УДК 343.14(477):004
DOI 10.31558/2786-5835.2026.1.1.15

Шумило Микола Єгорович,
головний науковий співробітник
Інституту правотворчості та науково-правових
експертиз НАН України,
доктор юридичних наук, професор,
член-кореспондент НАПрН України
ORCID: https://orcid.org/0000-0003-0268-7961

Кузнецов Віталій Володимирович,
головний науковий співробітник
Інституту правотворчості та науково-правових
експертиз НАН України,
доктор юридичних наук, професор
ORCID: https://orcid.org/0000-0003-1727-4019

Метелев Олексій Павлович,
доктор філософії в галузі права,
доцент Національної академії Служби безпеки України
ORCID: https://orcid.org/0000-0003-2969-8388

ДОПУСТИМІСТЬ ПРОТОКОЛІВ НСРД З ДОДАТКАМИ, ЩО МАЮТЬ ВІДОМОСТІ У ЦИФРОВІЙ ФОРМІ ДЛЯ ОТРИМАННЯ СУДОВИХ ДОКАЗІВ

Статтю присвячено дослідженню допустимості протоколів негласних слідчих (розшукових) дій з додатками, що містять відомості в цифровій формі, у процесі формування судових доказів. Обґрунтовано, що специфіка правового регулювання НСРД, порядку їх проведення та способів фіксації результатів істотно ускладнює перевірку допустимості відповідних відомостей, особливо у випадках використання аудіо-, відеозаписів, електронних даних, носіїв комп'ютерної інформації та інших цифрових матеріалів. Показано, що визнання таких відомостей допустимими залежить не лише від дотримання загальних вимог кримінального процесуального законодавства, а й від належної технічної перевірки їх цілісності та автентичності. У дослідженні проаналізовано нормативні підстави проведення НСРД, вимоги до протоколів і додатків до них, а також типові недоліки документування, що можуть ставити під сумнів допустимість одержаних доказів. Особливу увагу приділено значенню «ланцюга зберігання доказів» (chain of custody), процедурі хешування, перевірці метаданих, а також можливості виявлення монтажу, модифікації чи іншого втручання в цифрові файли. Наголошено, що встановлення допустимості таких матеріалів має здійснюватися в умовах змагального судового розгляду з урахуванням права сторони захисту на перевірку дотримання процесуального порядку їх отримання.

У роботі акцентовано, що сама лише формальна наявність протоколу НСРД та доданих до нього цифрових носіїв не є достатньою для визнання відповідних відомостей допустимими доказами. Аргументовано, що оцінка таких матеріалів потребує поєднання процесуально-правового аналізу з дослідженням технічних характеристик цифрової інформації, які дають змогу встановити її походження, цілісність і відсутність стороннього втручання. Зроблено висновок, що допустимість протоколів НСРД із цифровими додатками визначається сукупністю процесуальних і технологічних критеріїв. Необхідними для цього є пере-

вірка законності підстав проведення НСРД, дотримання правил фіксації та збереження цифрової інформації, встановлення її незмінності й достовірності походження, а також використання в судовому розгляді спеціальних знань експертів і спеціалістів. Доведено, що лише комплексне врахування цих вимог дає змогу визнати відомості, одержані внаслідок НСРД, належною доказовою основою у кримінальному провадженні.

Ключові слова: *аудіоконтроль особи, відеоконтроль особи, автентичність цифрової інформації, допустимість доказів, додатки до протоколу, електронні дані, кримінальне процесуальне законодавство, ланцюг зберігання доказів, негласні слідчі (розшукові) дії, протокол, цілісність даних, цифрові докази.*

Постановка проблеми. У чинному Кримінальному процесуальному кодексі України (далі – КПК) негласні слідчі (розшукові) дії (далі – НСРД) належать до числа способів збирання доказів (ст. 93 КПК) [1]. Ступінь їх нормативного упорядкування, порядок і режим проведення істотно відрізняються від слідчих (розшукових) дій. Вони проводяться таємно, без чітко встановленої процесуальної форми, нерідко із застосуванням спеціальних технічних засобів, які обробляють інформацію з обмеженим доступом. Під час проведення слідчих (розшукових) дій органи досудового розслідування, оперативні співробітники діють відкрито: виступають від свого імені; повідомляють особам про учасників і мету проведення процесуальних дій, роз'яснюють їм права і обов'язки. Водночас під час проведення НСРД використовуються інші методи: нерідко участь виконавців маскується або легендується, відбувається втручання у приватне спілкування (телефонні розмови, інтернет-з'єднання, месенджери), здійснюється негласне візуальне спостереження за особою або місцем, отримуються відомості від анонімних джерел. Якби ці особи знали, що їх прослуховують чи за ними здійснюється негласне спостереження, то, мабуть, ніколи б не обговорювали підготовку і способи вчинення та маскування злочинів і таке інше.

