

ПРОБЛЕМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ

УДК 343.985:343.721

DOI <https://doi.org/10.32782/2709-9261-2025-4-16-2>

Головкін Сергій Вікторович,

кандидат юридичних наук, доцент,

доцент кафедри кримінального процесу та криміналістики

факультету підготовки фахівців для органів досудового розслідування

Національної поліції України

(Донецький державний університет внутрішніх справ, м. Кропивницький)

ORCID: <https://orcid.org/0000-0002-3204-2286>



ДЕЯКІ АСПЕКТИ ПРОВЕДЕННЯ НЕВЕРБАЛЬНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВ, УЧИНЕНИХ У КІБЕРПРОСТОРИ

У статті розглянуто окремі аспекти проведення невербальних слідчих (розшукових) дій під час розслідування шахрайств, учинених у кіберпросторі. Обґрунтовано значення правильного поєднання процесуальних і тактичних засад проведення слідчих (розшукових) дій для забезпечення ефективності доказування у кримінальних провадженнях цієї категорії. Особливу увагу приділено обшуку як ключовій невербальній слідчій (розшуковій) дії. Визначено об'єкти, що підлягають виявленню та вилученню. Наголошено на необхідності залучення спеціалістів у галузі комп'ютерної техніки та кібербезпеки, а також на дотриманні спеціальних правил поводження із цифровими доказами під час їх огляду, фіксації та вилучення.

Ключові слова: слідчі (розшукові) дії, тактика обшуку, кіберпростір, шахрайство, методика розслідування.

Постановка проблеми. Досудове розслідування шахрайств, учинених у кіберпросторі, являє собою складну розумову діяльність слідчого у взаємодії з оперативними підрозділами зі встановлення всіх обставин їх учинення, де головну роль відіграють різні заходи, насамперед слідчі (розшукові) дії, під час проведення яких відбуваються виявлення, фіксація та вилучення, а іноді й дослідження, оцінювання та використання доказів. Успішне закінчення досудового розслідування залежить від низки факторів, найважливішим з яких є правильне (з погляду кримінального процесуального закону) і ефективне (у тактичному сенсі) проведення слідчих (розшукових) дій. Під час проведення будь-якої слідчої (розшукової) дії необхідно розглядати її із двох сторін: процесуальної та тактичної, тільки таке поєднання дає позитивний результат. Забезпеченню науковості підготовки та проведення слідчих (розшукових) дій сприяє їх криміналістичний розподіл на вербальні і невербальні дії (залежно від форми отримання інформації та особливостей її джерела). До невербальних дій традиційно відносять слідчі (розшукові) дії, спрямовані на отримання доказів за допомогою дослідження матеріального середовища. Під час проведення таких слідчих (розшукових) дій мовний спосіб збирання інфор-

мації поступається місцем іншим методам і прийомам. До них належать різні види огляду, обшук, освідування. Загальні тактичні рекомендації проведення невербальних заходів полягають в організації підготовки та проведення слідчих (розшукових) дій, послідовності та повноти дослідження матеріальних об'єктів, технічному оснащенні, залученні до участі відповідних фахівців.

Аналіз останніх досліджень та публікацій. Проблематика розслідування шахрайств загалом і учинених у кіберпросторі зокрема, проведення слідчих (розшукових) дій досліджена у працях багатьох науковців, серед яких: Г.С. Бідняк, С.В. Головкін, І.О. Коваленко, О.В. Ковальчук, Т.В. Коршикова, М.М. Майстренко, І.І. Татарин, М.М. Єфімов, Н.В. Павлова, С.В. Самойлов, С.В. Чучко. Водночас окремі аспекти проведення невербальних слідчих (розшукових) дій під час розслідування шахрайств, учинених у кіберпросторі, розглянуті не досить системно та повно.

Метою статті є дослідження окремих аспектів проведення невербальних слідчих (розшукових) дій під час розслідування шахрайств, учинених у кіберпросторі.

Виклад основного матеріалу. Розслідування шахрайств, учинених у кіберпросторі, передбачає викори-

стання пошукових дій, які сприяють виявленню джерел доказової та орієнтуючої інформації. Відшукання прихованих об'єктів може бути здійснено під час проведення обшуку, процесуальний порядок проведення якого визначений ч. 3 ст. 208, ст. ст. 223, 234–236 Кримінального процесуального кодексу (далі – КПК) України.

