DOI 10.34132/mspc2025.01.11.10

Елучка Казарян

ОСОБЛИВОСТІ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНОЇ ЕКСПЕРТИЗИ ПРИ РОЗСЛІДУВАННІ УМИСНИХ ВБИВСТВ ІЗ МОТИВІВ РАСОВОЇ, НАЦІОНАЛЬНОЇ ЧИ РЕЛІГІЙНОЇ НЕТЕРПИМОСТІ

Розглянуто значення використання спеціальних знань у кримінальному провадженні, зокрема шляхом призначення судових експертиз. Особливу увагу приділено інформаційно-комп'ютерній експертизі у справах про умисні вбивства, вчинені з мотивів нетерпимості. Визначено роль інформаційно-комп'ютерної експертизи у виявленні цифрових слідів, які свідчать про мотив злочину, його підготовку та організацію. Окреслено потенціал зазначеної експертизи у викритті організованих угруповань та встановленні ідеологічного підґрунтя злочину.

Ключові слова: *судова експертиза, інформаційно-комп'ютерна експертиза, цифрові сліди, мотив нетерпимості, кримінальне провадження.*

У процесі кримінального провадження важливу роль відіграє використання спеціальних знань, зокрема шляхом призначення судових експертиз. Вони забезпечують неупереджене дослідження об'єктів, явищ чи процесів з метою отримання обґрунтованих висновків, які мають доказове значення. Судова експертиза як процесуальна форма застосування спеціальних знань є необхідним елементом ефективного розслідування, особливо у складних та резонансних справах.

У науковій літературі судову експертизу трактують як процесуальну дію, що передбачає дослідження речових доказів, матеріалів, об'єктів чи осіб з метою встановлення фактичних обставин, які мають значення для кримінального провадження. Проведення експертизи здійснюється за дорученням слідчого судді чи суду, наданим за клопотанням сторони кримінального провадження [1, с. 422]. Її особливість полягає в тому, що експертні дослідження дозволяють встановити факти, які неможливо з'ясувати за допомогою інших слідчих (розшукових) дій, але які відіграють важливу роль у кримінальному провадженні.

Згідно зі ст. 1 Закону України «Про судову експертизу», вона визначається як дослідження об'єктів, явищ чи процесів із застосуванням спеціальних знань у галузях науки, техніки, мистецтва, ремесел тощо з метою надання висновку з питань, що мають значення для судового розгляду. Водночас стаття 7^1 цього ж Закону встановлює, що підставою для проведення експертизи є відповідна постанова органу досудового розслідування, судове рішення або договір з експертною установою чи експертом – у разі її проведення на замовлення інших осіб [2].

Кримінальний процесуальний кодекс України також регулює порядок призначення та проведення експертизи. Зокрема, ч. 1 ст. 242 цього Кодексу визначає, що експертизу здійснюють експертна установа або експерти, які залучаються сторонами кримінального провадження або слідчим суддею за клопотанням сторони захисту у випадках, коли для встановлення обставин, що мають значення для кримінального провадження, потрібні спеціальні знання. А згідно з ч. 2 ст. 84 Кримінального процесуального кодексу України, висновок експерта належить до процесуальних джерел доказів [3].

У контексті розвитку інформаційного суспільства дослідження цифрових слідів набуває особливого значення під час розслідування умисних вбивств, скоєних із мотивів расової, національної чи релігійної нетерпимості, оскільки такі сліди можуть вказувати на наявність спеціального мотиву – нетерпимості. З урахуванням сучасних наукових підходів до визначення доцільності проведення судових експертиз у справах зазначеної категорії, варто наголосити на необхідності проведення інформаційно-комп'ютерної експертизи (далі – ІКЕ), яка є підвидом комп'ютерно-технічної експертизи, що належить до інженерно-технічних судових експерти. Цей вид експертизи забезпечує виявлення, фіксацію, аналіз та збереження цифрових доказів, які в інших умовах можуть залишатися недоступними. Завдяки використанню сучасних технологій стає можливим аналіз інформації з комп'ютерних пристроїв, мобільних телефонів, хмарних сервісів та соціальних мереж. Це особливо важливо в умовах, коли злочинці дедалі активніше застосовують цифрові технології для планування, координації та поширення протиправних дій, що суттєво ускладнює застосування традиційних методів розслідування. У таких випадках ІКЕ часто виступає єдиним ефективним способом отримання достовірної інформації.