Аналіз останніх досліджень та публікацій. Особливості доказування та проблеми допустимості і належності доказів у кримінальному процесі були об'єктом ґрунтовних наукових розробок багатьох відомих вчених. Так, дослідженню актуальних проблем доказового права присвятили свої роботи такі процесуалісти: Ю. П. Алєнін, Н. В. Глинська, І. В. Гловюк, Ю. М. Грошевий, В. П. Гмирко, О. В. Капліна, М. М. Михеєнко, В. Т. Нор, М. А. Погорецький, Д. Б. Сергєєва, С. М. Стахівський, В. М. Тертишник, Л. Д. Удалова, М. Є. Шумило та інші. Їх праці внесли неоціненний вклад у науку кримінального процесу, але з огляду на розвиток нових інформаційних технологій питання допустимості протоколів негласних слідчих (розшукових) дій з додатками, що містять відомості в цифровій формі, у процесі формування судових доказів, на нашу думку, потребує більш прискіпливого аналізу.

Постановка завдання. Мета статті – визначити особливості забезпечення допустимості протоколів негласних слідчих (розшукових) дій з додатками, що містять відомості в цифровій формі, у процесі формування судових доказів.

Виклад основного матеріалу дослідження. З метою забезпечення об'єктивності більшість НСРД, які передбачають втручання у приватне спілкування, проводиться з використанням технічних засобів: це аудіо-, відеоконтроль особи (ст. 260 КПК), зняття інформації з електронних комунікаційних мереж (ст. 263 КПК), зняття інформації з електронних інформаційних систем (ст. 264 КПК), обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК), спостереження за особою, річчю або місцем (ст. 269 КПК), аудіо-, відео контроль місця (ст. 270 КПК) тощо. Відповідно до п. 4.1 Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні (далі – Інструкція), перебіг і результати проведеної НСРД фіксуються у протоколі слідчим, якщо вона проводилася за його безпосередньої участі, а в інших випадках – уповноваженим працівником оперативного підрозділу. У п. 4.7 даної Інструкції вказується, що «до протоколу долучаються додатки, якими можуть бути: спеціально виготовлені копії, зразки об'єктів, речей і документів, письмові пояснення спеціалістів, які брали участь у проведенні відповідної дії, стенограма, аудіо-, відеозаписи, фототаблиці, схеми, зліпки, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу». Результати фіксації таких процесуальних дій, як правило, фіксуються на носіях цифрової інформації [2]. У п. 4.8. згаданої Інструкції наголошується, що фіксація результатів негласної слідчої (розшукової) дії повинна здійснюватися так, щоб завжди була можливість експертним шляхом встановити достовірність цих результатів. Ця вимога Інструкції повністю корелює з принципами Міжнародної організації комп'ютерних доказів (IOCE – International Organization on Computer Evidence), згідно з якими: 1) під час роботи з цифровими доказами повинні виконуватись всі загальні судово-експертні процедурні принципи (що означає – цифрові докази мають зберігатися і бути доступними для перевірки, щоб мати судову доказову цінність); 2) дії по дослідженню вилучених цифрових доказів не повинні вносити в них зміни; 3) у разі необхідності надання кому-небудь доступу до оригіналу цифрового доказу він повинен бути навчений і проінструктований відповідним чином; 4) вся діяльність, що стосується конфіскації (вилучення), доступу, зберігання і передачі цифрового доказу, повинна бути повністю задокументована і доступна для ознайомлення; 5) особа, в розпорядженні якої знаходиться цифровий доказ, повністю відповідальна за всі дії, які вчинені відносно цього доказу; 6) будь-яка агенція, яка відповідає за вибірку з пам'яті, вилучення, зберігання або передачу цифрового доказу, повинна погоджувати свою діяльність із цими принципами [3]. Якщо зазначені вище принципи IOCE не можуть бути дотримані, то відомості в цифровій формі навряд чи будуть прийняті як докази в суді.

