Цифрові докази (цифрова інформація) – інформація, створена за допомогою високих інформаційних технологій. У наукових джерелах закордонних країн широкого застосування набув термін digital evidence (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передають з використанням комп'ютерної чи іншої техніки.

На думку А. В. Ратнова (2021), цифрова інформація існує в «електронно-цифровому» середовищі та не завжди набуде характеру, статусу і характеристик доказу в кримінальному провадженні. Вона характеризується наявністю метаданих (з англ. «дані про дані»), які створює разом із кожним файлом автоматично програма або автор цифрової інформації.

А. В. Скрипник (2022) вважає, що ознака позбавлення суб'єктивності не є абсолютно притаманною цифровим доказам, адже авторство належить людині. Іншими ознаками є такі: можливість існування в статичній та динамічній формах, закодованість (через що є потреба у перетворенні в таку форму, яка може бути сприйнята людиною; мобільність; тиражованість; «невловний характер інформації» і легкість внесення змін або знищення. Для відтворення цифрової інформації потрібні апаратні й програмні умови.

Цифрові докази – це «фактичні дані, які подано в цифровій формі та зафіксовано на будь-якому типі носія» або «інформація в електронній (цифровій) формі, що має значення для досудового та судового розгляду й надається стороною провадження (справи) для її оцінки слідчим, прокурором або судом».

Слушно зазначає В. Ю. Шепітько (2023), що разом із терміном «цифрові докази» використовують й інші, наприклад: «електронні докази», «електронні сліди», «цифрові джерела інформації», «електронні документи» тощо. Цифрові докази потребують новітніх підходів для їх збирання, зберігання, використання та дослідження під час доказування в кримінальному провадженні. Фактично можна констатувати появу окремого криміналістичного напрямку – «цифрової криміналістики» (Shepitko, V., & Shepitko, M., 2021).

Цифрова криміналістика – це окрема криміналістична теорія і вид судової експертизи, що ставить своїм завданням дослідження цифрових доказів з використанням криміналістичної техніки та наявних методик для досудового розслідування та судового розгляду.

Цілком логічною видається позиція О. Козицької (2020) про те, що в майбутньому основу доказової бази формуватимуть саме електронні докази, оскільки цифровий прогрес не оминув і сферу кримінальних процесуальних відносин. Дедалі частіше місцем або засобом вчинення кримінальних правопорушень стає кіберпростір. Багато інформації, яка має орієнтовне чи доказове значення для розкриття та розслідування кримінальних правопорушень, зберігають в електронно-цифровому вигляді.

Електронні докази, на думку І. А. Смаль (2021), дедалі частіше стають одним з основних доказів у процесі розслідування кримінальних правопорушень, що зумовлено тим, що збільшується кількість кримінальних правопорушень, які вчиняють за допомогою мережі «Інтернет»; власники телефонів зберігають на своїх пристроях важливі відомості: геолокації, фотографії, відео, листування, що можуть містити цінну для правоохоронних органів доказову інформацію.

Свого часу класифікацію електронних доказів запропонував Європейський комітет з правової кооперації, створений при Раді Європи. У класифікації виокремлено «три типи електронних доказів, які можна використати в суді: докази із загальнодоступних вебсайтів, таких як публікації в блогах і зображення, завантажені на вебсайти соціальних мереж; суттєві докази (або докази змісту), тобто електронна пошта чи документи в цифровому форматі, які не є публічно доступними і які зберігаються на сервері; дані, призначені для ідентифікації користувача та дані про трафік («метадані»), які використовують для ідентифікації особи шляхом виявлення джерела зв'язку, а не вмісту».

Погоджуємося з позицією І. В. Басистої (2024), що для позначення інформації в бінарному вигляді доцільно послуговуватися таким слововжитком, як «цифрова», а не «електронна». Слід відмежовувати «цифрову інформацію» від «цифрових доказів», до яких ставлять вимоги належності, допустимості, достовірності.

Розглянуто поняття та особливості електронних доказів, способи їх збирання та правильне процесуальне оформлення результатів процесуальних дій, спрямованих на їх збирання (Holovkin et al., 2022).

Згідно з положеннями ст. 84 Кримінального процесуального кодексу України, доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому КПК порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.

На практиці цифровими доказовими відомостями є або речові докази (наприклад, жорсткий диск або оперативна пам'ять, на яких може міститися доказово значуща цифрова інформація) або документи (матеріали цифрової фотозйомки, звукозапису, відеозапису та ін.).

Згідно зі ст. 98 КПК, речовими доказами є матеріальні об'єкти, що були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можна використати як доказ факту чи обставин, що встановлюють під час кримінального провадження, зокрема предмети, що були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення.

Статтею 99 КПК передбачено, що документом є спеціально створений для збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості. Ці відомості можуть бути використані як доказ факту чи обставин, що встановлюють під час кримінального провадження.

Документами, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть бути:

1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема комп'ютерні дані);

2) матеріали, отримані під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надала Верховна Рада України;

3) складені в порядку, передбаченому КПК, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії;

4) висновки ревізій та акти перевірок;

5) довідки, висновки та інші документи спеціалістів[1].

Матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази[2].

З огляду на зазначене, надзвичайно важливим є висвітлення виявлення та збирання цифрових доказів саме під час формування матеріалів оперативно-розшукової діяльності як документів та відповідного джерела процесуальних доказів.

