

Судово-експертне дослідження відео-, звукозаписів: особливості та обмеження

Костянтин Нікулін

старший судовий експерт, сектору комп'ютерно-технічних, телекомунікаційних досліджень та досліджень відео-, звукозапису лабораторії інженерно-технічних досліджень, Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м Харків, Україна, ORCID: <https://orcid.org/0000-0002-0665-6313>, e-mail: knikuln87@gmail.com

Ольга Брендель

PhD, завідувач сектору комп'ютерно-технічних, телекомунікаційних досліджень та досліджень відео-, звукозапису лабораторії інженерно-технічних досліджень, Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м Харків, Україна, ORCID: <https://orcid.org/0000-0002-1723-0203>, e-mail: olgabrenda@ukr.net

Висвітлено основні особливості проведення судової експертизи відео-, звукозапису, аналіз сучасних способів фальсифікації аудіо-, відеоданих; узагальнення підходів до встановлення їх автентичності; особливості проведення експертиз з урахуванням сучасних способів і засобів вчинення правопорушень.

Ключові слова: експертиза відео-, звукозапису; монтаж; симуляція голосу; ланцюг зберігання.

Forensic Examination of Video and Audio Recordings: Features and Limitations

Kostiantyn Nikulin, Olha Brendel

The abstracts highlight the main features of conducting forensic examination of video and audio recordings, and analyze modern methods of falsifying audio and video data; a generalization of approaches to establishing their authenticity; and the features of conducting examinations taking into account modern methods and means of committing offenses.

Keywords: video and audio recording examination; editing; deepfake audio; chain of custody.

У сучасних умовах відео-, звукозапис є одним із найпоширеніших видів цифрових доказів, що можуть містити відомості про обставини злочину, особу правопорушника, механізм учинення діяння та інші істотні деталі. Повномасштабна війна, яку веде російська федерація проти України, спричинила не лише гуманітарну та економічну кризу, а й кардинальні зміни у способах вчинення правопорушень. В умовах воєнного стану активно застосовуються сучасні інформаційні технології, цифрові платформи, засоби дистанційної комунікації та відео-, аудіофіксування. У цих умовах значно зросло навантаження на систему судово-експертних установ, особливо у сфері експертизи відео-, звукозапису, що відіграє важливу роль у визначенні обставин справи, автентичності доказів і джерела походження інформації.

Водночас технічна доступність програм редагування, можливості створення мон-

тажу, симуляцій голосу (*deepfake audio*) та зміни метаданих відеозаписів створюють вагомий виклик для експертної практики. Особливості таких матеріалів потребують нових підходів до експертних досліджень і постійного оновлення технічного арсеналу судово-експертних установ [1]. Питання вдосконалення методів судових експертиз відео-, звукозаписів в умовах війни набуває особливої актуальності, коли цифрові докази часто є єдиним засобом встановлення істини. Судова експертиза відео-, звукозапису є однією з найбільш складних і водночас найважливіших галузей криміналістичних досліджень. Її метою є не лише підтвердження або спростування факту монтажу, а й визначення умов, у яких був створений запис, ототожнення особи за голосом, визначення технічних характеристик пристрою тощо. Ефективність таких досліджень безпосередньо впливає на достовірність доказової бази.



Цифровізація державного управління та системи правосуддя значно підвищила значення електронних доказів у розгляді адміністративних справ. Згідно із загальним визначенням у Кодексі адміністративного судочинства України (далі — КАСУ), *«електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звуко- записи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі»* [2]. Судово-експертна діяльність регламентується також Законом України «Про судову експертизу» та відповідними інструкціями Міністерства юстиції України. Ці документи визначають завдання експерта, його процесуальний статус, а також вимоги до збереження цифрових носіїв і ланцюга передачі доказів (*chain of custody*). КАСУ передбачає подання електронних доказів у вигляді оригіналу, електронної копії, засвідченої електронним підписом, або паперової копії. Утім на практиці поняття «оригінал» електронного доказу є предметом суперечок, адже цифрові дані залишаються ідентичними під час копіювання. У практиці Європейського Союзу та США значна увага приділяється саме збереженню цифрової цілісності файлів, що є необхідною умовою допустимості доказів у суді [3]. Матеріали відео-, звукозаписів розглядаються як джерела доказів, а також як об'єкти криміналістичних експертних досліджень. Вони слугують підґрунтям для формування такого важливого доказу, як висновок експерта. Особливості цих матеріалів як об'єктів дослідження, різноманітність завдань, які можуть бути поставлені перед експертами, а також низка інших чинників обумовлюють певні специфічні аспекти, на які замовникам варто звернути увагу під час призначення експертизи.