Визнання допустимості протоколів негласних слідчих (розшукових) дій залежить від дотримання дозволів і заборон у кримінальному провадженні. Тому

необхідною умовою правомірного проведення НСРД є наявність для цього передбачених законом підстав, які включають сукупність інформаційних, нормативних і фактичних умов: 1) наявність відомостей про можливість отримання (перевірки) доказів (ст. 223 КПК); 2) неможливість отримати (перевірити) докази в інший спосіб (ч. 2 ст. 246 КПК). Останній складник підстав для прийняття такого рішення потребує конкретності і достатнього рівня обґрунтування. Як справедливо зазначає Г. Борейко, «слідчий, прокурор повинен зазначити, які заходи вже вжито для отримання (перевірки) доказів, однак їх проведення не дало необхідних результатів, для отримання доказів іншим шляхом» [4, с. 136]. Протоколи НСРД повинні відповідати загальним правилам фіксації у кримінальному провадженні. Водночас до оформлення таких процесуальних документів та додатків до них (ст. 104–106 КПК) існують певні особливості оформлення протоколу НСРД та додатків до нього, а саме: 1) у вступній частині протоколу НСРД додатково повинно бути зазначене відповідне рішення про проведення цієї НСРД – ухвала суду, постанова слідчого або прокурора; 2) можлива періодичність складання протоколів за результатами їх проведення; 3) фіксація їх результатів повинна здійснюватися так, щоб завжди була можливість експертним шляхом встановити достовірність цих результатів; 4) необхідність дотримання режиму секретності під час їх складання та роботи з ними [5, с. 38]. Фрагментарний аналіз змісту протоколів НСРД з додатками, що мають відомості у цифровій формі, свідчить про їх характерні недоліки, які ставлять під сумнів допустимість отриманих доказів. Так, у цих процесуальних документах не вказуються: особи, які фактично проводили НСРД, відомості про використані технічні засоби, про характер з'єднань, які можуть мати значення для конкретного кримінального провадження; не відображається перебіг і результати НСРД; залучаються не оригінали, а копії носіїв цифрової інформації і таке інше.

З метою законного і обґрунтованого визнання допустимості протоколів НСРД для отримання судових доказів важливо враховувати призначення інституту допустимості у процедурі формування судових доказів. На нашу думку, воно полягає в такому:

– абсолютній забороні використання доказових матеріалів, отриманих унаслідок катувань, нелюдського чи іншого поводження з людиною, що принижує її гідність;

– недопущення внесення навмисних спотворень змісту доказового матеріалу;

– забезпечення умов процесуальної перевірки перебігу і результатів одержання доказових відомостей;

– встановлення узгодженості доказу, отриманого з порушенням встановленого порядку з іншими доказами у кримінальному провадженні;

– констатації характеру процесуального правопорушення і його вплив на ступінь ураженості юридичної сили пропонованого стороною обвинувачення доказового матеріалу;

– забезпечення кооперaційної діяльності сторін і суду для ухвалення останнім справедливого судового рішення.

Такі особливості правового регулювання, порядку і методів проведення НСРД явно ускладнюють перевірку їх допустимості для формування судових доказів. Тому закон не завжди може дати вичерпної відповіді на всі питання як допустимості, так і недопустимості, що виникають у практиці його застосування. В таких випадках допустимість визначається не законом, а правосвідомістю, шляхом тлумачення його смислу через призму конкретної процесуальної ситуації. У зв'язку з цим необхідно застосовувати змагальний стандарт допустимості доказів. Це означає, що допустимість має формуватися судом за участю сторін судового процесу (ст. 89 КПК). Змагальний порядок встановлення допустимості включає: 1) активність сторін у постановці без обмежень питань щодо допустимості і недопустимості доказів; 2) відповіді на ці питання дає суд з урахуванням оцінки позицій сторін; 3) суд може проявити розумну активність у дослідженні цих питань під час формування власного внутрішнього переконання за відсутності належної активності сторін. Суд є суб'єктом оцінки допустимості судових доказів, керуючись стандартом «поза розумним сумнівом». Усі неспростовані сумніви щодо допустимості доказів, поданих стороною обвинувачення, повинні тлумачитися на користь обвинуваченого. Змагальність, рівність сторін, безпосередність, гласність – все це дає змогу перевірити верифікованість даних, що визначають їх допустимість.