Матеріали оперативно-розшукової діяльності становлять документацію, яка показує зміст і результати оперативно-розшукових заходів, проведених у встановленому законодавством порядку.

Згідно з положеннями ст. 8 Закону України «Про оперативно-розшукову діяльність», ухвалення рішення про проведення оперативно-розшукових заходів, подання та розгляд відповідних клопотань, проведення оперативно-розшукових заходів, фіксація та використання їх результатів, проведення цих заходів до постановлення ухвали слідчого судді та інші питання їх проведення регулюються згідно з положеннями глави 21 Кримінального процесуального кодексу України з урахуванням особливостей, встановлених цим Законом, щодо мети проведення оперативно-розшукових заходів, суб'єкта ініціювання та проведення цих заходів, обґрунтування клопотання про їх проведення та підстав для його задоволення слідчим суддею, використання результатів оперативно-розшукових заходів та інших питань, обумовлених специфікою мети їх проведення. Ухвалює рішення про проведення оперативно-розшукових заходів, які не потребують дозволу слідчого судді або рішення прокурора, керівник відповідного оперативного підрозділу або його заступник з повідомленням про ухвалене рішення прокурора[3].

З огляду на зазначені законодавчі реалії, вважають за доцільне застосовувати методику отримання цифрових доказів, напрацьовану в кримінальному процесі та криміналістиці й під час проведення оперативно-розшукової діяльності з урахуванням її особливостей.

Серед основних способів отримання цифрових доказів у межах кримінального процесу доцільно виокремити:

1. Під час проведення слідчих дій (оформлюють протоколом з додатками, який є джерелом доказів):

а) огляд матеріалів з відкритих джерел (застосування принципів протоколу Берклі).

Слушною є позиція М. І. Пашковського (2024), що цифрові дані з відкритих джерел, а саме текстова інформація, відео-, аудіозаписи, фото і та інші графічні зображення разом з інформацією про використані засоби та способи оприлюднення зазначених відомостей можуть бути доказами в кримінальних провадженнях про подію кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення) та про винуватість

[1] Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17/ed20120413#Text

[2] Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

[3] Там само.

підозрюваного, обвинуваченого у вчиненні кримінального правопорушення, форму вини, мотив і мету вчинення кримінального правопорушення (пп. 1, 2 ч. 1 ст. 91 КПК України).

Протокол Берклі – це механізм фіксації цифрової інформації з відкритих джерел, встановлений світовою практикою документування злочинів. Тобто документуванню підлягають не лише фактичні дані приватного спілкування, а й інформація з відкритих джерел з метою подальшого її використання як доказу для правосуддя (Havryliuk et al., 2024).

Протокол Берклі розробили в Центрі прав людини Каліфорнійського університету в Берклі разом з Офісом Верховного комісара ООН з прав людини. Протокол являє собою практичний посібник з ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права.

У Протоколі наголошено на стандартах розслідування порушень міжнародного права, зокрема порушень прав людини та норм міжнародного кримінального права, включно з воєнними злочинами, злочинами проти людяності та геноцидом. Крім того, положення Протоколу можуть застосовувати до інших видів розслідувань, зокрема в межах національних чи муніципальних судів (Berkeley Protocol, 2024).

Збирати онлайн-контент можна вручну за стандартною операційною процедурою або автоматизовано за допомогою різноманітних інструментів, зокрема, з використанням можливостей OSINT.

Актуальність питання полягає в тому, що Рада Європи замовила підготовку звіту, який охоплює порівняльне дослідження та аналіз чинних національних правових положень, ухвалених або адаптованих з урахуванням впливу електронних доказів на правила доказування та способи доказування, з акцентом на провадженнях у сферах цивільного, адміністративного та комерційного права (The use of electronic.., 2016).

О. Користін, Б. Денисенко (2024) слушно стверджують, що OSINT, або інформація з відкритих джерел, є найширшим поняттям й охоплює «всю (загальнодоступну) інформацію з відкритих джерел у будь-якому форматі, що може бути здобута будь-яким законним та етично прийнятним шляхом без жодних обмежень чи то безплатно, чи на платній основі». Тому «простий збір та надання необробленої, сирої інформації не є OSINT».

Під час оцінки отриманих з відкритих джерел цифрових даних важливо поставити собі питання, а чи не є такі відомості дезінформацією. Сучасні технології дають змогу створювати deepfake неймовірної якості та глибини.

В. Матвєєв (2023) вважає, що таку дезінформацію продукують з різною метою, зокрема й задля психологічного впливу, загострення діалогу, шахрайства, фінансових афер тощо. Головно те, що через поширення фейків є ймовірність і порушення приватності, що в кінцевому результаті негативно впливатиме на особисте життя та професійну сферу тих, про кого поширили такі фейки;

б) отримання шляхом тимчасового доступу до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку.

Здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку без їх вилучення (ст. 159 КПК)[1];

в) тимчасове вилучення майна під час обшуку чи огляду вилучення в межах обшуку, особистого обшуку під час затримання особи на підставі ст. 208 КПК України.

У разі потреби слідчий чи прокурор виготовляє за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невіддільних частинах. Копіювання такої інформації здійснюють із залученням спеціаліста.

