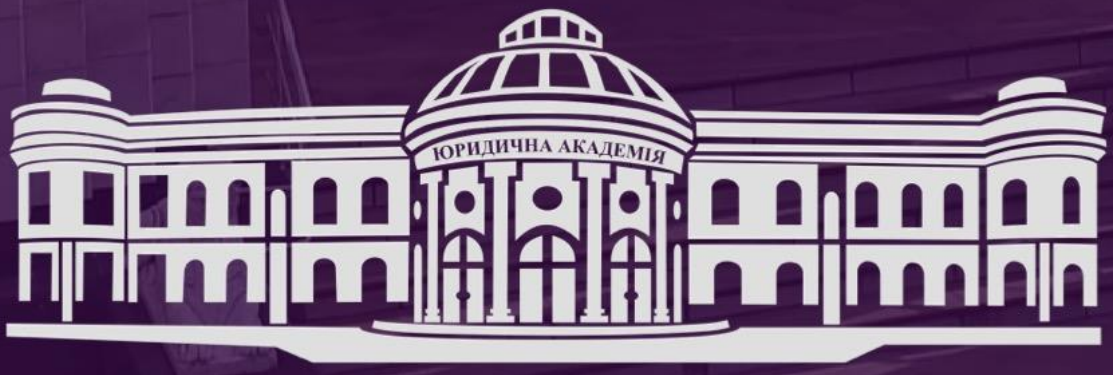
Національний університет «Одеська юридична академія»
Факультет прокуратури та слідства (кримінальної юстиції)
Кафедра криміналістики, судових експертиз та поліграфології

Національний центр судових експертиз при
Міністерстві юстиції Республіки Молдова
Одеський науково-дослідний інститут судових
експертиз Міністерства юстиції України

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ЕКСПЕРТНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: МІЖНАРОДНИЙ ДОСВІД ТА НАЦІОНАЛЬНА ПРАКТИКА»

27 листопада 2025 року, місто Одеса



EXPERT SUPPORT IN THE INVESTIGATION OF ORGANIZED CRIME: INTERNATIONAL EXPERIENCE AND NATIONAL PRACTICE

Proceedings of the International Scientific and Practical Conference

27 November 2025

Odesa
2025

УДК 340.6:343.9.022 (062)

Рекомендовано до друку рішенням кафедри криміналістики, судових експертиз та поліграфології НУ«ОЮА» (протокол № 9 від 24 листопада 2025 року)
Рекомендовано до друку рішенням Вченої ради ОНДІСЕ (протокол №9 від 1 грудня 2025 року)

Експертне забезпечення розслідування організованої злочинності: міжнародний досвід та національна практика: збірник матеріалів міжнар. наук.-практ. конф. м. Одеса, 27 листоп. 2025 р. / [орг. комітет: С. Ківалов, М. Аракелян, О. Катарага, Д. Кішко, Д. Колодін, А. Колодіна, Л. Аркуша та ін.]; Нац. ун-т Одеськ. юрид. акад. кафедра криміналістики, суд. експертиз та поліграф.; Нац. центр суд. експерт. при Міністер. юстиц. Респуб. Молдова; Одеськ. Наук.-дослідн. ін-т суд. експер. Міністер. юстиції України. Одеса: НУ «ОЮА», 2025. 450 с.

У збірнику викладено матеріали Міжнародної науково-практичної конференції «Експертне забезпечення розслідування організованої злочинності: міжнародний досвід та національна практика», в якій взяло участь понад 100 науковців і практиків з України та інших держав Європи. Представлено актуальні дослідження обговорень таких наукових і практичних проблем, як: експертне забезпечення протидії окремим видам організованої злочинності; використання спеціальних знань та експертне забезпечення розслідування організованої злочинності в умовах збройного конфлікту; міжнародна співпраця у сфері експертного забезпечення протидії організованій злочинності: досвід та практика; інформаційне забезпечення правоохоронних органів у боротьбі з організованою злочинною діяльністю; інноваційні технології та сучасні методи розслідування у протидії організованій злочинності; кримінально-правові, кримінально-процесуальні та кримінологічні проблеми забезпечення протидії організованій злочинності.