Під час встановлення допустимості матеріалів НСРД, отриманих із застосуванням цифрових технологій, явно недостатньо лише юридичних засобів. Виникає потреба у спеціальних технічних знаннях, коли це стосується перевірки їх достовірності.

Якщо ж ідеться про специфічну оцінку носіїв цифрової інформації, одержаних внаслідок проведення НСРД, допустимість останніх передбачається через обов'язкову перевірку двох аспектів: цілісності (integrity) та автентичності (authenticity).

Цілісність стосується незмінності даних із моменту їх фіксації під час НСРД до моменту дослідження в суді. Міжнародний досвід дослідження цифрової інформації показує, що для гарантованого збереження цілісності доказів у цифровій формі, ретельну увагу необхідно приділяти саме дотриманню належної процесуальної процедури фіксації проведення НСРД, допущення спеціалістів для роботи з технічними засобами обробки та збереження цифрової інформації, а також забезпечення можливості всім сторонам кримінального провадження мати доступ до цифрової доказової бази.

Натомість автентичність (справжність) стосується джерела походження даних. Суд має бути впевнений, що цей доказ походить саме від того джерела, про яке заявляє сторона обвинувачення. Саме тому для забезпечення цілісності та автентичності використовується процедура хешування – створення унікального «цифрового відбитка» для будь-якого обсягу даних (файла аудіозапису, відео чи електронного документа). Спеціальна програма (алгоритм, наприклад, SHA-256) зчитує увесь вміст файла (кожен біт) і перетворює його на унікальний рядок символів фіксованої довжини. Однакові значення хеш-сум в оригінальному файлі і його копії свідчать про їх абсолютну ідентичність.

На нашу думку, хеш-сума – головний маркер допустимості для суду: якщо у файлі змінити хоча б одну кому, одну секунду тиші або один піксель, то хеш-сума файлу зміниться повністю. Неможливо підправити файл так, щоб його «цифровий відбиток» залишився, як в оригінальному файлі.

Досліджуючи міжнародний досвід оцінки допустимості доказів у цифровій формі, Г. К. Авдєєв зазначає, що у США суди встановлюють автентичність (справжність, достовірність) цифрових доказів відповідно до Правила 901 FREUSA за такою схемою: перевірка факту отримання цифрової інформації з конкретного цифрового пристрою, встановлення повної відповідності з оригіналом або з першою процесуально зафіксованою копією, встановлення відсутності змін з моменту їх фіксації. Для перевірки достовірності великого масиву цифрових даних використовується повна копія даних електронного пристрою, яка зберігає логічну структуру накопичувача інформації (включаючи видалені файли) та яку виготовляє спеціально залучений судовий експерт або спеціаліст [6, с. 160].

Далі треба зазначити, що коли проводяться звичайні слідчі (розшукові) дії (далі – СРД), наприклад, допит, фіксація доказових відомостей здійснюється слідчим безпосередньо. Водночас, коли проводиться більшість НСРД (наприклад, втручання у приватне спілкування – § 2 Глави 21 КПК), то така безпосередність просто неможлива через чинник обов’язкового застосування технічних засобів (технічна фіксація апаратно-програмними комплексами (далі – АПК) або спеціальними технічними засобами (далі – СТЗ), копіювання отриманих відомостей, документування (складання протоколу слідчим відбувається часто через тривалий час після проведення самої дії НСРД), зберігання (необхідність забезпечення специфічних умов збереження цифрової інформації)).

Проведення обов’язкової експертної оцінки додатків до протоколу НСРД, без якої в судовому розгляді майже неможливо визначити допустимість доказів, необхідне саме через проблематичність забезпечення виконання вимог ст. 23 КПК. Оскільки НСРД проводяться негласно, то сторона захисту в такому разі позбавлена можливості контролювати процес запису (формування доказових відомостей). Тому проведення експертизи (фоноскопічної, комп’ютерно-технічної

тощо) стає єдиним інструментом, що дає змогу підтвердити: відсутність ознак монтажу або вибіркового стирання / модифікації інформації; відповідність технічних характеристик запису пристрою, на якому він нібито здійснювався; цілісність метаданих файлів.