У практичній діяльності під час проведення обшуку виникає низка проблем, пов'язаних з отриманням цифрових доказів з відповідних електронних носіїв інформації.

По-перше, зазвичай відсутня згода особи на надання доступу до пристрою без необхідності подолання засобів логічного захисту (блокування, паролі тощо.), що надалі ускладнює роботу фахівця, який його оглядає або проводить експертизу.

Таку проблему частково можна розв'язати уважним дослідженням інших предметів та документів, які виявлені під час обшуку та які можуть бути носіями інформації та надати можливості щодо подальшого подолання систем логічного захисту.

Доцільно проводити глибоку інформаційно-аналітичну роботу щодо особи під час підготовки до проведення слідчої дії, а також комплексний аналіз матеріалів попередньо проведених НСРД та ОРЗ (за наявності) з метою виявлення необхідних відомостей.

По-друге, навіть у разі добровільного надання особою доступу до пристрою, повне копіювання інформації з нього може зайняти значний час, з огляду на значний обсяг пам'яті

[1] Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17/ed20120413#Text

сучасних технічних засобів, наявність значної кількості файлів на них тощо.

Вбачається за доцільне концентруватися на конкретній інформації, яка може мати значення для досудового розслідування кримінального провадження (фотографії документів, список контактів особи, листування електронною поштою, в месенджерах між учасниками протиправної діяльності тощо).

– Відшукання під час проведення судової комп'ютерно-технічної експертизи.

Під час проведення зазначеної експертизи здійснюють відшукання, вилучення та систематизацію необхідної інформації. Отримані внаслідок проведення експертизи фактичні дані фіксують у висновку експерта та додатках до нього.

Після приєднання висновку експерта до матеріалів кримінального провадження встановлені в ньому фактичні дані можна використовувати для з'ясування необхідних обставин вчинення кримінального правопорушення.

– Добровільне надання особою цифрових доказів під час проведення слідчих дій (допиту, одночасного допиту, огляду місця події тощо.

2) Під час негласних слідчих розшукових дій (якщо відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати шляхом проведення гласних слідчих (розшукових) дій), переважну більшість яких згідно з положеннями ст. 246 КПК проводять у разі розслідування тяжких або особливо тяжких злочинів:

а) проведення аудіо-, відеоконтролю особи (є різновидом втручання у приватне спілкування, яке проводять без її відома на підставі ухвали слідчого судді, якщо є достатні підстави вважати, що розмови цієї особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування) (ст. 260 КПК) та аудіо-, відеоконтролю місця (ст. 270 КПК)[1];

б) зняття інформації з електронних комунікаційних мереж (комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг) є різновидом втручання у приватне спілкування, що проводять без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можливо встановити обставини, які мають значення для кримінального провадження) (ст. 263 КПК)[2];

в) зняття інформації з електронних інформаційних систем, яка полягає в пошуку, виявленні й фіксації відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача) (ст. 264 КПК)[3].

Зняття інформації з електронних інформаційних систем або їх частин можна здійснювати за допомогою безпосереднього фізичного доступу до них і шляхом програмного віддаленого проникнення.

Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

У практичній діяльності зазвичай аналіз отриманої за результатами проведення НСРД інформації (листування в месенджерах) здійснюється за допомогою спеціалізованого програмного забезпечення та може бути доволі затяжним процесом з огляду на значний обсяг аналізованої інформації (листування в групах, новинні канали, побутова інформація тощо.)

Для підвищення ефективності зазначеної роботи доцільним є концентрація зусиль на вивченні листування між учасниками злочинної схеми, робочих груп і документів, які в них пересилають. Водночас можна використовувати пошук за відповідними ключовими словами.

– Обстеження публічно недоступних місць, житла чи іншого володіння особи шляхом таємного проникнення в них, зокрема з використанням технічних засобів, з метою виявлення і фіксації слідів вчинення тяжкого або особливо тяжкого злочину, в тому числі цифрових (ст. 267 КПК)[4].

У межах проведення цього виду НСРД можливе дослідження електронних носіїв інформації та електронних-обчислювальних машин та негласне отримання з них потенційних цифрових доказів.

– Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК)[5].

Під час досудового розслідування тяжких або особливо тяжких злочинів можуть бути отримані відомості, речі й документи, які мають значення для досудового розслідування, особою, яка відповідно до закону виконує спеціальне завдання, беручи участь в організованій групі чи злочинній організації, або є учасником зазначеної групи чи організації, який на конфіденційній основі співпрацює з органами досудового розслідування.

– Використання конфіденційного співробітництва (ст. 275 КПК)[6].

[1] Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17/ed20120413#Text

[2] Там само.

[3] Там само.

[4] Там само.

[5] Там само.

Слідчий має право використовувати інформацію, отриману внаслідок конфіденційного співробітництва з іншими особами, або залучати цих осіб до проведення негласних слідчих (розшукових) дій у випадках, передбачених цим Кодексом.

Протоколи про хід і результати проведеної негласної слідчої (розшукової) дії (або її етапів) складає слідчий, якщо дію проводять за його безпосередньої участі, в інших випадках – уповноваженим працівником оперативного підрозділу. Протоколи мають відповідати загальним правилам фіксації кримінального провадження.