ІКЕ спрямована на встановлення обставин, пов'язаних із процесами створення, обробки та зберігання інформації на комп'ютерних та магнітних носіях. Основне завдання цієї експертизи полягає у пошуці, виявленні, відтворенні та технічному аналізі даних, які були створені користувачем або програмним

забезпеченням у комп'ютерній системі [4, с. 141]. Так, для проведення ІКЕ експерту надаються різноманітні об'єкти дослідження, зокрема персональні комп'ютери, мобільні телефони, планшети, носії даних (жорсткі диски, флеш-накопичувачі) та інші електронні пристрої, які можуть містити сліди злочинної діяльності. Експерт може визначити, чи містить наданий об'єкт інформацію у будь-якому вигляді (файли, аудіо, відео, листування, пости у соціальних мережах тощо), яка стосується наявності ознак, що можуть свідчити про наявність мотиву нетерпимості. Крім того, експерт може встановити чи містить об'єкт дослідження видалені файли (графічні, текстові, відео, аудіо) і чи можливо їх відновити [5, с. 268-269].

ІКЕ проводиться для виявлення, фіксації та аналізу даних з цифрових носіїв, що можуть підтверджувати підготовку або вчинення злочину. Вона відіграє ключову роль у розкритті злочинів з мотиву нетерпимості, оскільки дозволяє ідентифікувати відповідний мотив шляхом дослідження інформаційного контенту, електронного листування та комунікацій у соціальних мережах. У межах ІКЕ фахівці здійснюють аналіз комп'ютерної техніки, мобільних пристроїв та цифрових носіїв з метою пошуку файлів, що містять ознаки екстремістського змісту, а також вивчають листування, історію браузера, месенджери (наприклад, WhatsApp, Telegram) та інші джерела цифрових доказів. Особливості цієї експертизи обумовлені необхідністю не лише встановлення факту вчинення протиправних дій, але й виявлення спеціального мотиву, викриття організованих злочинних угруповань, аналізу пропагандистських матеріалів, а також подоланням технічних бар'єрів, пов'язаних із використанням сучасних методів шифрування даних.

У випадках, коли комп'ютерні дані, що зберігаються у пам'яті електронно-обчислювальної техніки, були створені або змінені внаслідок дій правопорушника чи інших осіб під час або у зв'язку із вчиненням кримінального правопорушення, такі дані набувають доказового значення. Вони можуть бути вилучені й проаналізовані як електронні (цифрові) сліди правопорушення. У цьому контексті доцільно розглядати електронні (цифрові) сліди як комп'ютерну інформацію, що виникла або зазнала модифікацій у результаті взаємодії користувача з комп'ютерною технікою, пов'язаної зі злочинною діяльністю [6, с. 230]. Комп'ютерну інформацію умовно поділяють на два основні типи: перший – це дані, які створює та використовує сам користувач, а другий – це інформація, сформована комп'ютерними програмами з метою забезпечення функціонування інформаційних процесів у системі.

Одним із основних завдань ІКЕ є виявлення мотиву нетерпимості. У багатьох випадках злочинці залишають цифрові сліди, які свідчать про їхні умисні дії, здійснені у цифровому (віртуальному) середовищі, які спрямовані на формування, розвиток і реалізацію ідеологічного, інформаційного та організаційного підґрунтя для вчинення насильницького злочину, зумовленого ідеєю ворожнечі до певної групи за ознаками раси, етнічного походження, релігії або світогляду. Це можуть бути відеозаписи, текстові документи, листування в соціальних мережах або месенджерах, що містять ворожі висловлювання або прямі погрози на адресу певних соціальних, етнічних чи релігійних груп. Аналіз подібних матеріалів дозволяє встановити зв'язок між особою підозрюваного та ідеологічною платформою, що надихала його на вчинення злочину.

Особливу увагу під час ІКЕ приділяють цифровим доказам, пов'язаним із споживанням, поширенням і взаємодією користувача з екстремістським контентом. Такий контент розміщується у відкритому або напівзакритому доступі – зокрема в соціальних мережах, спеціалізованих Telegram-каналах, Discord-серверах, на форумах або платформах типу Reddit. Йдеться про перегляди відео з насильницьким або пропагандистським змістом, читання і збереження текстів, мемів, маніфестів тощо. До типових цифрових слідів цього процесу належать історія пошукових запитів, кеш-пам'ять браузера, список підписок, вподобань, відвідані ресурси, завантажені файли. Їх виявлення дозволяє відтворити етапи ідеологічної трансформації особи – від ознайомлення з радикальним контентом до внутрішнього прийняття і реалізації ворожих установок у формі насильницьких дій.

