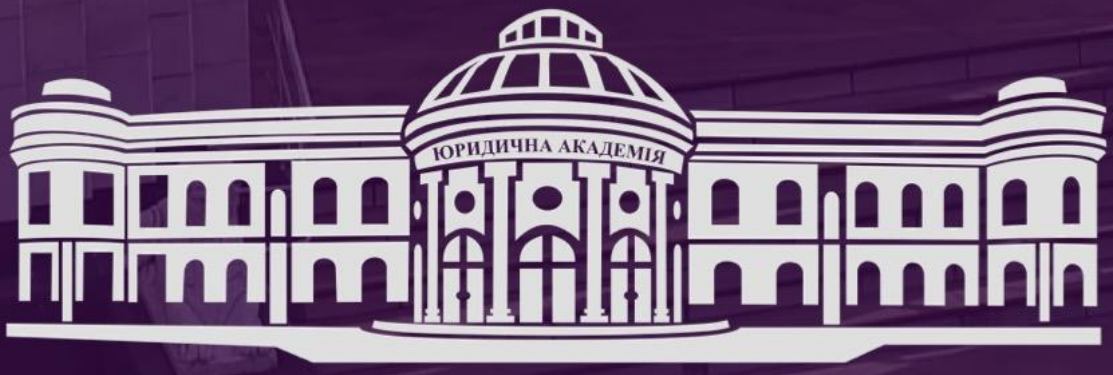
Національний університет «Одеська юридична академія»
Факультет прокуратури та слідства (кримінальної юстиції)
Кафедра криміналістики, судових експертиз та поліграфології

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.

Ващук Олеся
доктор юридичних наук, професор,
дослідник Гданського університету,
м. Гданськ, Республіка Польща
ORCID: https://orcid.org/0000-0003-3161-2870
електронна адреса: earth.olesia@gmail.com

АЛГОРИТМ ФІКСАЦІЇ ТА ЕКСПЕРТНОГО АНАЛІЗУ ЦИФРОВИХ КОМУНІКАЦІЙ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ ГРУП У МЕСЕНДЖЕРАХ TELEGRAM, WHATSAPP І SIGNAL

У тезах запропоновано покроковий алгоритм фіксації, зберігання та експертного аналізу цифрових комунікацій організованих злочинних груп у месенджерах Telegram, WhatsApp і Signal. Розглянуто типові помилки та надано практичні рекомендації для слідчих і судових експертів.

Ключові слова: цифрові докази, месенджери, Telegram, WhatsApp, Signal, експертний аналіз, організована злочинність.

Vashchuk Olesia
Doctor of Law, Professor,
researcher at the University of Gdansk, Gdansk, Republic of Poland, Odesa, Ukraine

ALGORITHM FOR RECORDING AND FORENSIC ANALYSIS OF DIGITAL COMMUNICATIONS OF ORGANIZED CRIMINAL GROUPS IN TELEGRAM, WHATSAPP AND SIGNAL

The paper presents a step-by-step algorithm for recording, preserving, and forensic examination of digital communications of organized criminal groups in Telegram, WhatsApp and Signal. Typical procedural errors and practical recommendations are outlined.

Key words: digital evidence, messengers, organized crime, forensic analysis, digital trace.

У сучасному цифровому середовищі мобільні месенджери стали ключовими платформами для комунікації, координації та конспірації діяльності організованих злочинних груп. Telegram, WhatsApp і Signal забезпечують високий рівень приватності завдяки застосуванню наскрізного шифрування, а також функціям прихованих і секретних чатів, автоматичного видалення повідомлень, анонімізації облікових записів, тимчасових номерів і використання VPN, що суттєво ускладнює процес фіксації, вилучення, збереження та експертного аналізу

цифрових даних та обумовлює потребу у чіткому, науково обґрунтованому алгоритмі роботи з такими доказами.

Цифрові комунікації у месенджерах є не лише засобом передавання інформації, але й цифровим відображенням структури та динаміки діяльності організованих груп. Саме вони дозволяють відтворити розподіл ролей, встановити механізми координації, визначити ієрархічні зв'язки, виявити ключових організаторів та виконавців, а також підтвердити планування злочинних дій, їх узгодженість у часі й просторі. Усе це значною мірою залежить від якості первинної фіксації даних, оскільки втручання в інтерфейс месенджера або вміст пристрою може призвести до незворотних змін.

Первинна фіксація повинна здійснюватися з максимальною точністю та безперервністю шляхом відеозапису всіх дій під час огляду пристрою. Важливо фіксувати інтерфейс месенджера в реальному часі, стан чатів, наявність непрочитаних повідомлень, назви груп, кількість учасників, часові мітки, ідентифікатори користувачів, дані про адміністраторів і характер налаштувань приватності. Відеозапис повинен документувати навіть найдрібніші дії, що унеможливлює сумніви щодо цілісності даних і демонструє, що інформація не була змінена в процесі огляду. Недостатня фіксація або відсутність відеозапису належить до найтиповіших помилок, які істотно підривають доказову цінність інформації.