Кожний протокол про результати проведеної негласної слідчої (розшукової) дії з додатками не пізніше 24 годин після його складання передають прокурору, який здійснює нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва і, відповідно, є процесуальним доказом (документом)[1].

З погляду криміналістики, звернемося до Основних положень державного стандарту ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», що набув чинності з 1 січня 2019 року.

Стандарт ISO/IEC 27037:2012 надає настанови для специфічної діяльності з оброблення потенційних цифрових доказів. Такими процесами є: ідентифікація, збирання, здобуття та збереження потенційних цифрових доказів. Ці процеси потрібні під час слідства для забезпечення цілісності цифрових доказів, тобто застосування прийнятної методології їх, яка гарантує допустимість доказів у законодавчих, дисциплінарних та інших відповідних судових процесах. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть бути корисними на стадії аналізування потенційних цифрових доказів.

С. М. Виганяйло (2023) вважає, що цей стандарт також спрямовано на інформування осіб, які ухвалюють рішення, та тих, кому потрібно визначати надійність потенційних цифрових доказів, що були їм надані. Він прийнятний для організацій, яким необхідно захищати, аналізувати та презентувати потенційні цифрові докази. Він важливий для правоохоронних органів, які формують та запроваджують процедури щодо цифрових доказів часто як частину доказів більшого об'єму.

Оскільки під час оперативно-розшукової діяльності гласні слідчі дії не проводять, доцільним є впровадження принципів Протоколу Берклі, а саме огляду матеріалів з відкритих джерел під час оперативного пошуку або кримінального аналізу.

Оперативний пошук – це здійснюваний оперативними підрозділами комплекс оперативних і розвідувальних заходів, спрямованих на безпосереднє та аналітичне отримання, перевірку, систематизацію та використання інформації про ознаки дій, що посягають на суспільні відносини, а також осіб, причетних до їх вчинення, виявлення осіб і фактів, що становлять оперативний інтерес.

Згідно з визначенням поняття форми ОРД, С. П. Пекарський (2022) зазначає, що для неї характерна пошукова робота, яку розуміємо як систему заходів, спрямованих на одержання фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена КК України, її повну і швидку перевірку та фіксацію.

Кримінальний аналіз – це діяльність, яка використовує систематичні методи та інформацію для вивчення проблем злочинності й правопорушень з метою підтримки діяльності правоохоронних органів. Він передбачає виявлення, збір, пояснення та оцінку інформації про стан злочинності, її причини, а також просторові та часові чинники, щоб допомогти у затриманні злочинців, об'єктивному розумінні кримінального середовища та зниженні рівня злочинності.

Як приклад, під час пошукової роботи можна використовувати матеріали журналістських розслідувань, аналітичні матеріали громадських організацій, інтернет-ресурсів, що надають можливість дослідження витрат публічних коштів тощо.

Доцільним є вивчення та перевірка відомостей з повідомлень про протиправну діяльність у соціальних мережах, спеціалізованих каналах у месенджерах тощо.

Отримані в такий спосіб цифрові докази в комплексі з іншими матеріалами можуть бути використані як підстави для заведення оперативно-розшукової справи, а після їх належної перевірки – для початку досудового розслідування, попередження, виявлення, припинення і розслідування кримінальних правопорушень, взаємного інформування підрозділів, уповноважених на оперативно-розшукову діяльність, інших правоохоронних та державних органів відповідно до положень статті 10 Закону України «Про оперативно-розшукову діяльність».

Крім того, важливим джерелом отримання цифрових доказів у межах оперативно-розшукової діяльності є проведення оперативно-розшукових заходів у порядку статті 8 Закону України «Про оперативно-розшукову діяльність». Їхнє здійснення регулюється згідно з положеннями глави 21 КПК з урахуванням особливостей, встановлених цим Законом.

[6] Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17/ed20120413#Text

[1] Там само.

Серед зазначених ОРЗ можна виокремити передбачені п. 2, 7, 8, 9-14 ч. 1 Закону України «Про оперативно-розшукову діяльність».

Зміст та вимоги до протоколів проведення ОРЗ загалом відповідають аналогічним до протоколів НСРД щодо форми, долучення додатків тощо.

Зазначені матеріали можуть бути використані:

1) як приводи та підстави для початку досудового розслідування відкриття кримінального провадження та подальшої легалізації у встановленому законом порядку;

2) отримання фактичних даних, які можуть бути доказами в кримінальному провадженні.

Водночас у практичній діяльності під час використання протоколів проведення оперативно-розшукових заходів сторона обвинувачення постає перед такою проблематикою під час оцінки доказів судом.

Протоколи ОРЗ зазвичай оцінюють комплексно як один доказ – «матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність». Натомість протоколи проведення НСРД – кожен окремо як «складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії».

Така практика сприяє знеціненню протоколів проведення ОРЗ як джерела доказів та мінімізації їх впливу на доказову базу, що потребує виправлення.

Ще одним важливим джерелом інформації, від якого можуть надходити цифрові докази, є використання можливостей конфіденційної співпраці й гласних і негласних штатних та позаштатних працівників у межах оперативно-розшукової діяльності.

З огляду на викладене потрібно передбачити механізм використання такої інформації як доказів у кримінальному провадженні, наприклад у разі наявності згоди та подальшої конфіденційної співпраці вже в межах досудового розслідування.