Потенційна допустимість матеріалу, одержаного за результатами проведення НСРД, нівелюється в разі неможливості встановити, де перебував первинний носій інформації, починаючи від моменту завершення конкретної НСРД аж до моменту призначення експертизи. Якщо в «ланцюгу збереження доказів» фіксується наявність так званих «сірих плям» (наприклад, диск не був опечатаний у належний спосіб), то виникає цілком обґрунтований сумнів щодо його автентичності.

Якщо ж ідеться про підходи до оцінки матеріалів, отриманих органами досудового розслідування внаслідок проведення СРД та НСРД, то вони різні:

– на етапі верифікації матеріалів: якщо йдеться про СРД, то предмет (документ) оглядається та описується безпосередньо слідчим у присутності понятих; водночас, якщо це стосується НСРД, то тільки експертна оцінка може підтвердити / спростувати факт втручання в цифровий матеріал;

– на етапі судового розгляду, коли йдеться про оцінку результатів СРД, то здійснюється допит понятих про те, що вони бачили під час СРД; коли ж йдеться про матеріали НСРД, то тут обійтися без допиту експерта / спеціаліста щодо технічної неможливості підробки цифрових даних неможливо.

До того ж для оцінки допустимості доказових відомостей, отриманих внаслідок НСРД, критичним є встановлення додержання вимог правила «ланцюга зберігання доказів» (chain of custody). Це пов’язано з тим, що результати проведення цих НСРД (аудіо-, відеофайли, дані з месенджерів) мають цифрову (нематеріальну) природу, що дає змогу легко змінити / модифікувати / видалити, оскільки цифрова інформація складається з «видимих проявлених» даних та «невидимих» метаданих. Тому оцінка допустимості має брати до уваги зв’язок «дані – метадані». Дані (data) – це безпосередньо зміст НСРД (аудіозапис, відео, інтернет-трафік). Метадані (metadata) – це так звані «дані про дані». Вони автоматично створюються технічним засобом (АПК, СТЗ) і містять: точний час і дату створення файла, технічні характеристики пристрою (серійний номер камери, версія прошивки), геопозицію (якщо є GPS-модуль), історію модифікацій і змін файла (якщо файл відкривали або редагували).

Забезпечення згадуваного вище «ланцюга зберігання доказів», нерозривність володіння (continuity of possession), експертна ідентифікація втручання / невтручання, а також використання хеш-суми як цифрового підпису «ланцюга зберігання доказів» у НСРД – це основа їх допустимості. Слідчий стандарт допустимості (проста наявність підпису в протоколі) тут не працює, бо підпис не

гарантує, що аудіофайл не був змонтований за допомогою штучного інтелекту чи звичайного редактора.

Зазначимо, що технології Deepfake та Generative AI (генеративного штучного інтелекту) – давно загальнодоступні, тому звичайний підпис (слідчого) на паперовому протоколі перестав вже бути повною гарантією автентичності.

Для прикладу наведемо перелік деяких редакторів на базі штучного інтелекту: AI Audio Synthesis, Voice Cloning – дають змогу клонування голосу; AI Noise Removal&Insertion, Adobe Audition, Audacity – дають змогу робити безшовну склейку (cross-fade), змінювати темп мовлення без зміни висоти голосу, вилучати частки «не» або змінювати контекст речення через перестановку слів тощо.

У науковому та експертному середовищі існує переконання, що справжній доказ допустимості цифрового файла в нашу епоху вже знаходиться в Log-файлах (журналах реєстрації подій) самого обладнання та у хеш-сумах. Якщо цифровий файл був «пропущений» через ШІ-редактор, то його внутрішня структура (метадані та бітовий потік) зміниться, а отже, хеш-сума оригінального цифрового файлу і хеш-сума диска з протоколом не будуть ідентичними. Тому через негласність процедури проведення НСРД сторона обвинувачення має через «ланцюг зберігання» (chain of custody) довести, що вона не зловживала своїми повноваженнями, формуючи доказові матеріали.