Висловлюємо вдячність усім авторам за активну участь, якісний науковий матеріал та високий рівень академічної доброчесності.

Матеріали викладені в авторській редакції.

Відповідальність за зміст, наукову новизну, коректність цитування та достовірність фактичного матеріалу несуть автори.

UDC 340.6:343.9.022 (062)

Recommended for publication by the decision of the Department of Criminalistics, Forensic Examinations and Polygraphology NU «OLA» (Pr. 9, November 24, 2025)
Recommended for publication by the decision of the Academic Council of ONDISE (Pr. 9, December 1, 2025)

Expert Support in the Investigation of Organized Crime: International Experience and National Practice: Proceedings of the International Scientific and Practical Conference (Odesa, 27 November 2025) / [Organizing Committee: S. Kivalov, M. Arakelyan, O. Cataraga, D. Kishko, D. Kolodin, A. Kolodina, L. Arkusha et al.]; National University «Odesa Law Academy», Department of Criminalistics, Forensic Examinations and Polygraphology; National Centre of Judicial Expertise of the Ministry of Justice of the Republic of Moldova; Odesa Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine. Odesa:NU«OLA», 2025. 450 p.

The Proceedings contain papers presented at the International Scientific and Practical Conference «Expert Support in the Investigation of Organized Crime: International Experience and National Practice», which brought together over 100 scholars and practitioners from Ukraine and other European countries. The materials address urgent scientific and practical issues, such as expert support for combating specific types of organized crime; the use of specialized knowledge and expert support for investigating organized crime during armed conflict; international cooperation in forensic support for combating organized crime; information support for law enforcement in countering organized criminal activity; innovative technologies and modern investigative methods; and criminal law, criminal procedure, and criminological issues in ensuring effective counteraction to organized crime.

We express our sincere gratitude to all authors for their active participation, high-quality academic contributions, and strong adherence to academic integrity.

The materials are published in the authors' original versions.

Authors bear responsibility for the content, scientific novelty, accuracy of citations, and reliability of factual information.

Колодін Денис
доктор юридичних наук, професор,
декан факультету прокуратури та слідства (кримінальної юстиції)
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000-0001-6368-0849
електронна адреса: kolodinodessa@gmail.com

Колодіна Анна
кандидат юридичних наук, доцент
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000-0002-7097-0155
електронна адреса: padey_anya@ukr.net

ВИДИ ТА НАПРЯМИ ІДЕНТИФІКАЦІЙНИХ ДОСЛІДЖЕНЬ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВ, ВЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ ТЕЛЕКОМУНІКАЦІЙНИХ ЗАСОБІВ

Проаналізовані основні особливості, види та напрями ідентифікаційних досліджень під час розслідування шахрайств, вчинених із використанням телекомунікаційних засобів.

Ключові слова: спеціальні знання, call-центр, телекомунікаційні засоби, розслідування, експертне забезпечення, комп'ютерно-технічна експертиза, організована злочинна діяльність.

Kolodin Denis
Doctor of Law, Professor,
Head of the Faculty of Prosecution and Investigation (Criminal Justice),
National University «Odesa Law Academy», Odesa, Ukraine

Kolodina Anna
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminalistics, Forensic Examinations and Polygraphology,
National University «Odesa Law Academy», Odesa, Ukraine

TYPES AND DIRECTIONS OF IDENTIFICATION RESEARCH DURING THE INVESTIGATION OF FRAUD COMMITTED USING TELECOMMUNICATIONS MEANS

The main features, types and directions of identification research during the investigation of fraud committed using telecommunications means are analyzed.

Keywords: special knowledge, call - center, telecommunications, investigation, expert support, computer technical expertise, organized crime

Стрімкий розвиток інформатизації та діджиталізації в суспільстві вплинули на всі сфери життєдіяльності. Дане явище безумовно має свої переваги та недоліки. Дійсно, з застосуванням цифровізації можна відмітити підвищення ефективності та швидкості процесів роботи у важливих інституціях нашої держави; оптимізація управлінських рішень; прозорість і контроль; доступність послуг та інформації; підвищення безпеки; розширення інноваційних можливостей; покращення комунікацій та ін. Але, якщо говорити про недоліки, то саме швидкий розвиток цифровізації зумовив зростання великої кількості злочинних проявів, а саме: розширення можливостей для здійснення кіберзлочинів; збільшення масштабу та швидкості шахрайства; анонімність та ускладнення ідентифікації злочинців; труднощі верифікації інформації; висока латентність шахрайських злочинів; залежність суспільства від цифрових сервісів; можливість створення транснаціональних платформ; ускладнення збирання та збереження цифрових доказів.