Аналіз українських і міжнародних джерел свідчить, що цифрові докази стають невіддільною частиною кримінального процесу та оперативно-розшукової діяльності. В Україні сформувалася ґрунтовна наукова дискусія щодо їх природи та застосування, але законодавче регулювання потребує подальшого вдосконалення. Міжнародний досвід демонструє, що ефективне використання цифрових доказів можливе лише за належної процедури збереження та перевірки автентичності. У перспективі важливим є поєднання наукових напрацювань, міжнародних стандартів і практичних методів OSINT для формування цілісної системи роботи із цифровими доказами в Україні.

Незважаючи на значні досягнення, цифрові докази пов'язані з низкою викликів. Передусім це питання автентичності: цифрова інформація легко піддається зміні, тому важливо гарантувати її незмінність за допомогою хешування та інших технічних засобів.

Другий виклик – забезпечення ланцюга збереження (chain of custody), що особливо актуально в умовах транскордонних розслідувань.

Третя проблема – допустимість у суді, оскільки законодавство часто відстає від технологічних реалій. Додатковими викликами є великі обсяги цифрових даних та потреба у спеціальній експертизі.

Можна погодитися з думкою Г. К. Авдєєвої (2023) про те, що, незважаючи на появу наприкінці XX століття нових поколінь електронних пристроїв та програмних продуктів, що призвело до виникнення нових типів сигналів і форматів даних, збільшення кількості способів кодування і перетворення інформації в цифровому вигляді, у кримінальному процесуальному законодавстві України не лише бракує визначення терміна «цифрові докази», а й не зазначений порядок їх збирання, зберігання, аналізу та використання у кримінальному провадженні.

С. М. Виганяйло (2023) вважає, що в умовах війни в Україні актуальним стає питання електронних цифрових доказів як воєнних, так і цивільних злочинів. Дуже багато питань постає із цього приводу, а саме: що ми можемо вважати електронним цифровим доказом (які формати можуть бути в суді доказами; що є оригіналом чи дублікатом, чи копією), хто та як може збирати такі докази, як і куди передавати.

Відповідність стандартам цифрових доказів є дуже важливою, адже електронні дані набагато легше змінити чи підробити, ніж традиційні форми доказів, необхідно дотримуватися правил поводження з даними, які нададуть можливість забезпечити допустимість доказів.

О. П. Метелев (2023) порушує питання використання в кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності.

Науковці доводять, що переважну більшість цифрової інформації, яка надалі може мати доказове значення, отримують шляхом проведення негласних заходів під час контррозвідувальної та оперативно-розшукової діяльності. Така цифрова інформація, на думку авторів, може слугувати лише приводами та підставами для початку досудового розслідування в кримінальному провадженні.

Недостатня гармонізація кримінального процесуального законодавства та законодавства, що регулює контррозвідувальну і оперативно-розшукову діяльність, негативно впливає на ефективність виконання оперативними підрозді-

лами своїх завдань. Подальша реформа вітчизняної правоохоронної системи має відбуватися за прикладом провідних західних країн та США, де поняття «оперативно-розшукова діяльність» взагалі немає. У більшості закордонних демократичних країн світу таємне поліцейське розслідування є кримінально-процесуальною діяльністю, що являє собою гласні та негласні процесуальні дії, які здійснюють під керівництвом прокурора.

Погоджуючись із цією позицією в частині недостатньої гармонізації законодавства, не підтримуємо думку про обмежене використання матеріалів ОРД та КРД лише як приводів та підстав для початку досудового розслідування в кримінальному провадженні.

Крім того, з огляду на європейську практику, яка підкреслює важливість та пріоритетність превентивної діяльності правоохоронних органів, підвищену увагу до аналізу тенденцій і прогнозування розвитку злочинності, а також встановлення причин та умов, які сприяють вчиненню правопорушень, що відповідають одній з форм оперативно-розшукової діяльності – оперативно-розшуковій профілактиці, вважають недоцільним рух правової доктрини до заперечення поняття «оперативно-розшукова діяльність».

Висновки

Дослідження підтвердило, що цифрові докази є невіддільною складовою сучасного кримінального процесу та оперативно-розшукової діяльності. Вони дають змогу ефективно документувати протиправні дії та підвищувати результативність правоохоронної системи. Водночас залишаються актуальними проблеми автентичності, допустимості та збереження цифрових даних. Необхідним є вдосконалення законодавчої бази України, гармонізація норм кримінального процесуального права з міжнародними стандартами, а також впровадження сучасних методів цифрової криміналістики.

Ефективне використання цифрових доказів, отриманих під час оперативно-розшукової діяльності, потребує внесення змін до кримінального процесуального законодавства та Закону України «Про оперативно-розшукову діяльність».

Отже, вбачається за доцільне:

1. Для приведення кримінального процесуального законодавства відповідно до вимог сучасності доповнити ч. 2 ст. 84 КПК поняттям «цифрові докази».

Доцільно додати спеціальну статтю КПК (наприклад 99-1), у якій визначити, що цифрові докази – це відомості або документи в цифровій або електронній формі, що містять інформацію про обставини, які мають значення для кримінального провадження, отримані під час досудового розслідування чи оперативно-розшукової діяльності.