Електронні сліди мають особливу цінність у розслідуванні тяжких злочинів, зокрема умисних убивств, навіть якщо самі обставини цих слідів не пов'язані безпосередньо з моментом скоєння злочину. Такі цифрові дані можуть сприяти розкриттю суб'єктивної сторони злочину, зокрема виявленню мотивів, цілей та психологічних характеристик правопорушника, а також встановленню його місцеперебування. Особливо важливим є аналіз інформації, що дозволяє з'ясувати, чи був злочин скоєний на ґрунті нетерпимості. Подібна інформація може міститися у висловлюваннях особи в соціальних мережах, листуванні, коментарях або публікаціях, зроблених до або після злочину.

Цифрові сліди, що зберігаються на віддалених інформаційних носіях і знаходяться у відкритому доступі в Інтернеті – наприклад, на платформах соціальних мереж або форумах з екстремістським контентом, – можуть бути виявлені й зафіксовані за допомогою стандартних засобів комп'ютерної техніки, зокрема персонального комп'ютера та веббраузера. Методи фіксації таких слідів включають збереження вебсторінок у форматі *.html, друк їхнього вмісту, а також відеозапис екрана під час огляду вебресурсу. Таке документування має важливе значення для подальшого криміналістичного аналізу цифрових доказів і правової оцінки дій підозрюваного [7, с. 169]

Наступним важливим аспектом є розкриття злочинних угруповань, оскільки злочини з мотивів нетерпимості часто вчиняються не індивідуально, а у складі організованих груп. Аналіз цифрових даних може допомогти правоохоронним органам ідентифікувати структуру угруповань, їхню внутрішню комунікацію, роль кожного учасника та ступінь координації їхніх дій. Дослідження електронних листувань, файлів, спільних чатів у месенджерах або зашифрованих каналів зв'язку дозволяє отримати докази змови

або спільного планування злочину: вибір цілі (жертви або місця), дати, методу, маршруту тощо. Поширеною є практика обміну схемами, зображеннями зброї, інструкціями з виготовлення вибухових речовин, а також обговорення питань маскування, відступу, запису відео нападу. Також використовуються засоби захисту комунікацій (VPN, Tor, зашифровані месенджери), що ускладнює фіксацію таких даних.

Ще одним із ключових напрямів ІКЕ є можливість відновлення раніше видаленої інформації, яка може мати доказове значення у кримінальному провадженні. За допомогою спеціалізованого програмного забезпечення, такого як EnCase, можна відновити видалені повідомлення, файли або історію переглядів у браузері. Крім того, експерти здійснюють аналіз соціальних мереж, щоб виявити участь підозрюваних у групах, що пропагують насильство чи нетерпимість, досліджують електронну комунікацію та встановлюють осіб, які створювали чи поширювали ворожі матеріали.

Однак проведення ІКЕ пов'язане з низкою проблем. Однією з основних є складність доступу до зашифрованих даних, особливо якщо злочинці використовують VPN, Tor чи спеціальні програми для автоматичного видалення інформації. Разом із цим, розслідування злочинів із використанням цифрових технологій супроводжується значними технічними перешкодами. Однією з основних є шифрування даних у сучасних засобах комунікації. Популярні месенджери (наприклад, Signal, Telegram) та електронні поштові сервіси (Proton Mail) використовують технології наскрізного шифрування, що унеможливлює отримання змісту повідомлень без доступу до пристрою підозрюваного. Крім того, злочинці можуть використовувати спеціалізовані програми для автоматичного знищення даних, зокрема Burner App або Secure Erase, що ускладнює відновлення доказової інформації.

У ході розслідування умисних вбивств із мотивів нетерпимості доцільно формулювати такі запитання:

– Чи виявлено надані комп'ютерні дані (файли, листування, медіаконтент), що містять ознаки закликів до насильства щодо певної расової, національної або релігійної групи?

– Чи є на пристрої підозрюваного збережені або відновлені повідомлення, які свідчать про плани щодо вчинення злочину?

