

DOI <https://doi.org/10.32782/2786-9156.111.3.92-101>
УДК 343.98

Коваль А. А., доктор юридичних наук, професор, завідувач кафедри конституційно-го та адміністративного права і процесу Чорноморського національного університету імені Петра Могили (м. Миколаїв, Україна)

e-mail: alla.koval@chmnu.edu.ua

ORCID iD: <https://orcid.org/0000-0002-8638-5698>

Петренко К. Д., адвокат, адвокатське об'єднання «Актум» (м. Львів, Україна)

e-mail: advokatya82@gmail.com

ORCID iD: <https://orcid.org/0009-0007-2244-9000>

МОВА ВОРОЖНЕЧІ В ЦИФРОВОМУ ПРОСТОРІ: ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ

У статті проаналізовано особливості розслідування кримінальних правопорушень, пов'язаних із поширенням мови ворожнечі в цифровому просторі, зокрема в соціальних мережах. Визначено, що мова ворожнечі в інтернеті – це публічні висловлювання, спрямовані на приниження гідності, дискримінацію або розпалювання ненависті до окремих осіб чи груп за ознаками раси, національності, мови, релігії, статі тощо. Акцентовано увагу, що запобігання й протидія мові ворожнечі та розпалюванню ненависті в соціальних мережах мають складний і багатокомпонентний характер. Особливого значення в цьому процесі набуває розслідування кримінальних правопорушень цієї категорії, метою якого є притягнення винних до кримінальної відповідальності. Зважаючи на цифрову природу таких правопорушень, акцент зроблено на специфіці доказування, необхідності застосування інструментів цифрової криміналістики й міждисциплінарного підходу. Проаналізовано правову кваліфікацію дій за статтями КК України, наведено приклади судової практики. Окрема увага приділена ролі експертизи (лінгвістичної, психологічної, комп'ютерно-технічної) у процесі доведення мотиву ненависті й ідентифікації правопорушника. Розкрито методи виявлення цифрових слідів, збору доказів, проблематику анонімності й обмеженого доступу до серверів соціальних платформ. У статті також охарактеризовано ключові напрями цифрової криміналістики, які застосовуються під час розслідувань, зокрема аналіз мобільних пристроїв, хмарних сховищ, месенджерів, соціальних мереж, геолокаційних даних і цифрових слідів поведінки. Автори наголошують на важливості залучення фахівців із цифрової аналітики й OSINT, що суттєво підвищує ефективність виявлення правопорушень у середовищі інформаційних загроз. Висвітлено практику ЄСПЛ щодо меж свободи вираження та мови ворожнечі. Запропоновано підходи до вдосконалення ефектної й слідчої практики.

Ключові слова: мова ворожнечі, дискримінація, відповідальність, кримінальні правопорушення, розслідування, судові експертизи, слідчий, експерт, цифрова криміналістика.

Постановка проблеми. У сучасному інформаційному суспільстві цифрові комунікаційні платформи, зокрема соціальні мережі, відіграють ключову роль у формуванні громадської думки, політичних позицій і соціальних взаємодій. Проте водночас вони стали середовищем, у якому активно поширюється мова ворожнечі – публічні висловлювання, що містять ознаки нетерпимості, дискримінації, приниження гідності особи або груп за ознаками раси, національності, релігії, статі, сексуальної орієнтації, мови, місця проживання, соціального статусу чи політичних переконань.

Особливої гостроти ця проблема набуває в умовах воєнного стану, коли країна стикається з масштабними загрозами в різних сферах, у тому числі в інформаційному просторі. Використання мови ворожнечі в цифрових медіа є не лише фактором дестабілізації суспільства, а й інструментом інформаційної війни, спрямованої на підірив національної єдності, провокування агресії, страху та ненависті.

У цьому контексті постає нагальна потреба у створенні ефективних механізмів виявлення, дослідження й документування проявів мови ненависті в мережевому середовищі. Застосування цифрових інструментів моніторингу, аналізу та розслідування таких висловлювань потребує міждисциплінарного підходу, що поєднає юридичні, соціологічні, лінгвістичні й інформаційно-технологічні знання.

Таким чином, проблема розслідування мови ворожнечі в цифровому просторі, зокрема в соціальних мережах, є надзвичайно актуальною, оскільки безпосередньо пов'язана з гарантіями прав людини, інформаційною безпекою, суспільною злагодою та ефективним функціонуванням демократичних інституцій в умовах нових глобальних викликів.