2. З метою удосконалення можливостей використання матеріалів ОРД як допустимих доказів у межах кримінального провадження внести зміни до п. 3 ч. 2 ст. 99 КПК, зокрема після слів: «складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій» додати формулювання «та оперативно-розшукових заходів».

3. У статті 8 Закону України «Про оперативно-розшукову діяльність» зазначити, «що за результатами проведення оперативно-розшукових заходів складають протоколи відповідно до вимог КПК України, які можуть бути визнані доказами в межах кримінального провадження».

4. Додати до Закону України «Про оперативно-розшукову діяльність» нову статтю: «Аналітична робота та використання її результатів».

Підрозділи, що здійснюють оперативно-розшукову діяльність, мають безпосередній, зокрема автоматизований, доступ до автоматизованих інформаційних і довідкових систем, реєстрів і банків (баз) даних, власником (адміністратором) яких є державні органи або органи місцевого самоврядування, користуються державними, зокрема урядовими, засобами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами.

Порядок такого доступу визначають відповідні міжвідомчі угоди (договори), спільні накази (розпорядження) та протоколи до них або в порядку електронної інформаційної взаємодії, якщо інше не передбачено законом.

Аналітичну роботу можна здійснювати з використанням аналітичних інструментів – спеціального програмного забезпечення з оброблення інформації та перетворення її у форму, прийнятну для розуміння та використання.

Результати аналітичної роботи можуть використовувати як підставу для оперативно-розшукової діяльності або як доказ у кримінальному провадженні в разі їх підтвердження додатковими матеріалами, зібраними згідно з Кримінальним процесуальним кодексом України.

5. Передбачити законодавчий механізм залучення конфіденційних джерел та отриманих від них під час оперативно-розшукової діяльності матеріалів за наявності добровільної згоди до подальшої конфіденційної співпраці в межах досудового розслідування.

Зазначені зміни дадуть можливість більш ефективно використовувати цифрові докази, отримані під час оперативно-розшукової діяльності для виконання її завдань та зростання ефективності діяльності правової системи загалом.

References

[1] Avdieieva, H.K. (2023). Digital evidence and artificial intelligence systems in law enforcement activities. *Issues of combating crime*, 46, 32-40. DOI: 10.31359/2079-6242-2022-46-32

[2] Basysta, I.V., Havriliuk, L.V., Hutnyk, A.V., & Khytra, A.Ya. (2024). Using digital data from open sources during the investigation of criminal offenses: some aspects. *Scientific and informational bulletin of the Ivano-Frankivsk University of Law named after King Danylo Halytsky. Series "Law",* 17, 227-243. DOI: 10.33098/2078-6670.2024.17.29.227-243

[3] Batyrhareieva, V.S., & Netesa, N.V. (2024). The use of information and telecommunication technologies by offenders when committing actions related to the glorification of the aggressor: criminological and criminal law analysis based on case law. *Issues of combating crime*, 47, 18-29. DOI: 10.31359/2079-6242-2024-47-18

[4] Berkeley Protocol on Digital Open Source Investigations. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. (2024). Retrieved from https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

[5] Fomina, T.H., & Rachynskyi, O.O. (2023). Electronic evidence in criminal proceedings: problematic issues of theory and practice. *Bulletin of the Kharkiv National University of Internal Affairs,* 3(102), 207-220. DOI: 10.32631/v.2023.3.43

[6] Harasymov, O.I., Marko, S.I., & Riashko, O.V. (2023). Digital evidence: some problematic issues regarding their concept and use in criminal proceedings. *Scientific Bulletin of the Uzhhorod National University. Series "Law",* 75, 158-162. DOI: 10.24144/2307-3322.2022.75.2.25

[7] Havryliuk, L.V., Basysta, I.V., & Afonin, D.S. (et al.). (2024). *The use of electronic evidence during pre-trial investigations of crimes against peace, security of mankind and international law and order (Berkeley Protocol).* M.S. Tsutskiridze (Eds.). Kyiv: DNDI MIA of Ukraine; Polytechnics.

[8] Holovkin, B.M., Denykovych, O.I., Lutsyk, V.V., & Tsekhan, D.M. (2022). *Cybercrime and digital evidence = Cybercrime and digital evidence.* O. Denykovych, H. Shmeltser (Eds.). Lviv: Ivan Franko National University of Lviv. Retrieved from https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

[9] Hutnyk, A.V., & Khytra, A.Ya. (2022). *Criminal procedural and forensic principles of using electronic documents in evidence.* Lviv: LvDUVS. Retrieved from https://dspace.lvduvs.edu.ua/handle/1234567890/4725

[10] Hutsaliuk, M.V., Gavlovskyi, V.D., & Khakhanovskyi, V.H. (et al.). (2020). *The use of electronic (digital) evidence in criminal proceedings.* O.V. Korneiko (Eds.). (2nd, rev.). Kyiv: Nat. acad. of internal affairs. Retrieved from https://elar.navs.edu.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content

[11] Korystin, O., & Denysenko, B. (2024). Section 23. Methodological principles of OSINT. *Implementation of the philosophy of "Intelligence-led Policing" in the criminal analysis system of the National Police of Ukraine* (pp. 289-297). Kyiv. DOI: 10.36486/978-966-2310-66-5-23