Тому, цифровізація, попри значний позитивний потенціал, одночасно створює сприятливі негативні умови для розвитку шахрайських схем, а злочинні технології з кожним роком набувають все більш організованого, транснаціонального характеру та становлять загрозу як для економіки так і для національної безпеки держави. Безумовно, що під час розслідування таких злочинів, вагоме місце займають суб'єкти та інституції, які забезпечують використання спеціальних знань під час виявлення, документування та досудового розслідування кримінальних правопорушень. Все це вимагає від правоохоронних органів нових підходів до криміналістичного, експертного забезпечення розслідувань даної категорії справ та удосконалення міжнародної взаємодії та системної цифрової освіти населення, що і обумовлює актуальність та своєчасність вибору наукового дослідження.

Надзвичайно важливим є врахування положень Розділу XVI Кримінального кодексу України, який встановлює кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж, а також мереж електрозв'язку. Норми цього розділу мають пряму криміналістичну релевантність , оскільки більшість сучасних шахрайських схем та злочинних технологій (зокрема , діяльність call-центрів, фішингові операції, використання IP-телефонії чи месенджерів) базуються на неправомірному доступі, втручанні чи використанні інформаційних технологій, передбачених статтями 361-363-1 КК України [4, с.187]

Дослідивши тенденцію та статистичні дані, можна констатувати за інформацією наданою Офісом Генерального прокурора, за останні два роки ситуація з шахрайськими call-центрами стала масштабним транснаціональним

явищем, де Україна фігурує як країна – жертва і як територія діяльності частини таких структур. Кількість випадків шахрайств та онлайн-правопорушень в Україні утричі зросла порівняно з 2022 роком, що пов'язано, зокрема, з діяльністю орієнтовно 1500 шахрайських call-центрів на території країни.

Упродовж 2023-2025 рр. домінують декілька великих блоків - схем, які масово реалізуються через call-центри, а саме:

1. Псевдоінвестиційні та криптоінвестиційні схеми зазвичай діють в двох напрямах: *по-перше, «*брокерські*»* call-центри телефонують громадянам ЄС, Великої Британії, Канади, Казахстану, тощо, пропонуючи «високоприбуткові інвестиції» у валюту, акції, криптовалюту, CFD тощо; *по-друге,* жертв кібершахрайств «супроводжують» довгий час, демонструючи їм фейкові кабінети, підроблену «прибутковість», а на етапі виведення коштів вимагають сплату комісії, податків та страхових внесків;
2. Busines email compromise / call-центри, які розповсюджують бізнес - шахрайства за допомогою використання дзвінків разом із фішинговими листами, де шахраї телефонують від імені банку, постачальника, державного органу, підтверджуючи фейкові рахунки, реквізити, тощо. За дослідницькими даними за 2023-2024 рр. було зареєстровано понад 9200 бізнес-шахрайств такого типу.
3. «Техпідтримка» (Microsoft/Norton, антивірус, оптимізація роботи комп'ютера), класична модель здійснення шахрайської схеми, в якій фіктивний call-центр представляється міжнародною IT – компанією, отримує за допомогою шкідливого ПЗ віддалений доступ до комп'ютера (AnyDesk, TeamViewer), далі безпосередньо незаконно отримує кошти, або змушує сплатити «за послуги чи захист комп'ютера.