Чинний КПК України під обшуком розуміє слідчу (розшукову) дію, яка проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте в результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб [1].

Відмінність обшуку від інших слідчих (розшукових) дій полягає насамперед у примусовому характері, який характеризується тим, що обшук може бути проведений без згоди особи, що обшукується, та відповідно передбачає створення напруги між слідчим і особами, в яких проводиться обшук. Під час проведення обшуку слідчий має право відкривати закриті приміщення і сховища, речі, якщо особа, присутня при обшуку, відмовляється їх відкрити або обшук здійснюється за відсутності осіб, зазначених у ч. 3 ст. 236 КПК України. Здійснювати ці й інші дії примусового характеру під час проведення обшуку слідчий може лише за наявності в нього вмотивованої ухвали слідчого судді про надання дозволу на обшук житла чи іншого володіння особи (ст. 30 Конституції України [2], ч. 2 ст. 234 КПК України).

Процес проведення обшуку, як і будь-якої іншої слідчої (розшукової) дії, передбачає такі етапи: 1) підготовку до проведення (підготовчий етап); 2) проведення слідчої (розшукової) дії (робочий етап); 3) фіксацію перебігу й результатів (завершальний етап). Надалі слідчий здійснює оцінювання отриманих під час проведення слідчої (розшукової) дії результатів і визначає їхню значущість та місце в системі доказової інформації [3, с. 212].

Практика досудового розслідування кримінальних правопорушень переконливо засвідчує, що результативність проведення обшуку зумовлюється рівнем підготовленості слідчого, коректним визначенням об'єктів і територій, які підлягають обстеженню, чіткою ідентифікацією предметів, що мають бути виявлені та вилучені, а також дотриманням вимог законності під час оформлення і фіксації результатів цієї слідчої (розшукової) дії

На підготовчому етапі обшуку слідчому доцільно здійснити такі організаційно-тактичні заходи:

1) встановити місцезнаходження, особливості планування приміщення, у якому планується проведення обшуку, з'ясувати систему охорони об'єкта, а також визначити можливі шляхи відходу осіб, причетних до вчинення кримінального правопорушення;

2) зібрати інформацію про наявні у приміщенні засоби зв'язку та комп'ютерну техніку, що дасть змогу окреслити межі місця обшуку та конкретизувати коло об'єктів, які підлягають пошуку;

3) залучити спеціалістів, які володіють необхідними знаннями, уміннями й практичними навичками для надання ефективної допомоги слідчому під час підготовки та безпосереднього проведення обшуку. Універсальними в цьому контексті є товаровознавці, криміналісти, мистецтвознавці, бухгалтери, а також фахівці у сфері цифрових засобів зв'язку та комп'ютерних технологій;

4) визначити дату, час і місце проведення обшуку, його орієнтовну тривалість, а також заходи, спрямовані на забезпечення оперативності та конфіденційності цієї слідчої дії. Оптимальною є ситуація відсутності підозрюваного в місці проведення обшуку, що мінімі-

зує можливість активної протидії та створює умови для швидкого виявлення і належного вилучення об'єктів пошуку. Водночас присутність родичів або близьких осіб підозрюваного може сприяти формуванню в них негативного ставлення до вчиненого злочину, що надалі може бути використано у визначенні тактики проведення інших слідчих (розшукових) дій, зокрема допитів свідків;

5) провести інструктаж осіб, залучених до участі в обшуку, із чітким визначенням індивідуальних завдань для кожної з них;

6) здійснити вивчення особи підозрюваного, приділивши особливу увагу рівню його злочинних навичок, умінь та можливих форм протидії слідству;

7) забезпечити участь понятих у порядку, передбаченому кримінальним процесуальним законодавством [4, с. 135–136].

Поділяємо наукову позицію Т.В. Коршикової, відповідно до якої організація та здійснення обшуку у кримінальних провадженнях щодо шахрайств, учинених із використанням електронно-обчислювальної техніки, мають суттєві відмінності порівняно із проведенням обшуку під час розслідування традиційних форм шахрайства. Такі особливості зумовлені, з одного боку, реальною загрозою умисного знищення інформації, що міститься в електронно-обчислювальній техніці, а також самої техніки як носія доказової інформації, а з іншого – ризиком її пошкодження внаслідок необережних або некваліфікованих дій слідчого чи інших членів слідчо-оперативної групи, що може призвести до втрати електронних слідів злочину [5, с. 140–141].