[12] Kozytska, O. (2020). On the concept of electronic evidence in criminal proceedings. *Legal Scientific Electronic Journal,* 8, 418-421. DOI: 10.32782/2524-0374/2020-8/103

[13] Matvieiev, V. (2023). Problems and challenges related to the collection of electronic evidence. *Site "Justtalk".* Retrieved from https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv

[14] Metelev, O.P. (2023). Digital evidence in criminal proceedings: specific characteristics. *Bulletin of criminal justice,* 1-2, 42-53. DOI: 10.17721/2413-5372.2023.1-2/42-53

[15] Pashkovskyi, M.I. (2024). Circumstances that are important for criminal proceedings and the relevance of digital evidence from open sources. *Scientific perspectives*, 10(52), 984-998. DOI: 10.52058/2708-7530-2024-10(52)-984-998

[16] Pavlova, Yu.S. (2023). Classification of electronic evidence: theoretical and practical aspects. *State and regions. Series "Law",* 3(81), 32-36. DOI: 10.32782/1813-338X-2023.3.5

[17] Pekarskyi, S.P. (2022). *Fundamentals of operational and investigative activities of criminal police units.* Kyiv: Dakor.

[18] Ratnova, A.V. (2021). Criminal procedural and forensic fundamentals of using electronic documents in evidence. *Doctoral thesis.* Lviv. Retrieved from https://dspace.lvduvs.edu.ua/handle/1234567890/3747

[19] Shepitko, V.Yu. (2023). The use of digital information in proving war and other crimes during the war of Russia against Ukraine. *Current problems of combating crime and corruption:* collection of theses of the All-Ukrainian scientific-practical conference (pp. 177-182). Kharkiv: Yurait. Retrieved from https://ivpz.kh.ua/wp-content/uploads/2023/03/%D0%90%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%96-%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC

%D0%B8-%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97-%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%96-%D1%82%D0%B0-%D0%BA%D0%BE%D1%80%D1%83%D0%BF%D1%86%D1%96%D1%97_17.02.23.pdf

[20] Shepitko, V.Yu., & Shepitko, M.V. (2021). *Criminal law, forensics and forensic sciences*. Kharkiv: Pravo.

[21] Shumylo, M.Ye., Yurka, R., & Kaplina, V.A. (2019). Information theory of evidence and problems of using electronic means of evidence in criminal proceedings. *Bulletin of the National Academy of Legal Sciences of Ukraine*, 26(2), 137-152. Retrieved from http://nbuv.gov.ua/UJRN/vapny_2019_26_2_12

[22] Skrypnyk, A.V. (2022). *Using digital information in criminal procedural evidence.* Kharkiv: Law. Retrieved from https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=4651&download_id=1537&srsltid=AfmBOoqLhpnR4HME2gQaaOF9flO1sCaApqN4AmIYYXg0YEZC9wdMpE1R

[23] Smal, I.A. (2021). Problematic aspects of the use of electronic evidence in criminal proceedings. Law and Society, 4, 226-232. DOI: 10.32842/2078-3736/2021.4.30

[24] The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. (2016). *European Committee on Legal Co-Operation (CDCJ)*. Retrieved from https://rm.coe.int/1680700298

[25] Vyhaniailo, S.M. (2023). Electronic digital evidence in martial law conditions. *Science in martial law conditions: searches, problems, development prospects:* materials of the All-Ukrainian scientific-practical conference (pp. 17-19). Dnipro: DDUVS. Retrieved from https://er.dduvs.edu.ua/bitstream/123456789/11655/5/%D0%9A%D0%BE%D0%BD%D1%84%2003.05.pdf

Список використаних джерел

[1] Авдєєва Г. К. Цифрові докази та системи штучного інтелекту в правоохороній діяльності. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 32–40. DOI: 10.31359/2079-6242-2022-46-32

[2] Басиста І. В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія «Право».* 2024. Вип. 17. С. 227–243. DOI: 10.33098/2078-6670.2024.17.29.227-243

[3] Батиргареєва В. С., Нетеса Н. В. Використання правопорушниками інформаційно-телекомунікаційних технологій під час вчинення дій, пов'язаних із глорифікацією агресора: кримінологічний та кримінально-правовий аналіз за матеріалами судової практики. *Питання боротьби зі злочинністю.* 2024. № 47. С. 18–29. DOI: 10.31359/2079-6242-2024-47-18

[4] Berkeley Protocol on Digital Open Source Investigations. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian La.* 2024. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

[5] Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник Харківського національного університету внутрішніх справ.* 2023. № 3 (102). С. 207–220. DOI: 10.32631/v.2023.3.43

[6] Гарасимов 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. С. 158–162. DOI: 10.24144/2307-3322.2022.75.2.25

[7] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / [Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін та ін.] ; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України ; Політехніка, 2024. 196 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

[8] Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посіб. / за ред. О. Денькович, Г. Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

[9] Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : кол. монографія. Львів : ЛьвДУВС, 2022. 204 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4725

[10] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доповн. Київ : Нац. акад. внутр. справ, 2020. 104 с. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content

[11] Користін О., Денисенко Б. Розділ 23. Методологічні засади OSINT. *Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України* : монографія. Київ, 2024. С. 289–297. DOI: 10.36486/978-966-2310-66-5-23

[12] Козицька О. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал.* 2020. № 8. С. 418–421. DOI: 10.32782/2524-0374/2020-8/103