Отже, лише поєднання процесуального (хто, коли, куди передав) та технологічного ланцюга (хеш-суми, метадані, експертний висновок) дають змогу суду прийняти рішення про допустимість матеріалів НСРД у якості судового доказу.

Для визначення допустимості судових доказів, отриманих на основі НСРД, можуть також залучатися додаткові засоби перевірки. Так, оскільки ці слідчі дії є негласними, суд повинен переконатися у відсутності провокації, законності підстав та автентичності отриманих матеріалів. Для цього зазвичай використовують такі процедури:

1. Допит співробітника (оперативного підрозділу або слідчого).

Оскільки, згідно з ч. 1 ст. 256 КПК, протоколи щодо проведення негласних слідчих (розшукових) дій, аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі і документи або їх копії можуть використовуватися в доказуванні на тих самих підставах, що і результати проведення інших СРД під час досудового розслідування, суд має право допитати особу, яка складала протокол або проводила дію, для з’ясування: чи не було провокації (активної поведінки співробітників), які саме технічні засоби використовувалися (чи відповідають вони тим, що вказані в протоколі), дотримання часових меж (чи не здійснювався запис до або після терміну, визначеного ухвалою слідчого судді). Також співробітник може бути допитаний як свідок, проте з дотриманням заходів безпеки (зміна зо-

внішності, голосу або дистанційно), якщо це необхідно для збереження державної таємниці.

Хоча, на нашу думку, допит оперативного співробітника або слідчого – це доволі дискусійний (через зацікавленість та упередженість), але загальноприйнятий засіб перевірки «процесуальної чистоти» проведеної НСРД.

2. Перевірка належної процедури фіксації результатів НСРД (допит експерта в суді; консультації та роз'яснення спеціаліста).

Як уже зазначалося, ця перевірка має здійснюватися так, щоб завжди була можливість експертним шляхом встановити достовірність цих результатів, а протокол проведення НСРД повинен відповідати загальним правилам фіксації кримінального провадження. Особливо це стосується НСРД, під час яких здійснюється втручання у приватне спілкування (загальні положення про таке втручання викладені у ст. 258 КПК). Як уже зазначалося вище, це сфера переважно цифрових технологій, де без участі експерта (ст. 356 КПК) та спеціаліста (ст. 360 КПК) визначити допустимість отриманих доказових відомостей практично неможливо. Участь спеціаліста в дослідженні доказів під час судового розгляду не перешкоджає йому бути експертом у цьому кримінальному провадженні, якщо це дозволяє його кваліфікація, за винятком випадків, зазначених у ч. 2 ст. 79 КПК.

Тому в судовому засіданні спеціаліст надає роз'яснення щодо технічної автентичності: механізму копіювання інформації з СТЗ на матеріальний носій інформації (первинний носій); перевірки метаданих файлів (дата створення, геопозиція, зміни і т. ін.), що підтверджує неперервність «ланцюга зберігання доказів»; демонстрація того, що програмне забезпечення, використане для зняття інформації, виключає можливість стороннього втручання.

Показання та консультації спеціаліста в судовому засіданні допомагають підтвердити, що цифрові доказові відомості, представлені в суді, є автентичними. Експерт допитується для роз'яснення положень свого висновку. У контексті НСРД головна увага приділяється методології та категоричності.

У питанні методології (як саме ви це перевірили?) головна увага приділяється тому, чи відповідає спосіб експертного дослідження сучасному рівню розвитку техніки (в епоху штучного інтелекту). Експертні методики досліджень, звичайно, постійно оновлюються та перепрацьовуються, водночас іноді вони можуть бути безсилими проти сучасних методів фальсифікації та модифікації цифрових даних. Коли ставиться питання експерту про методологію, ставиться під сумнів не те, чи дотримався він кроків відповідної експертної методики, а те, чи є його загальний науковий підхід релевантним для виявлення сучасних цифрових маніпуляцій з потенційним цифровим доказом. Експерт має пояснити свій методологічний підхід: як, наприклад, результати аналізу файлової системи (метаданих) корелюють із результатами лінгвістичного аналізу.