Як свідчить статистика надана Офісом Генерального прокурора, станом на 07.11.2025 р. прокурори викрили та припинили діяльність мережі з 14 шахрайських call-центрів, які працювали зокрема в Запорізькій, Рівненській, Черкаській областях та місті Києві. Незаконний бізнес маскували під псевдоброкерський сервіс та фіктивні інвестиційні платформи. Оператори телефонували людям, представлялися нібито співробітниками міжнародних фінансових компаній. Вони переконували громадян вкладати кошти у «високоприбуткові інвестиції» та обіцяли швидкий і гарантований заробіток. Насправді кошти потерпілих одразу переводилися на рахунки організаторів. Серед потерпілих: громадяни України, країн Європи та Азії [2]. Серед слідчих розшукових дій проведено десятки обшуків, під час яких вилучено: понад 800 одиниць комп'ютерної техніки; майже 500 мобільних телефонів; серверне обладнання, яке забезпечувало функціонування «служб підтримки» та платіжних шлюзів; чорнові записи з даними потерпілих та алгоритмами спілкування з ними; іншу документацію та речові докази, що мають доказове значення. Наразі встановлюються організатори мережі, а також особи, причетні до її фінансування та технічного забезпечення. Офіс Генерального прокурора продовжує комплексні

заходи з виявлення, документування та ліквідації шахрайських call-центрів, які масово діють на території України, та видурюють у громадян їхні кошти.

Виходячи з предмету нашого дослідження, хотілось би звернути увагу та підкреслити важливе значення видів та напрямів ідентифікаційних досліджень під час розслідування шахрайств, вчинених із використанням телекомунікаційних засобів.

Слушно звернутись до понятійно-категоріального апарату і зазначити, що у процесі розслідування кримінальних правопорушень досить часто необхідно ідентифікувати об'єкт (встановити, виявити його тотожність) і для цього потрібна *криміналістична ідентифікація* – це процес установлення тотожності об'єктів шляхом проведення порівняльного дослідження їх загальних та окремих ознак, які мають значення для розкриття і розслідування кримінальних правопорушень та судового розгляду [1, с. 62]. У теорії і практиці криміналістики якщо говорити про види криміналістичної ідентифікації *за суб'єктами здійснення дослідження,* її можуть здійснювати експерт, слідчий, суддя, спеціаліст, тому її можна поділити за суб'єктом здійсненя на: оперативну; слідчу; експертну; судову.

Під час розслідування шахрайств з використанням телекомунікаційних засобів проводять ідентифікаційні дослідження цифрових доказів, таких як: аналіз даних електронних листів, повідомлень у месенджерах та історії браузера, а також встановлення особистості за IP-адресою, телефонним номером та іншою інформацією, яка має доказове значення.

До найбільш поширених і доказово значущих видів ідентифікаційних досліджень в зазначеній категорії справ можна виділити наступні:

1. Ідентифікація особи, яка здійснює комунікацію.

- *Ідентифікація за даними облікових записів,* що полягає в дослідженні електронних листів, повідомлень у месенджерах та соціальних мережах для виявлення підозрілої активності, перевірки відправників та вмісту повідомлень; зв'язок шахрая з акаунтами в месенджерах (Telegram, WhatApp, Viber).
- *Аналіз вихідних файлів* (наприклад, вкладених файлів), які можуть містити шкідливе програмне забезпечення або бути частиною шахрайської схеми;
- *Ідентифікація абонента (особистості) за телекомунікаційними даними,* що передбачає: визначення IP-адреси, з якої надходили повідомлення або здійснювалися дії, для ідентифікації пристрою та мережі, що використовувалися шахраєм; використання інформації про телефонні номери для встановлення власника SIM-карти та перевірки історії дзвінків, якщо це можливо відповідно до законодавства, прив'язка SIM- карти до конкретного пристрою, дослідження маршрутів з'єднань, місцезнаходження.
- *Голосова (фонетична) ідентифікація,* полягає в порівняльному аналізі (ототожненні) голосу операторів шахрайських call-центрів; встановлення індивідуальних ознак мовлення; визначення статі, віку, психологічного стану (за наявності достатнього акустичного матеріалу).

2. Ідентифікація пристроїв, засобів зв'язку та технічної інфраструктуру (ЕОМ).

-*Ідентифікація мобільного або стаціонарного пристрою,* здійснюється за допомогою техніко-комп'ютерної експертизи смартфонів та VoIP-телефонів; відновленні видалених контактів, журналів дзвінків, чатів; визначення часу та способу використання пристрою. Підставою проведення експертизи є відповідне судове рішення чи рішення органу досудового розслідування, або договір з експертом чи експертною установою - якщо експертиза проводиться на замовлення інших осіб [3].