Аналіз останніх досліджень і публікацій. Окремі аспекти мови ворожнечі досліджували С. Лихова, Г. Рибальченко, О. Львова, М. Медведєва. Питання протидії злочинам на ґрунті ненависті, розробляли й продовжують розробляти С. Алфьоров, В. Бурлака, О. Горбачова, Н. Дрьоміна-Волок, Е. Казарян, В. Ковальчук, О. Колб, А. Корнієнко, О. Крюков, В. Куц, О. Мартиненко, Т. Пазинич та інші. Сучасні виклики цифрової криміналістики є предметом дослідження Г. Авдєєвої, М. Соколенка, Р. Степанюка, В. Шевчука, В. Шепітька й багатьох інших вітчизняних і зарубіжних учених. Проте питання розслідування кримінальних правопорушень, пов'язаних із використанням мови ворожнечі в цифровому просторі, потребують окремого поглибленого дослідження.

Формулювання цілей. Метою статті є на підставі дослідження теоретичних засад і практичних аспектів розслідування кримінальних правопорушень, пов'язаних із використанням мови ворожнечі у цифровому просторі, визначити особливості доказування й нормативно-правового забезпечення цього процесу в умовах воєнного стану. На основі аналізу чинного кримінального та кримінального процесуального законодавства України в поєднанні з практикою Європейського суду з прав людини (далі – ЄСПЛ) передбачається виявити ознаки мови ворожнечі як окремого виду мовленнєвого делікту. З урахуванням сучасних правових, криміналістичних та експертних підходів – надати характеристику методів ідентифікації анонімних правопорушників, а також визначити роль лінгвістичної, психологічної й комп'ютерно-технічної експертизи в доказуванні мотиву ненависті.

Виклад основного матеріалу. Рухаючись курсом євроінтеграції, Україна взяла на себе зобов'язання дотримуватися міжнародних стандартів щодо рівності й недискримінації, зокрема Конвенції про захист прав і основних свобод [1], Рамкової конвенції Ради Європи про захист національних меншин, Рекомендації СМ/Rec(2022)16 Комітету Міністрів державам-членам щодо боротьби з мовою ворожнечі [2], Рекомендації № R (97) 20 Комітету Міністрів державам-членам щодо «мови ненависті» [3].

Проте використання ненависті й розпалювання ворожнечі поширюється. Так, за даними Національної поліції України та громадських моніторингових організацій, у 2024 році зареєстровано понад 370 фактів публічного поширення мови ворожнечі в соціальних мережах. При цьому близько 70% таких випадків стосувались ознак дискримінації за національною, релігійною або сексуальною ознакою [4].

Варто зазначити, що в національному законодавстві відсутнє легальне визначення мови ворожнечі. Тому, спираючись на європейське законодавство, а також на практику його застосування, ми запропонували власну дефініцію цього явища: «Мова ворожнечі – це будь-яке публічне висловлювання або дія, що має на меті або може мати наслідком поширення нетерпимості, ворожості, приниження гідності, дискримінації чи насильства стосовно особи чи групи осіб за захищеними ознаками. Мова ворожнечі включає заклики до дискримінації, пропаганду переваги однієї групи над іншою, дегуманізацію, а також поширення ворожих або принизливих образів» [5, с. 616].

Правове регулювання відповідальності за кримінальні правопорушення, пов'язані з мовою ворожнечі, здійснюється за ст. 161 Кримінального кодексу (далі – КК) України – порушення рівноправності громадян; ст. 300 КК України – розповсюдження творів, що пропагують насильство та жорстокість; ст. ст. 109, 110 КК України – публічні заклики до насильницької зміни влади, посягання на територіальну цілісність; ст. 436 КК України – пропаганда війни (у випадках, коли мова ненависті має форму воєнної пропаганди або підбурювання до збройного конфлікту); ст. 436-1 КК України – виготовлення, поширення комуністичної та націонал-соціалістичної (нацистської) символіки, пропаганда тоталітарних режимів (може застосовуватися, якщо мова ворожнечі пов'язана з героїзацією таких режимів або пропагандою їхніх ідеологій) [6].