– Чи використовувались спеціальні засоби для приховування інформації (VPN, анонімайзери, зашифровані канали)?

Таким чином, ІКЕ забезпечує комплексне дослідження цифрових носіїв інформації з метою виявлення доказів, які безпосередньо стосуються мотивів нетерпимості, характеру комунікацій, використаних технічних засобів, а також учасників злочинної діяльності. Її застосування є невід'ємною умовою ефективного розслідування в умовах цифровізованого суспільства.

References

1. **Shepityko, V. Yu., Zhuravel, V. A., Konovalova, V. O., et al.** (2019). *Kryminalistyka [Forensics]*. Kharkiv: Pravo [in Ukrainian].
2. Zakon Ukrainy «Pro sudovu ekspertyzu» [Law of Ukraine «On Forensic Examination»]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/4038–12#Text [in Ukrainian].
3. Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].
4. **Karpinska, N., & Krykunov, O.** (2017). Okremi pytannia provedennia sudovoi komp'iuterno-tekhnichnoi ekspertyzy u kryminalnomu sudochynstvi [Certain Issues of Conducting Computer and Technical Forensic Examinations in Criminal Proceedings]. *Istoryko-pravovyi chasopys - Historical and Legal Journal*, 1 (9), 140–144 [in Ukrainian].
5. Kazarian, E. (2023). The Use of Special Knowledge in the Investigation of Murders Motivated by Racial, National or Religious Intolerance. *Věda a Perspektivy,* 12 (31), 260–271. DOI: 10.52058/2695-1592-2023-12(31)-260-271.
6. Kovalenko, A.V. (2022). Poniattia ta sutnist elektronnykh (tsyfrovykh) slidiv kryminalnoho pravoporushennia [The Concept and Essence of Electronic (Digital) Traces of a Criminal Offense]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E.O. Didorenka – Bulletin of the Luhansk State University of Internal Affairs named after E. O. Didorenko*, 4, 226–236 [in Ukrainian].
7. Kazarian, E. (2023). Elektronni (virtualni) slidy v rozsliduvanni umysnykh ubyvstv iz motyviv rasovoi, natsionalnoi chy relihiinoi neterpymosti [Electronic (Virtual) Traces in the Investigation of Murders Motivated by Racial, National or Religious Intolerance]. Proceedings from *mizhnar. nauk.-prakt. konf. z nahody 100-richchia Natsionalnoho naukovoho tsentru «Instytut sudovykh ekspertyz im. Zasl. prof. M. S. Bokariusa» «Aktualni pytannia sudovoi ekspertyzy i kryminalistyky» – International Scientific and Practical Conference Dedicated to the 100th Anniversary of the National Scientific Center «Institute of Forensic Examinations named after Honored Professor M. S. Bokarius» «Current Issues of Forensic Science and Criminalistics»* (pp. 168–170). Kharkiv: NSC «Institute of Forensic Examinations named after M. S. Bokarius» [in Ukrainian].

DOI 10.34132/mspc2025.01.11.10

PECULIARITIES OF INFORMATION AND COMPUTER FORENSICS IN THE INVESTIGATION OF INTENTIONAL HOMICIDES MOTIVATED BY RACIAL, NATIONAL, OR RELIGIOUS INTOLERANCE

The peculiarities of electronic traces in the investigation of intentional murders The significance of using specialized knowledge in criminal proceedings is examined, particularly through the appointment of forensic examinations. Special attention is given to information and computer forensics (ICF) in cases of intentional homicides committed with motives of intolerance. The role of ICF in identifying digital traces that indicate the motive, preparation, and organization of the crime is outlined. The potential of ICF in uncovering organized groups and establishing the ideological background of the offense is highlighted.

Keywords: *forensic examination, information and computer forensics, digital traces, motive of intolerance, criminal proceedings.*

Відомості про автора / Information about the Author

Елучка Казарян, доктор філософії у галузі права, старший викладач кафедри конституційного та адміністративного права і процесу, Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: kazarian.e@chmnu.edu.ua, orcid: https://orcid.org/0000-0002-7353-2599.

Eluchka Kazarian, PhD in Law, Senior Lecturer at the Department of Constitutional and Administrative Law and Procedure of the Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: kazarian.e@chmnu.edu.ua, orcid: https://orcid.org/0000-0002-7353-2599.

Стаття отримана редакцією 22.05.2025.