У цьому контексті Вищий антикорупційний суд та Верховний Суд зараз активно запозичують міжнародну практику, згідно з якою оцінка експертизи йде за «критеріями Дауберта» (наукової обґрунтованості), коли суд оцінює саме наукову методологію: «Чи перевірялася теорія (falsifiability)? Чи проходила вона рецензування (peer review)? Який рівень похибки (error rate) в експертному висновку?».

Питання категоричності (наскільки ви впевнені?) стосується висновків щодо ідентифікації та втручання. Дуже часто у висновках експертів з комп'ютерно-технічних експертиз поряд з категоричними формулюваннями (не виявлено / виявлено, не визначено / визначено), застосовуються ймовірнісні формулювання (ймовірно).

Важливо зазначити, що експертиза цифрових носіїв та відомостей відповідає лише на запитання, які поставлені слідчим, а тому постановка правильних та однозначних запитань має бути максимально критичною.

Так, на думку В. Ю. Шепітька та Є. Є. Демидової, працівники правоохоронних органів не повною мірою використовують потенціал комп'ютерно-технічної експертизи у зв'язку з необізнаністю з наявністю широкого кола питань, які вона може допомогти з'ясувати, а використовуючи лише більш традиційні підходи до формулювання запитань. До того ж ініціатори проведення судових експертиз допускають також певні помилки, що ускладнюють або унеможливлюють її проведення [7, с. 179].

На практиці перевірка допустимості доказових відомостей, отриманих під час проведення НСРД за допомогою апаратно-програмних комплексів (АПК) та спеціальних технічних засобів (СТЗ) в умовах таємності, є найскладнішим етапом судового розгляду. Тут виникає конфлікт між дотриманням державної таємниці і правом обвинуваченого та сторони захисту на справедливий суд і захист.

На наш погляд, існує три основні фільтри перевірки допустимості доказових відомостей:

1) Процесуальний фільтр. Оскільки сторона захисту не може перевірити законність моменту фіксації доказових відомостей, суд має перевірити «паперовий» слід-фундамент НСРД – це перевірка легітимності «входу» в НСРД, перевірка відсутності «плодів отруйного дерева». Для цього процесуально передбачено:

– розсекречення процесуальних матеріалів-підстав для проведення НСРД (ст. 290 КПК);

– дотримання встановлених законом строків проведення НСРД;

– суб'єктність (ст. 246 КПК).

2) Зіставлення з іншими доказами, отриманими внаслідок проведення СРД в межах цього кримінального провадження. Це максимально важливо, оскільки

результати проведення НСРД мають бути лише непрямими доказами через відсутність можливості безпосереднього доступу та усвідомлення суддею під час їх оцінки (без посередництва техніки). Така процедура необхідна, оскільки матеріали НСРД не можуть існувати «у вакуумі», їх результати мають корелювати з результатами інших слідчих розшукових дій (гласних та негласних).

3) Можливість оскарження стороною захисту процедури (дотримання «ланцюга зберігання доказів» (chain of custody), пошук «плодів отруйного дерева») та змісту матеріалів досудового розслідування, які базуються на матеріалах НСРД (тест на провокацію: суд досліджує і має дослідити, хто був ініціатором розмови? чи був тиск? чи вчинив би підозрюваний злочин без втручання агента? і т. ін.; викривлення контексту: записи, трафіки та інші матеріали НСРД, які «вирвані» з контексту, можуть використовуватись стороною обвинувачення – мають бути в додатках до протоколу НСРД увесь об'єм напрацьованих матеріалів).

4) Залучення спеціаліста для перевірки «ланцюга збереження доказів».

Висновки. Вирішення питання допустимості протоколів НСРД з додатками у цифровій формі насампепред вимагає дотримання загальних правил, встановлених у кримінальному процесуальному законодавстві (ст. 86, 87, 89 КПК). Водночас така процесуальна діяльність передбачає застосування, крім юридичних засобів, спеціальних технічних знань у сфері інформаційних технологій, а саме:

1) обов'язкову перевірку їх цілісності (незмінності даних з моменту їх фіксації) і автентичності (достовірність походження даних) шляхом використання процедури хешування з метою можливого виявлення втручання і змін у ряді символів фіксованої довжини;

2) можливість допитів у судовому засіданні слідчих, оперативних працівників, які брали участь у проведенні НСРД, а також залучення спеціалістів і експертів для надання пояснень: а) щодо технічної автентичності: механізму копіювання інформації спеціальними технічними засобами на матеріальний носій інформації (первинний носій); б) перевірки, окрім даних, також метаданих файлів (дата створення, геопозиція, зміни і т. ін.), що підтверджують безперервність «ланцюга зберігання доказів»; в) демонстрації того, що програмне забезпечення, використане для зняття інформації, виключає можливість стороннього втручання.