Варто акцентувати увагу на тому, що запобігання й протидія мові ворожнечі та розпалюванню ненависті в соціальних мережах має складний і багатокомпонентний характер. Особливого значення в цьому процесі набуває розслідування кримінальних правопорушень цієї категорії, метою якого є притягнення винних до кримінальної відповідальності.

Цифрова природа кримінальних правопорушень, пов'язаних із розпалюванням ворожнечі та дискримінацією в соціальних мережах, зумовлює низку особливостей розслідування.

Виявлення й фіксація факту розпалювання або поширення ненависті (ворожнечі) є першим етапом розслідування. Крім звернення потерпілих до правоохоронних органів, передбачається моніторинг відкритих джерел, що здійснюється відповідними підрозділами кібербезпеки, зокрема Facebook, X (Twitter), Telegram, TikTok, YouTube, Instagram. Сервери соцмереж часто розміщені за межами України, що ускладнює оперативне отримання інформації. Тому важливо оформлювати міжнародні запити (MLAT, Interpol), використовувати канали співпраці з платформами (наприклад, Facebook Transparency Center).

При виявленні публікацій, коментарів, відео чи зображень, які можуть містити мову ненависті, контент необхідно належним чином зафіксувати шляхом створення скріншотів, відеозапису екрану, збереження метаданих (URL-адреса, дата, акаунт, IP, хештони тощо).

У контексті сучасних підходів до розслідування злочинів дедалі більшого значення набувають інструменти цифрової криміналістики, які активно використовуються як у міжнародній, так і в національній практиці. Їх застосування сприяє виявленню, фіксації та доведенню фактів злочинів, а також забезпеченню реалізації принципу невідворотності покарання. У спеціальній літературі акцент робиться на комплексному використанні таких засобів:

- пошукові механізми за ключовими словами та хештегами, списки яких формуються відповідно до тематичного чи регіонального спрямування;
- технології обробки великих даних (Big Data) для виявлення закономірностей і візуалізації інформаційних потоків;
- вивчення геолокаційної інформації, а також фото – й відеоматеріалів з відкритих джерел і цифрових платформ;
- застосування програмного забезпечення для обробки зображень і відео з метою виявлення фальсифікацій або підтвердження автентичності;
- дослідження даних з електронних пристроїв включно з аналізом збережених файлів, повідомлень, записів розмов;
- ідентифікація користувачів та об'єктів за допомогою систем розпізнавання облич, що поєднується з пошуком відповідностей у базах даних.

Ці інструменти, будучи технологічно складними, водночас відкривають нові можливості для цифрової доказової діяльності й у справах про злочини, пов'язані з мовою ворожнечі [7, с. 32].

Серед актуальних напрямів цифрово-криміналістичних досліджень також виокремлюють такі:

- аналіз даних, збережених у хмарних сховищах, зокрема виявлення, вилучення й автентифікація інформації, що міститься на зовнішніх серверах;
- дослідження мобільних пристроїв, передусім смартфонів, з метою встановлення структури даних, історії комунікацій, видалених об'єктів тощо;
- аналіз застосунків для обміну інформацією (месенджерів, соціальних мереж, програм шифрування), що використовуються з мобільних пристроїв і комп'ютерів;
- дослідження пристроїв інтернету речей (IoT) – «розумних» приладів, підключених до мережі, таких як камери відеонагляду, трекери, датчики;
- мережеві розслідування, які передбачають аналіз структури трафіку, логів доступу, IP-адрес і цифрових слідів у мережах;
- аналіз новітніх інтерактивних пристроїв і віртуальних помічників (зокрема Amazon Alexa, Google Assistant, Siri), які здатні зберігати записи голосових команд та активностей користувача;
- дослідження нестандартних джерел даних, що не пов'язані безпосередньо зі смартфонами, до них зараховують локальні й онлайн-бази даних, системи миттєвих повідомлень (наприклад, AOL IM), оперативну пам'ять (у т. ч. волатильну), сегменти даркнету, програмні засоби приховування слідів (антикриміналістики), видалені або фрагментовані файли, флеш-накопичувачі, криптовалюти тощо;
- цифровий аналіз поведінки осіб або груп, який дає змогу реконструювати їхню активність, взаємодії, соціальні зв'язки та комунікаційні шаблони;
- цифрова криміналістична розвідка включно з OSINT (розвідкою на основі відкритих джерел), що використовується для виявлення загроз, підтвердження фактів або ідентифікації суб'єктів правопорушень у відкритому інформаційному середовищі [8].