З огляду на це однією із ключових умов підготовчого етапу проведення обшуку безпосередньо за місцем імовірного вчинення шахрайства із застосуванням електронно-обчислювальної техніки є реалізація комплексу таких заходів:

1) одержання відомостей про об'єкти, що підлягають відшукуванню та вилученню, зокрема електронно-обчислювальну техніку (персональні комп'ютери, ноутбуки, сервери тощо), програмне забезпечення та носії інформації, а також про особу (осіб), підозрювану у скоєнні шахрайства, рівень її професійної підготовки у сфері використання комп'ютерної техніки, можливі способи подолання інформаційного захисту, знищення даних і приховування слідів злочину, а також види електронної інформації, що можуть мати доказове значення;

2) залучення спеціалістів, зокрема експертів комп'ютерно-технічних підрозділів Експертної служби МВС України або працівників підрозділів кіберполіції Національної поліції України;

3) забезпечення участі понятих, доцільним є залучення осіб, які мають базові знання у сфері комп'ютерних технологій;

4) підготовка технічних засобів і спеціальних пристроїв, призначених для коректного зчитування, копіювання та збереження інформації, вилученої з електронно-обчислювальної техніки;

5) проведення детального інструктажу членів слідчо-оперативної групи й інших учасників обшуку з акцентом на неухильне дотримання встановлених правил поведінки з комп'ютерною технікою та носіями інформації, а також на технічно грамотне здійснення пошуку електронних доказів і релевантної інформації [5, с. 140–141].

Склад слідчо-оперативної групи визначається метою обшуку та прогнозованими умовами його проведення. Окрім слідчого, понятих і працівників оперативних під-

розділів, до участі в обшуку можуть залучатися спеціаліст-криміналіст, перекладач, кінолог зі службовим собакою, а також інші особи, виконання функцій яких потребує спеціальних професійних знань і навичок. У разі вчинення активної протидії з боку осіб, які перебувають на об'єкті обшуку, необхідно застосовувати заходи, спрямовані на нейтралізацію такого опору та забезпечення швидкого і безпечного проникнення до приміщень, що підлягають обшуку.

Результати проведеного С.С. Вітвіцьким, О.О. Волобуєвою та А.О. Волобоєвим дослідження свідчать, що обшук (робоча стадія) починається з таких попередніх дій (заходів), як: непомітне прибуття СОГ (48,4%); попереднє обстеження прилеглої до об'єкта обшуку території (29,17%); виставлення постів (групи перехвату) (37,5%); супроводження представника громадськості чи житлово-експлуатаційної контори для оперативного проникнення на об'єкт обшуку (25%); додержання заходів безпеки (69,55%); застосування технічних засобів аудіо-, відеофіксування (68,9%); проникнення до об'єкта обшуку та його оперативне обстеження (з метою встановлення кількості присутніх і недопущення втечі, опору, знищення речових доказів тощо) (41,99%); пред'явлення службового посвідчення (47,12%); ознайомлення обшукуваного з ухвалою слідчого судді (83,65%); пропонування добровільно видати об'єкти пошуку (63,14%); обшук присутніх осіб (52,24%) [6, с. 174].

Як обґрунтовано зазначає Т.А. Абушов, проведення обшуку є складним комплексом організаційних і тактичних дій, спрямованих на реалізацію низки процесуальних завдань. До них належать: ознайомлення особи, у якої проводиться обшук, із процесуальними документами, що слугують правовою підставою для його здійснення; належне процесуальне оформлення залучення учасників обшуку, роз'яснення їм прав, обов'язків, мети та порядку проведення слідчої (розшукової) дії, повідомлення про використання технічних засобів, а також забезпечення можливості реалізації ними наданих процесуальних прав. Важливим завданням є створення умов для безперервного та якісного безпосереднього контакту учасників обшуку з об'єктами дослідження відповідно до попередньо визначеного розподілу функцій (об'єкт пошуку, власник приміщення, члени його сім'ї тощо), забезпечення інформаційної взаємодії між учасниками обшуку й об'єктами дослідження з використанням пізнавальних методів [7, с. 203].

Окрім того, у процесі обшуку відбувається здобуття нової матеріальної доказової та орієнтувальної інформації, встановлення її джерел, перевірка, уточнення і доповнення вже наявних у кримінальному провадженні відомостей, забезпечення збереження шуканих об'єктів від умисних дій осіб, зацікавлених у їх приховуванні, фальсифікації або знищенні. Обшук також спрямований на усунення суперечностей у матеріалах кримінального провадження, перевірку загальних і окремих криміналістичних версій, їх коригування, формування нових версій і отримання від учасників обшуку доказової та іншої інформації, що має значення для розслідування, з подальшою фіксацією перебігу та результатів слідчої дії.