Процесуальний огляд мобільного пристрою повинен передбачати документування технічних характеристик, зокрема моделі, серійного номера, встановлених SIM-карт, типу мережевих підключень, версій операційної системи та всіх месенджерів, активних VPN, хмарних резервних копій і стану синхронізації, що дозволяють визначити потенціал відновлення інформації, встановити можливі механізми приховування діяльності та оцінити структуру цифрового сліду. Не менш важливим є аналіз хмарних сервісів, адже саме там часто зберігаються резервні копії, що можуть містити значний обсяг видалених або недоступних локально повідомлень.

Створення цифрової копії пам'яті пристрою у форматі forensic image є критичною умовою належного експертного аналізу. Копія повинна бути повною, цілісною та верифікованою за допомогою хеш-функцій MD5 або SHA-256, що гарантує незмінність даних у подальших дослідженнях. Збереження лише одного екземпляра копії суперечить вимогам цифрової криміналістики, тому повинні створюватися як мінімум два ідентичні резервні образи. Використання спеціалізованих інструментів дозволяє відновити тимчасові файли, системні журнали, кеші, фрагменти видалених зображень і повідомлень, а також метадані, які часто є навіть цінішими за контент повідомлень.

Особливості побудови баз даних месенджерів визначають специфіку експертного аналізу. У Telegram ключовими є локальні кеші, тимчасові файли, журнали взаємодії з ботами, фрагменти прихованих або секретних чатів, ID

користувачів, інформація про адміністраторів і залишки видалених файлів. У WhatsApp значну роль відіграють файли msgstore.db і wa.db, які містять історію переписок, вкладення та журнали викликів, а також можуть містити фрагменти видалених або змінених повідомлень. У Signal дані зберігаються у зашифрованому вигляді, однак навіть у таких умовах медіафайли часто зберігаються у відкритих кешах, які можуть бути цінним джерелом доказів.

Аналітичний етап дослідження передбачає встановлення ролей учасників групи, оцінку характеру їхньої взаємодії, визначення послідовності передавання команд і виконання завдань, аналіз часової узгодженості дій, виявлення кореляції між цифровими даними та іншими видами доказів. Застосування інструментів OSINT, аналіз геолокаційних даних, журналів входів, характеристик пристрою, поведінкових патернів і зв'язків між учасниками, що дозволяє формувати цифровий профіль користувача та відновлювати приховані елементи його діяльності. Використання систем візуалізації зв'язків (link analysis) дає можливість побудувати структуру комунікацій, визначити ключові вузли комунікаційної мережі та виявити латентні або епізодичні зв'язки між учасниками.

Усі ці дії неможливо здійснити належним чином без дотримання певного комплексу рекомендацій, який є основою правильної цифрової криміналістики. Слідчі та експерти повинні залучати спеціаліста на найраннішому етапі, забезпечувати повну незмінність даних, використовувати лише сертифіковані інструменти, фіксувати кожен крок за допомогою відеозапису, створювати кілька forensic-копій, документувати технічні параметри пристрою, досліджувати хмарні резервні копії, аналізувати метадані й цифрові відбитки пристроїв, звертати увагу на ознаки використання VPN та одноразових номерів, а також не нехтувати пошуком прихованих чатів, тимчасових каналів та залишків видаленого контенту, які зберігаються у кешах та системних журналах. Окрім того, під час аналізу необхідно поєднувати цифрові дані з іншими джерелами доказової інформації, зокрема геолокацією, журналами з'єднань, записами камер спостереження і банківськими операціями, що дозволяє формувати комплексний криміналістичний портрет діяльності групи.

У підсумку слід зазначити, що запропонований алгоритм фіксації та експертного аналізу цифрових комунікацій у месенджерах забезпечує цілісне, достовірне й науково обґрунтоване дослідження інформації, що має вирішальне значення для ефективної протидії організованій злочинності. Дотримання методичних, технічних та процесуальних вимог дає можливість уникнути критичних помилок, сформувати надійний доказовий масив і підвищити результативність кримінальних розслідувань у сучасних умовах стрімкого розвитку цифрових комунікацій.

Перелік використаних джерел:

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition. Academic Press, 2011.
2. Hoog A. Android Forensics. Investigation, Analysis and Mobile Security for Google Android. Syngress, 2011.
3. Ayers R. , Brothers S. and Jansen W. Guidelines on Mobile Device Forensics, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2014.
4. Ekbal R., Mastorakis N. E. Elimination and Analysis of Ephemeral Messages in Android Social Media Apps: A Forensic Perspective. International Journal of Computers 10, 2025.
5. Verhaar M. B. From Chat to Crime: Telegram's Secrets!. 2025.
6. Patel B., Mann P. S. A Survey on Mobile Digital Forensic: Taxonomy, Tools, and Challenges. Security and Privacy. 2025. Т. 8. №. 2.
7. Kim G. et al. Analyzing the Web and UWP versions of WhatsApp for digital forensics. Forensic Science International: Digital Investigation. 2025. Т. 52.