[13] Матвєєв В. Проблеми та виклики, пов'язані зі збором електронних доказів. *Justtalk :* [сайт]. 2023. URL: https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom- elektronnih-dokaziv

[14] Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* 2023. № 1–2. С. 42–53. DOI: 10.17721/2413-5372.2023.1-2/42-53

[15] Пашковський М. І. Обставини, що мають значення для кримінального провадження, та належність цифрових доказів з відкритих джерел. *Наукові перспективи.* 2024. № 10 (52). С. 984–998. DOI: 10.52058/2708-7530-2024-10(52)-984-998

[16] Павлова Ю. С. Класифікація електроних доказів: теоретичні та практичні аспекти. *Держава та регіони. Серія «Право».* 2023. № 3 (81). С. 32–36. DOI: 10.32782/1813-338X-2023.3.5

[17] Пекарський С. П. Основи оперативно-розшукової діяльності підрозділів кримінальної поліції : навч. посіб. Київ : Дакор, 2022. 186 с.

[18] Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філософії : 081 «Право». Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747

[19] Шепітько В. Ю. Використання цифрової інформації в доказуванні воєнних та інших злочинів під час війни Росії проти України. *Актуальні проблеми протидії злочинності та корупції :* зб. тез Всеукр. наук.-практ. конф. (Харків, 17 лют. 2023 р.). Харків : Юрайт, 2023. С. 177–182. URL: https://ivpz.kh.ua/wp-content/uploads/2023/03/%D0%90%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%96-%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8-%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97-%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%96-%D1%82%D0%B0-%D0%BA%D0%BE%D1%80%D1%83%D0%BF%D1%86%D1%96%D1%97_17.02.23.pdf

[20] Шепітько В. Ю., Шепітько М. В. Кримінальне право, криміналістика та судові науки : енциклопедія. Харків : Право, 2021. 508 с.

[21] Шумило М. Є., Юрка Р., Капліна В. А. Інформаційна теорія доказів та проблеми використання електронних засобів доказування у кримінальному провадженні. *Вісник Національної академії правових наук України.* 2019. Т. 26. № 2. С. 137–152. URL: http://nbuv.gov.ua/UJRN/vapny_2019_26_2_12

[22] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків : Право, 2022. 408 с. URL: https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=4651&download_id=1537&srsltid=AfmBOoqLhpnR4HME2gQaaOF9fIO1sCaApqN4AmIYYXg0YEZC9wdMpE1R

[23] Смаль І. А. Проблемні аспекти застосування електронних доказів у кримінальному судочинстві. *Право і суспільство.* 2021. № 4. С. 226–232. DOI: 10.32842/2078-3736/2021.4.30

[24] The use of electronic evidence in civil and administrative law proceedings and its affect on the rules of evidence and modes of proof. *European Committee on Legal Co-Operation (CDCJ).* Strasbourg, 27 July 2016. URL: https://rm.coe.int/1680700298

[25] Виганяйло С. М. Електронні цифрові докази в умовах воєнного стану. *Наука в умовах воєнного стану: пошуки, проблеми, перспективи розвитку :* матеріали Всеукр. наук.-практ. конф. (Дніпро, 3 трав. 2023 р.). Дніпро : ДДУВС, 2023. С. 17–19. URL: https://er.dduvs.edu.ua/bitstream/123456789/11655/5/%D0%9A%D0%BE%D0%BD%D1%84%2003.05.pdf

VASYLYNCNUK Viktor
Doctor of Law, Professor, Professor of the Department of Operational Investigation and National Security of the National Academy of Internal Affairs
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-5415-8450;
POPTANYCH Yurii
Postgraduate Student of the National Academy of Internal Affairs
Kyiv, Ukraine
ORCID: https://orcid.org/0009-0000-1680-5987

Use of Digital Evidence Obtained during Operational and Search Activities

Abstract. The article examines the issue of using digital evidence in criminal proceedings and operational-search activities. The relevance of digitalization for the development of the state, as well as its impact on the combating crime sphere, is determined. Particular attention is paid to the issue of authenticity, chain of custody and admissibility of digital evidence in judicial practice. National and international approaches are analyzed, and recommendations are proposed for improving legislation and practical use of digital evidence in Ukraine. The research is devoted to improving legislation and developing recommendations for practical units on the detection and use of digital evidence obtained during operational-search activities. The range of sources of obtaining digital evidence is determined from open sources (OSINT, Berkeley Protocol) to special technical measures during covert investigative (search) actions and operational-search activities. The main problems in the detection, fixation and use of digital evidence obtained during operational-search activities are identified. A number of amendments to the current legislation are proposed that may contribute to improving the results of using relevant materials in criminal proceedings. It is emphasized that the effective use of digital evidence in the activities of operational units increases the effectiveness of documenting crimes, contributes to strengthening the evidentiary base in criminal proceedings and developing the principle of the inevitability of punishment. It is noted that digital evidence is becoming an integral part of the modern criminal process and operational and investigative activities. The introduction of international standards, regulatory consolidation of the procedure for collecting, verifying and evaluating digital evidence will ensure increased efficiency of investigations, transparency of judicial proceedings and public trust in the justice system.

Keywords: evidence; criminal proceedings; operational and investigative activities; legal regulation; improvement; digitalization.