

мети вчинення злочину пояснюється виконанням військовослужбовцями держави-агресора злочинних наказів, що потребує додаткового дослідження ланцюгів командування.

Отже, можна дійти висновку, що проблеми досудового розслідування кримінальних правопорушень, вчинених військовослужбовцями Російської Федерації, насамперед пов'язані із особливостями встановлення обставин, що становлять предмет доказування. У результаті проведеного дослідження встановлено, що вирішення зазначених проблем потребує розширення криміналістичних підходів, ширшого застосування сучасних технологічних можливостей, а також посилення міжнародної взаємодії.

Список використаних джерел

1. Подоляка О., Курбатова І., Крютченка Л. Розслідування кримінальних правопорушень, вчинених військовослужбовцями: виклики воєнного стану та шляхи адаптації кримінального процесу. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. Вип. 2 (74). 2025. С. 89–97. URL: <https://doi.org/10.32689/2522-4603.2025.2.14>.
2. Собенко Н., Куренкова О. В Україні зареєстровано понад 213 тисяч воєнних злочинів росіян. *Суспільне новини*. 2026. URL: <https://suspilne.media/1255088-v-ukraini-zareestrovano-ponad-213-tisac-voennih-zlociniv-rosian/>.
3. Шевчишена К. П. Розслідування воєнних злочинів в Україні. *Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук*. 2024. С. 21. URL: https://www.navs.edu.ua/files/spec-vchena-rada/srd_26_007_03/2024/avtoref_shevchyshena.pdf.

Кравченко Наталія Володимирівна,
викладач кафедри криміналістики
навчально-наукового інституту права
та психології Національної академії
внутрішніх справ

СУЧАСНІ МОЖЛИВОСТІ ФОНОСКОПІЧНОЇ ЕКСПЕРТИЗИ У ВИЯВЛЕННІ «ДІПФЕЙКІВ» У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

Стрімкий розвиток генеративного штучного інтелекту зумовив появу принципово нових викликів для системи правосуддя. Одним із найбільш деструктивних інструментів у руках правопорушників стала технологія «Deepfake», яка дозволяє створювати високореалістичні аудіовізуальні підробки. В умовах воєнного стану використання синтезованого контенту набуває ознак інформаційних атак, спрямованих на дискредитацію військово-політичного керівництва та дезорієнтацію суспільства [2]. У зв'язку з цим, модернізація методів фоноскопичної експертизи стає критично важливою для ідентифікації підробленого мовлення та забезпечення допустимості доказів у суді.

Наукова новизна підходу до розв'язання цієї проблеми полягає в інтеграції автоматизованих аналітичних інструментів штучного інтелекту безпосередньо в експертну діяльність. Інтеграція цифрових технологій не замінює судового експерта, а підсилює його спроможності, скорочує час дослідження та підвищує об'єктивність висновків [5]. Сучасні методи детекції «дівфейків» базуються на пошуку специфічних цифрових аномалій, що виникають під час роботи

нейромереж, зокрема моделей GAN та VAE. Це дозволяє виявляти невідповідності у спектрограмах та фізіологічних параметрах мовця, які є невидимими для людського слуху.

Важливим аспектом сучасної експертизи є біометрична верифікація. Зокрема, інноваційним методом є детекція за мікроколиваннями кольору шкіри обличчя в такт серцебиттю (*blood flow detection*), оскільки генеративні алгоритми ще не здатні повноцінно імітувати такі складні фізіологічні процеси. У поєднанні з класичними методами фоноскопії, що аналізують тембральні характеристики, такий підхід забезпечує високу точність розпізнавання синтезованого голосу [7].

Процесуальний аспект збирання таких доказів вимагає суворого дотримання стандартів щодо огляду комп'ютерних даних відповідно до ст. 237 КПК України. Важливим є забезпечення ланцюга збереження доказів (*chain of custody*) та фіксація геш-значень цифрових об'єктів [4]. Гармонізація вітчизняної практики з міжнародними стандартами, зокрема з Протоколом Берклі, є необхідною умовою для того, щоб українські експертні висновки визнавалися у міжнародному правовому полі [3].

Окрему увагу слід приділити стандартам Ради Європи. Використання технологій розпізнавання біометричних даних у кримінальному провадженні має базуватися на принципах законності, прозорості та етики [1]. Адаптація методик під вимоги *EU AI Act* дозволяє створити прозорий механізм аудиту алгоритмів штучного інтелекту, що використовуються експертами, запобігаючи упередженості та помилковим спрацьовуванням [6].

Отже, сучасна фоноскопична експертиза трансформується у високотехнологічну галузь цифрової криміналістики. Подальший розвиток національних експертних служб має бути спрямований на впровадження автоматизованих систем розпізнавання фальсифікацій, що стане дієвою відповіддю на сучасні кіберзагрози.

Список використаних джерел

1. Ахтирська Н. М. Стандарти Ради Європи щодо використання технологій розпізнавання облич у кримінальному провадженні або на кого дивиться око Саурана. *Науково-інформаційний вісник Івано-Франківського університету імені Короля Данила Галицького*. 2023. Вип. 15 (27). Т. 1. С. 228–238.
2. Марчук М. Б., Лукічов В. В. Аналіз методів використання технології Deepfake для інформаційних атак. *Вінницький національний технічний університет*. 2025. С. 1–4.
3. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. 2020. 119 с.
4. Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. DOI: <https://doi.org/10.32631/vsa.2024.2.25> *Вісник Кримінологічної асоціації України*. 2024. № 2 (32). С. 344–353.
5. Чечіль Ю. Інтеграція цифрових технологій у судово-експертну діяльність. *Аналітично-порівняльне правознавство*. 2025. № 5 (3). С. 296–303.
6. The EU Artificial Intelligence Act. URL: <https://artificialintelligenceact.eu/the-act/>.
7. Digital and Multimedia Evidence. *The National Institute of Justice (NIJ)*. 2024. URL: <https://nij.ojp.gov/topics/forensics/digital-multimedia-evidence>.