У сукупності ці напрями свідчать про комплексність цифрової криміналістики як міждисциплінарної галузі, що поєднує правову, технічну, лінгвістичну й соціальну аналітику, необхідну для ефективного розслідування злочинів у цифровому середовищі, зокрема й тих, що пов'язані з мовою ворожнечі.

Окремим етапом розслідування є *технічна ідентифікація особи*. Зважаючи на можливість використання анонімних акаунтів чи VPN, фахівцям необхідно отримати дані провайдерів (IP-адреси, час з'єднання), установити зв'язок між акаунтом і конкретною особою, зокрема через лог-файли, мобільні пристрої, електронну пошту. Також необхідно забезпечити збереження цифрових доказів, зокрема скріншоти мають бути належно оформлені, засвідчені, з фіксацією URL, часу тощо.

Крім того, варто вказати й на складність установлення й доведення мотиву ненависті, який є обов'язковим елементом складу кримінального правопорушення. Важливо не лише зафіксувати сам факт поширення образливих або закличних висловлювань, а й довести, що діяння вчинене саме з мотиву ненависті – за ознаками раси, національності, статі, мови, релігії, сексуальної орієнтації тощо. Це вимагає кропіткої роботи, а саме контекстного аналізу публікацій, з'ясування частоти й спрямованості ворожих повідомлень, вивчення профілю особи (уподобання, підписки, попередні висловлювання).

Для доведення мотиву ненависті слідчі повинні враховувати практику ЄСПЛ, яка відмежовує «захищену свободу вираження поглядів» від «мови ворожнечі», яка не підлягає захисту. Наприклад, *Sürek v. Turkey* (№ 1) (1999): справа стосувалася публікації

в курдському журналі, що містила різко налаштовану риторику проти державних органів. ЄСПЛ установив, що стаття містила підбурювання до ворожнечі між етнічними групами та виправдовувала насильство, у висновку – це мова ворожнечі, тому не підлягає захисту за ст. 10 Конвенції [9].

Féret v. Belgium (2009) – політик поширював листівки з расистськими гаслами проти мігрантів. Позиція ЄСПЛ полягала в установленні, що висловлювання мали ксенофобський і расистський характер, підбурювали до дискримінації, а тому це мова ворожнечі, не захищається Конвенцією [10].

Garaudy v. France (2003) – за суттю справи, книга заявника заперечувала Голокост і містила антисемітські твердження. Згідно з позицією ЄСПЛ, це є запереченням історичних фактів, пов'язаних зі злочинами проти людяності, не захищене правом на свободу вираження. Як висновок, подібні висловлювання випадають із захисту ст. 10 згідно зі ст. 17 (заборона зловживання правами) [11].

Le Pen v. France (2010) – Жан-Марі Ле Пен зробив публічні заяви про мусульманську громаду у Франції, звинувачуючи її в загрозі для нації. ЄСПЛ визначив, що висловлювання були провокаційними та спрямованими на розпалювання релігійної ненависті. У висновку – обмеження свободи слова було виправданим, оскільки заява підбурювала до ворожнечі [12].

Також варто акцентувати, що в кримінальних провадженнях щодо розпалювання ворожнечі, дискримінації чи закликів до насильства в соціальних мережах ключовими для належної кваліфікації діяння й обґрунтування підозри або обвинувачення є застосування спеціальних знань, *експертних досліджень*.

Через багаторівневу природу цифрових злочинів у таких справах часто признають комплексні експертизи, що охоплюють кілька галузей знань: лінгвістичну (установлення ознак мови ворожнечі, закликів до насильства), психологічну (вивчення впливу контенту на емоційно-вольову сферу споживача), авторознавчу (визначення авторства тексту чи зображення), комп'ютерно-технічну (аналіз метаданих, IP-адрес, часових міток, джерела завантаження).

Якість експертного дослідження значною мірою залежить від чітких і коректних запитань, а саме: Чи містить текст ознаки розпалювання расової, національної, релігійної ворожнечі? Чи спрямовані висловлювання на приниження гідності конкретної соціальної групи? Чи є висловлювання закликом до дискримінації? Чи належить спірний текст (пост, коментар) конкретній особі? Неправильне формулювання може призвести до неінформативного висновку або потреби в повторному призначенні.