Особливого значення набуває визначення кола об'єктів пошуку та місць їх можливого знаходження. Вихідні дані для цього містяться в матеріалах кримінального провадження. У справах про шахрайства, учинені в кіберпросторі, ці питання вирішуються, зокрема, на підставі показань потерпілого щодо предмета посягання та способу заволодіння ним. Під час проведення обшуку

в таких кримінальних провадженнях застосовуються загальні тактичні принципи криміналістики, зокрема раптовість, планомірність, послідовність і використання техніко-криміналістичних засобів. Водночас обшук у справах цієї категорії має низку специфічних рис, пов'язаних як із характером об'єкта пошуку, так і з місцем його можливого знаходження.

Обов'язковому виявленню та вилученню підлягають: предмети, що стали об'єктом злочинного посягання; засоби вчинення кримінального правопорушення; предмети, вилучені із цивільного обігу, які підлягають вилученню незалежно від мети конкретної слідчої (розшукової) дії. Аналіз судово-слідчої практики свідчить, що найчастіше обшуки проводяться за місцем проживання (юридичним або фактичним) підозрюваного – у 55% випадків, за місцем його роботи – у 17%, за місцем проживання родичів чи знайомих – у 20%, а також у господарських приміщеннях і транспортних засобах – у 8% випадків [4, с. 136–137].

Більшість обшуків у кримінальних провадженнях про шахрайства, учинені в кіберпросторі, припадає на обстеження приміщень. Обшуки ділянок місцевості зазвичай здійснюються в межах огляду будівель і прилеглих до них територій. Основним завданням обшуку на будь-якій стадії досудового розслідування є виявлення, фіксація та вилучення предметів і документів, що мають доказове значення.

Як слушно зауважує С.В. Чучко, під час розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу «Інтернет», у процесі обшуку необхідно виявляти та вилучати документи, що містять відомості про потенційних покупців; мобільні телефони з адресними книжками, SMS та іншою інформацією про осіб, причетних до злочину; комп'ютерну техніку та носії інформації, на яких можуть зберігатися дані про протиправну діяльність, з особливою увагою до вебресурсів, через які здійснювалося розміщення оголошень [8, с. 142].

У дослідженні об'єктів обшуку у справах про шахрайства з використанням електронно-обчислювальної техніки Т.В. Коршикова пропонує поділяти їх на дві основні групи: по-перше, об'єкти, що свідчать про використання електронно-обчислювальної техніки у вчиненні злочину (комп'ютери, периферійні пристрої, комунікаційні засоби, носії інформації, роздруковані програмні і текстові файли); по-друге, об'єкти, які вказують на причетність конкретної особи до злочинної діяльності, зокрема електронні записні книжки, технічна документація, сліди рук на техніці та носіях інформації, а також майно, здобуте злочинним шляхом [5, с. 143].

Вилучення та пакування комп'ютерної техніки здійснюються з дотриманням загальних правил поводження з речовими доказами, проте специфіка жорстких дисків потребує особливого підходу до їх огляду. Такий огляд має проводитися за безпосередньої участі спеціаліста у сфері комп'ютерних технологій з обов'язковим протоколюванням усіх його дій. Доцільним є залучення понять, які володіють хоча б мінімальними знаннями в галузі комп'ютерної техніки, а також, за можливості, підозрюваного чи осіб, що мали доступ до відповідної техніки. Виявлену криміналістично значущу інформацію необхідно роздруковувати та засвідчувати підписами учасників слідчої дії. Аналогічні вимоги застосовуються і до зовнішніх накопичувачів інформації.

Після завершення обшуку комп'ютерна техніка та носії інформації вилучаються для подальшого дослідження шляхом призначення судової комп'ютерно-технічної експертизи [4, с. 139–140].