- *Ідентифікація мережевих слідів,* передбачає встановлення IP-адрес, маршрутів передавання даних; визначення використання VPN, проксі-серверів, TOR; ідентифікацію серверів, на яких розміщено шахрайський сайт чи CRM call-центру.

- *Ідентифікація обладнання call-центру,* полягає у детальному аналізі SIP-телефонії, VoIP-шлюзів, call-tracking систем; визначенні конфігурації серверів, розподілу ролей операторів та прив'язці конкретних пристроїв до зловмисників.

3. Ідентифікація цифрових слідів і даних у кіберпросторі.

- *OCINT-ідентифікація,* передбачає встановлення співробітників шахрайського call-центру через соцмережі; аналіз цифрових профілів, фотографій, місць роботи, контактів; виявлення пов'язаних компаній-оболонок, доменів, IP-кластерів.

- *Ідентифікація за логами,* полягає у аналізі логів месенджерів, серверів, платіжних платформ; встановленні часу, послідовності та характеру дій шахраїв; визначенні, чи здійснювалася масова розсилка, чи адресна атака.

- *Ідентифікація транзакцій,* здійснюється через цифрову ідентифікацію шляхів переказу коштів; зв'язок між банківськими картками, електронними гаманцями, криптогаманцями; встановлення кінцевого вигодоодержувача (beneficial owner) через аналіз блокчейну.

4. Ідентифікація джерел інформації та каналів поширення шахрайських схем.

- *Ідентифікація фейкових сайтів і платформ* поляє *у* дослідженні доменного реєстру, SSL-сертифікатів, хостингу; визначенні зв'язку між різними шахрайськими сайтами, "дзеркалами", підмінними адресами.

- *Ідентифікація контенту,* передбачає аналіз шаблонів листів, SMS, скриптів дзвінків; встановлення, чи належить контент одній злочинній групі; ознаки автоматизованого створення повідомлень (AI-генерація).

- *Ідентифікація групового впливу (criminological cluster analysis),* полягає у визначенні зв'язків між кількома кол-центрами; ідентифікації «мережевих суперструктур» — операторів, бухгалтерів, рекрутерів, маркетологів, дропів.

5. Ідентифікація поведінкових характеристик злочинця.

- *Поведінкове профілювання,* обумовлене аналізом повторюваних патернів дзвінків, часових інтервалів, поведінки в чатах; визначенням індивідуальних моделей шахрайської діяльності.

- *Ідентифікація соціально-психологічних ознак,* передбачає характеристику стилю комунікації; виявлення ознак маніпуляції, емоційного тиску, професійної підготовки оператора.

Підсумовуючи викладене, варто відмітити, що ідентифікаційні дослідження при розслідуванні шахрайств вчинених із використанням телекомунікаційних засобів, охоплюють комплекс технічних, цифрових, мовленнєвих та криміналістичних методів, спрямованих на встановлення особи злочинця, технічної інфраструктури, цифрових слідів та зв'язків між окремими епізодами (періодами шахрайських дій). Така широка модель ідентифікації дозволяє ефективно протидіяти високій латентності та транснаціональному характеру таких злочинів, забезпечуючи належну доказову базу для притягнення винних до відповідальності.

Перелік використаних джерел:

1. Криміналістика: підручник / [В.М. Шевчук, В.А. Журавель, В.Ю. Шепітько та ін.]за ред. В.М. Шевчука; Нац. Юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2024. 1008 с.
2. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора:* сайт. URL: https://gp.gov.ua/ua/posts/prokurori-pripinili-diyalnist-14-kol-centriv-cerez-yaki-vimanyuvali-grosi-v-gromadyan-ukrayini-krayin-jes-ta-aziyi
3. Про судову експертизу: Закон України від 01.01.2025р. № 28. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.
4. Кримінальний кодекс України: чинне законодавство із змінами та допов. на 01 липня 2024 року. Офіц. Текст. Київ: Алерта, 2024. 248 с.