Список використаних джерел

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. Редакція від 14.01.2021. URL: http://zakon5.rada.gov.ua/laws/show/4651-17 (дата звернення: 20.03.2026).
2. Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Інструкція затверджена спільним наказом Генеральної прокуратури України, МВС України, СБ України, Міністерством фінансів України, Адміністрацією ДПС України та Міністерством юстиції України від 16.11.2012

№ 114/1042/516/1199/936/1681/51. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення: 19.03.2026).
3. International Organization on Computer Evidence. URL: https://uia.org/s/or/en/1100029648 (дата звернення: 20.03.2026).
4. Борейко Г. Використання негласних слідчих (розшукових) дій та оперативно-розшукових заходів як засобів зловживання стороною обвинувачення під час їх проведення у кримінальному провадженні. *Право України*. 2023. № 2. С. 132–143. DOI: 10.33498/louu-2023-02-132.
5. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні: навчально-практичний посібник / С. С. Кудінов та ін. 2-ге вид. Харків: Оберіг, 2015, 424 с.
6. Авдєєв Г. К. Інноваційні методи та цифрові технології в криміналістиці і судовій експертизі: монографія / за заг. ред. В. Ю. Шепітька. Харків: Право, 2024. 208 с.
7. Шепітько В. Ю. Цифрова криміналістика та її роль у формуванні доказової інформації в умовах воєнних дій: монографія / за заг. ред. В. Ю. Шепітька. Харків: Право, 2025. 200 с.

Mykola Shumilo, Vitalii Kuznetsov, Oleksii Metelev. The admissibility of protocols of covert investigative (detective) activities with annexes containing information in digital form for the purposes of obtaining court evidence

This article examines the admissibility of protocols of covert investigative (search) operations with appendices containing information in digital form in the process of forming judicial evidence. It is argued that the specific nature of the legal regulation of covert investigative (search) operations, the procedure for their conduct and the methods of recording results significantly complicates the verification of the admissibility of the relevant information, particularly in cases involving the use of audio and video recordings, electronic data, computer storage media and other digital materials.

It has been shown that the admissibility of such evidence depends not only on compliance with the general requirements of criminal procedure law, but also on proper technical verification of its integrity and authenticity. The study analyses the legal basis for conducting digital forensics, the requirements for protocols and their annexes, as well as typical shortcomings in documentation that may call into question the admissibility of the evidence obtained. Particular attention is paid to the importance of the "chain of custody", the hashing procedure, metadata verification, and the ability to detect tampering, modification or other interference with digital files. It is emphasised that the admissibility of such materials must be determined in adversarial court proceedings, taking into account the defence's right to verify compliance with the procedural rules governing their acquisition.

The paper emphasises that the mere formal existence of an NSRD protocol and the digital media attached to it is not sufficient for the relevant information to be recognised as admissible evidence. It is argued that the assessment of such materials requires a combination of procedural and legal analysis with an examination of the technical characteristics of the digital information, which make it possible to establish its origin, integrity and the absence of external interference. It is concluded that the admissibility of NSRD protocols with digital attachments is determined by a combination of procedural and technological criteria. This requires verification of the legality of the grounds for conducting NSRD, compliance with the rules for recording and storing digital information, establishing its immutability and authenticity of origin, as well as the use of the specialist knowledge of experts and specialists in court proceedings. It has been demonstrated that only a comprehensive consideration of these requirements allows the information obtained as a result of NSD to be recognised as a valid evidential basis in criminal proceedings.

Keywords: *audio surveillance of individuals, video surveillance of individuals, authenticity of digital information, admissibility of evidence, annexes to the report, electronic data, criminal procedure law, chain of custody, covert investigative (detective) measures, report, data integrity, digital evidence.*

Дата першого надходження статті до видання: 27.04.2026 р.
Дата прийняття статті до друку після рецензування: 04.05.2026 р.