Під час здійснення огляду електронно-обчислювальної техніки слідчий та залучений спеціаліст, які безпосередньо виконують дії з відповідними технічними засобами, зобов'язані дотримуватися визначених криміналістичних вимог, спрямованих на забезпечення належного виявлення та збереження речових доказів, зокрема слідів папілярних узорів і об'єктів біологічного походження. До характерних особливостей цього етапу варто віднести такі аспекти:

1) пошук слідів пальців рук доцільно здійснювати на елементах керування електронно-обчислювальною технікою, зокрема клавіатури, маніпуляторі типу «миша», пристроях змінних носіїв інформації, кнопках увімкнення та інших органах управління (кнопках, пристроях подачі паперу тощо), а також на мережевих кабелях, розетках і робочому місці (столі), де розміщено відповідну техніку, і безпосередньо на корпусах пристроїв, що входять до її складу. У разі посягання на інформацію, яка зберігається на змінних носіях, відбитки пальців рук можуть бути виявлені як на носіях, так і на їх технологічному пакуванні;

2) підлягають виявленню сліди, що виникають унаслідок підключення додаткової апаратури до електронно-обчислювальної техніки, її систем або мереж, за допомогою яких здійснювалося несанкціоноване копіювання інформації. До таких слідів належать відбитки пальців рук на корпусі системного блока, платах і пристроях, розміщених усередині нього, у разі внутрішнього підключення, а також на з'єднувальних елементах, за допомогою яких підключалася додаткова техніка;

3) велике значення має виявлення об'єктів біологічного походження (крові, сперми, букального епітелію, слини, піднігтьового вмісту, кісток, зубів, волосся із цибулиною), які надалі можуть мати доказове значення у кримінальному провадженні. Такі об'єкти можуть бути на електронно-обчислювальній техніці, периферійних пристроях (принтерах, сканерах, клавіатурах, маніпуляторах, багатофункціональних пристроях, блоках безперебійного живлення, накопичувачах пам'яті, маршрутизаторах тощо), робочому місці (столі, стільці, підлозі, килимку для миші, інших предметах, розміщених поблизу), а також на одязі.

У разі виявлення електронно-обчислювальної техніки, що працює, слідчий і фахівець мають виконати низку послідовних дій. Насамперед необхідно зафіксувати у протоколі обшуку місцезнаходження технічних засобів і периферійних пристроїв із детальним зазначенням їх найменування, серійних номерів, комплектації (типів і наявності дисків, мережевих карт, роз'ємів тощо), наявності підключення до локальної або телекомунікаційних мереж, а також технічного стану пристроїв (цілісність, наявність слідів розтину тощо). Далі треба встановити, яка саме програма виконується на момент початку обшуку; у разі виявлення програм, спрямованих на знищення інформації, необхідно негайно припинити їх роботу та розпочати огляд електронно-обчислювальної техніки саме із цього об'єкта. Після зупинки виконання програм здійснюється вхід до операційної системи з метою з'ясування останніх викликаних програм. Наступним кроком є встановлення наявності зовнішніх пристроїв зберігання інформації, зокрема жорстких дисків, а також засобів віддаленого доступу до системи (підключення до локальної мережі, наявність модема). За необхідності вживаються заходи для встановлення паролів доступу до захищених програмних продуктів. Після цього всі активні програми мають бути коректно закриті, з урахуванням того, що неправильне завершення

їхньої роботи може призвести до втрати інформації або пошкодження програмного забезпечення. За наявності відповідної потреби програми та файли, що мають значення для кримінального провадження, копіюються на знімний жорсткий диск, який перебуває в користуванні територіальних органів або підрозділів Національної поліції.

На завершальному етапі електронно-обчислювальної техніки необхідно від'єднати від мережі електроживлення та телекомунікаційних мереж, вимкнути модем, зафіксувати у протоколі обшуку порядок проведення слідчої (розшукової) дії, після чого технічні засоби опечатуються та вилучаються разом із магнітними носіями для подальшого дослідження в лабораторних умовах. Додаткові периферійні пристрої доцільно вилучати лише тоді, коли ними безпосередньо користувалися підозрювані або коли у слідства виникають обґрунтовані сумніви щодо їхнього технічного стану та працездатності [9, с. 20–21].

Перебіг і результати проведення слідчої (розшукової) дії значною мірою зумовлюються слідчою ситуацією, що склалася під час здійснення обшуку. У науковій літературі такі ситуації традиційно поділяють на конфліктні та безконфліктні. За наявності ознак безконфліктної ситуації обшук може фактично набути форми тимчасового вилучення майна, коли особа, у якої він проводиться, добровільно передає об'єкти, що становлять інтерес для слідства. Водночас така демонстративна готовність до співпраці не завжди є свідченням добросовісної поведінки, оскільки може приховувати факти підміни предметів, неповної їх видачі або прагнення замаскувати більш значущі докази, зокрема й пов'язані з іншими епізодами злочинної діяльності.