Однією з головних проблем у сфері експертизи відео-, звукозапису є відсутність оригіналів записів. Часто до експерта надходять копії, які були передані через месенджери або соцмережі, унаслідок чого файл

знає перекодування, утрачає частину метаданих і характеристик сигналу. Це ускладнює визначення реальної структури запису. Окрім того, виявлення ознак монтажу потребує не лише технічного аналізу, а й глибоких знань у сфері акустики, фонетики, кінематографії та комп'ютерної графіки. Будь-яка помилка може призвести до неправильного тлумачення результатів [4].

Зазвичай сучасні методичні підходи до проведення експертизи відео-, звукозаписів передбачають поетапне дослідження:

- на підготовчому етапі — отримання матеріалів, створення копій із захистом від змін, фіксування технічних параметрів;
- на етапі попереднього аналізу — визначення формату файлу, кодека, частоти дискретизації, метаданих і структури контейнера та інших чинників, які мають значення для дослідження;
- на етапі основного дослідження — аналізування сигналу на наявність монтажу, оцінювання цілісності звукового тла, перевірка синхронності аудіо- та відеоряду тощо;
- етап ідентифікаційних досліджень передбачає встановлення особи за голосом, визначення джерела звуку або пристрою запису;
- заключний етап — оформлення експертного висновку із зазначенням методів, програм і результатів.

Для підвищення достовірності висновків експерти часто застосовують комбіновані методи, що поєднують різні методи дослідження, наприклад, порівняння спектрограм за допомогою кореляційних алгоритмів дає змогу з високою точністю виявляти вставлені або вирізані ділянки сигналу. Для проведення експертиз користуються як загальнодоступними програмами (*Audacity, Sonic Visualiser, Adobe Audition*), так і спеціалізованими системами, розробленими для криміналістичних цілей: *iZotope RX, Amped Authenticate, Forensic Audio Workstation, VideoCleaner, Avid Forensic Toolkit* тощо [3].

З розвитком штучного інтелекту з'явилися інструменти, що дають змогу створювати реалістичні синтетичні зображення та

голоси. Такі технології, як *DeepFake*, *Voice Cloning*, *AI Lip-Sync* тощо, уможливають підрубку відео-, звукозаписів на рівні, який важко відрізнити від оригіналу без спеціальної експертизи. Ці технології іноді застосовують для інформаційних провокацій, створення «компромату» або фальсифікації доказів у справах. Водночас умови отримання, передавання та зберігання таких матеріалів часто не відповідають вимогам криміналістичної «чистоти»: записи можуть бути уривчастими, повторно перекодованими, пересланими через месенджери (*Telegram*, *Viber*, *WhatsApp* тощо) або завантаженими у соціальні мережі. Це ускладнює завдання експерта, який має встановити, чи зазнавав запис монтажу або редагування; чи є він неперервним; чи відповідають його метадані фактичним обставинам тощо.

В умовах війни часто відсутня можливість вилучити пристрій, на який здійснено запис, або підтвердити ланцюг зберігання (*chain of custody*) [3]. Тому експерт повинен максимально точно описати як формат файлу, наявність перекодування, так і джерело отримання, будь-які ознаки втручання тощо.

Судова експертиза відео-, звукозапису залишається однією з найважливіших і найдинамічніших галузей криміналістичних досліджень. Її розвиток потребує поєднання традиційних методів з інноваційними технологіями цифрового аналізу, машинного навчання та штучного інтелекту. У сучасних умовах експертиза відео-, звукозапису є одним

із найважливіших інструментів установлення істини.

Експерт повинен не лише мати високий рівень технічних знань, а й розуміти психологію сприйняття, інформаційні ризики та сучасні методи цифрової підробки. Подальший розвиток експертної практики потребує інтеграції методів цифрової криміналістики, впровадження штучного інтелекту та міжнародної співпраці у сфері стандартизації процедур перевірки цифрових матеріалів.

Перелік джерел посилання

1. Nguyen Le T. D., Teh K. K., Dat Tran H. Continuous Learning of Transformer-based Audio Deepfake Detection. URL: <https://arxiv.org/pdf/2409.05924> (дата звернення: 04.11.2025).
2. Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV (зі змін та допов.). URL: <https://zakon.rada.gov.ua/laws/show/2747-15#Text> (дата звернення: 19.12.2025).
3. Scientific Working Group on Digital Evidence, «SWGDE Best Practices for Forensic Audio». URL: [https://www.swgde.org/documents/Current%20 Documents](https://www.swgde.org/documents/Current%20Documents) (дата звернення: 11.11.2025).
4. Брендель О. І. Дослідження автентичності цифрових відео- та звукозаписів. *Використання цифрових технологій у криміналістиці та судовій експертизі* : мат-ли міжнар. наук.-практ. кругл. столу (м. Харків, 11.12.2023) Харків, 2024. С. 56—61. URL: <https://surl.lu/eltqvf> (дата звернення: 19.12.2025).