Найчастіше слідчий стикається з конфліктними слідчими ситуаціями, що об'єктивно зумовлює необхідність застосування спеціальних тактичних прийомів і рекомендацій, орієнтованих на подолання протидії. У разі прогнозування або наявності такої ситуації доцільним є завчасне встановлення спостереження за об'єктом обшуку (за декілька годин до прибуття слідчого), що може сприяти виявленню та фіксації умовних сигналів, призначених для оповіщення співучасників про проведення слідчої дії. Якщо ж учасникам обшуку під різними приводами перешкоджають у доступі до приміщення, де він має проводитися, з метою запобігання знищенню або приховуванню предметів і документів, які підлягають відшукуванню, допускається застосування рішучих заходів, зокрема примусового проникнення до об'єкта обшуку через двері, вікна, горищні приміщення тощо [4, с. 148].

Завершальним та водночас надзвичайно важливим етапом обшуку є огляд вилучених об'єктів, фіксація їхніх індивідуальних характеристик і обставин виявлення. Протокол обшуку має містити вичерпний перелік вилучених предметів і документів із зазначенням їхніх загальних і окремих ознак і властивостей, наявних пошкоджень, особливих прикмет, індивідуальних номерів, кольору, форми, маси, розмірів, кількості, способу пакування та інших істотних характеристик. Усі вилучені об'єкти підлягають належному пакуванню та опечатуванню, що засвідчується підписами понятих та інших учасників слідчої (розшукової) дії.

Висновки. У підсумку доцільно зазначити, що визначальною роллю у формуванні доказової бази відіграють невербальні слідчі (розшукові) дії, насамперед обшук, який забезпечує виявлення, фіксацію та вилучення електронно-обчислювальної техніки, носіїв цифрової інформації та інших матеріальних об'єктів, що мають кримі-

налістичне значення. Ефективність проведення таких дій значною мірою залежить від належної підготовки слідчого, правильного визначення об'єктів і меж пошуку, своєчасного залучення спеціалістів у галузі комп'ютерної техніки та кібербезпеки, а також від дотримання вимог кримінального процесуального законодавства та криміналістичних рекомендацій. Специфіка цифрових доказів зумовлює необхідність застосування спеціаль-

них тактичних прийомів, спрямованих на запобігання знищенню або зміні електронної інформації та забезпечення її цілісності й допустимості у кримінальному провадженні. Урахування слідчої ситуації та можливих форм протидії під час проведення обшуку сприяє підвищенню результативності досудового розслідування та повноті встановлення обставин кримінального правопорушення.

Список використаних джерел

1. Кримінальний процесуальний Кодекс України від 13.04.2012 р. № 4651–VI. URL: <http://zakon3.rada.gov.ua/laws/show/4651-17> (дата звернення: 25.11.2025).
2. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 25.11.2025).
3. Слідчі (розшукові) дії : навчальний посібник / О. В. Авраменко та ін. ; за заг. ред. Р. І. Благуті, Є. В. Пряхіна. Львів : ЛьвДУВС, 2013. 416 с.
4. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. ... канд. юрид. наук. Харків, 2008. 216 с.
5. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. ... докт. філософ. Київ, 2021. 255 с.
6. Вітвіцький С. С., Волобуєва О. О., Волобоев А. О. Методика розслідування незаконного поводження зі зброєю та бойовими припасами : монографія. Київ : ВД «Дакор», 2021. 308 с.
7. Абушов Т. А. Система організаційних і тактичних дій під час проведення обшуку. *Науковий вісник Національної академії внутрішніх справ*. 2011. № 6. С. 198–205.
8. Чучко С. В. Розслідування шахрайств при купівлі-продажу товарів через мережу «Інтернет» : дис. ... докт. філософ. Дніпро, 2021. 276 с.
9. Доказування у справах про злочини, учинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки : методичні рекомендації. НАВС, 2020. 60 с.

References

1. Kryminalnyi protsesualnyi kodeks Ukrainy vid 13.04.2012 r. № 4651–VI [Criminal Procedure Code of Ukraine dated 13.04.2012 № 4651–VI] (2012). Retrieved from <http://zakon3.rada.gov.ua/laws/show/4651-17> (data zvernennia: 25.11.2025) [in Ukrainian].
2. Konstytutsiia Ukrainy vid 28.06.1996 r. № 254k/96-VR [Constitution of Ukraine dated 28.06.1996 № 254k/96-VR]. (1996). Retrieved from <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (data zvernennia: 25.11.2025). [in Ukrainian].
3. Slidchi (rozshukovi) dii: navchalnyi posibnyk [Investigative (detective) actions: a training manual] / O. V. Avramenko, R. I. Blahuta, Yu. V. Hutsuliak ta in.; za zah. red. R. I. Blahuty ta Ye. V. Priakhina (2013). Lviv: LvDUVS [in Ukrainian].
4. Holovkin, S. V. (2008). Kryminalistychna kharakterystyka shakhraistva vidnosno vlasnosti osoby ta yii vykorystannia na pochatkovomu etapi rozsliduvannia [Forensic characterization of fraud regarding a person's property and its use at the initial stage of the investigation]: dys. ... kand. yuryd. nauk. Kharkiv [in Ukrainian].
5. Korshykova, T. V. (2021). Rozsliduvannia shakhraistv, uchynenykh z vykorystanniam elektronno-obchysliuvalnoi tekhniky [Investigation of fraud committed using electronic computing technology]: dys. doktor filosofii. Kyiv [in Ukrainian].
6. Vitvitskyi, S. S., Volobuieva, O. O., & Voloboiev, A. O. (2021). Metodyka rozsliduvannia nezakonnoho povodzhennia zi zbroieiu ta boiovymy prypasamy [Methodology for investigating illegal handling of weapons and ammunition]: monohrafiia. Kyiv: VD “Dakor” [in Ukrainian].
7. Abushov, T. A. (2011). Systema orhanizatsiinykh i taktychnykh dii pid chas provedennia obshuku [System of organizational and tactical actions during a search]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav*, 6, 198–205 [in Ukrainian].
8. Chuchko, S. V. (2021). Rozsliduvannia shakhraistv pry kupivli-prodazhu tovariv cherez merezhu Internet [Investigation of fraud in the purchase and sale of goods via the Internet]: dys. ... doktor filosofii. Dnipro [in Ukrainian].
9. Dokazuvannia u spravakh pro zlochyyny, vchyneni shliakhom nezakonnykh operatsii z vykorystanniam elektronno-obchysliuvalnoi tekhniky: metodychni rekomendatsii [Evidence in cases of crimes committed through illegal operations using electronic computing equipment: methodological recommendations]. (2020). NAVS [in Ukrainian].

Holovkin Serhii,

Candidate of Law, Associate Professor,

Associate Professor at the Department of Criminal Procedure and Criminalistics, Faculty of Training Specialists
for Pre-Trial Investigation Bodies
of the National Police of Ukraine

(Donetsk State University of Internal Affairs, Kropyvnytskyi)

ORCID: <https://orcid.org/0000-0002-3204-2286>

**SOME ASPECTS OF CONDUCTING NON-VERBAL INVESTIGATIVE (SEARCH) ACTIONS
DURING THE INVESTIGATION OF FRAUD COMMITTED IN CYBERSPACE**

The article examines certain aspects of conducting non-verbal investigative (search) actions during the pre-trial investigation of fraud committed in cyberspace. The importance of the correct combination of procedural and tactical principles of conducting investigative (search) actions to ensure the effectiveness of evidence in criminal proceedings of this category is substantiated. Particular attention is paid to the search as a key non-verbal investigative (search) action, its coercive nature, stages of conduct and general tactical recommendations are revealed.

The specifics of the preparation, organization and conduct of a search in criminal proceedings on cyber fraud are analyzed, taking into account the risk of destruction or loss of electronic information. The range of objects subject to detection and seizure is determined, in particular electronic computing equipment, digital information carriers, means of communication and other material traces of criminal activity. The need to involve specialists in the field of computer technology and cybersecurity is emphasized, as well as compliance with special rules for handling digital evidence during its examination, fixation and removal.

It is concluded that taking into account the forensic features of conducting non-verbal investigative (search) actions, primarily searches, contributes to increasing the efficiency of investigating fraud committed in cyberspace and ensures the proper formation of the evidence base.

Key words: *investigative (search) actions, search tactics, cyberspace, fraud, investigation methodology.*

Надіслано до редколегії 28.11.2025
Рекомендовано до публікації 23.12.2025
Опубліковано 29.12.2025