Для передачі об'єкта на експертизу необхідно оформити цифрові докази належним чином (електронні носії, сертифіковані копії сторінок, витяги з логів); зафіксувати контекст публікації: дату, час, платформу, реакції користувачів; залучити технічного фахівця або слідчого-криміналіста для засвідчення достовірності інформації.

Не применшуючи ролі інших галузей знань, вважаємо за необхідне зупинитися на ролі саме лінгвістичної експертизи. У контексті дослідження мовного контенту, що потенційно містить ознаки протиправної поведінки, важливо розглядати такі матеріали з позицій лінгвістичної експертизи, яка спирається на методологічну базу філологічної науки, насамперед мовознавства. Саме спеціальні фахові знання в галузі лінгвістики дають змогу здійснювати поглиблений аналіз текстів з метою встановлення наявності мовленнєвих деліктів, спрямованості й функцій у конкретному комунікативному контексті, потенційного автора, особливо у випадку анонімних або екстремістських повідомлень.

Фактично лінгвістична експертиза є спеціалізованим мовознавчим дослідженням тексту або іншого мовного продукту, яке здійснюється з метою відповіді на запитання, що мають юридичне значення. Висловлене слово, незалежно від того, в усній чи письмовій формі, у певних обставинах може набувати юридично релевантного статусу, тобто розцінюватися як дія, що тягне за собою правові наслідки.

Об'єктом такого експертного дослідження є текст як елемент відповідного дискурсу, у котрому аналізуються комунікативні норми, що функціонують у межах певного соціального чи інформаційного простору. Відхилення від цих норм можуть бути інтерпретовані як правопорушення [13, с. 14].

Інакше кажучи, судова лінгвістична експертиза – це процесуально регламентоване дослідження мовленнєвих творів, що охоплює як формально-мовний, так і змістовно-смысловий рівні. Метою такого аналізу є виявлення лексичних конструкцій, стилістичних прийомів і семантичних одиниць, які можуть містити ознаки протиправного висловлювання, передбаченого конкретною нормою кримінального чи адміністративного законодавства.

В умовах все більшого значення інформаційних злочинів, особливо в цифровому середовищі, спостерігається трансформація лінгвістичної експертизи з факультативного, епізодичного інструмента в системний складник судово-експертної діяльності. Це особливо актуально в категоріях кримінальних проваджень, пов'язаних із поширенням мови ворожнечі, підбурюванням до насильства, дискримінацією, погрозами тощо, де без залучення спеціальних філологічних знань неможливо здійснити повноцінну правову оцінку текстуального доказового матеріалу [14, с. 106].

В аспекті теми дослідження доцільно визначити особливості експертного аналізу мовного контенту. Так, лінгвістична експертиза розглядає:

- лексичний склад (уживання образливих або агресивних слів);
- синтаксичні конструкції (чи мають імперативний, наказовий характер);
- стилістичні прийоми (сарказм, гіпербола, алюзії);
- контекст (попередні й наступні публікації, медійне оточення).

Варто зазначити, що не завжди володілець акаунту вказує свої персональні данні. У разі анонімного або фейкового акаунту постає завдання ідентифікації автора. Для цього призначається авторознавча експертиза. Вона дає змогу визначити стилістику викладення думки, лексичний портрет мовця, граматичні конструкції, наявні шаблони поведінки користувача в мережі. Ці дослідження мають імовірнісний характер, тому потребують ретельної аргументації.

Оскільки контент у соцмережах часто видаляється, своєчасне призначення експертизи є критичним. Слідчі мають фіксувати цифрові докази невідкладно та не зволікати з передачею матеріалів експертам.

В Україні проведення таких експертиз успішно виконуються низкою експертних установ, серед яких – експертні підрозділи МВС, науково-дослідні установи судових експертиз Мін'юсту, приватні експерти, які мають відповідну кваліфікацію й ліцензії. Співпраця слідчих з експертами повинна бути злагодженою, з дотриманням процесуальних гарантій і конфіденційності.

Цікаво, що в Україні спостерігається зростання кількості вироків за злочини, пов'язані з розпалюванням ворожнечі й дискримінацією. Зокрема, у період з 2019 по 2024 рік винесено 45 обвинувальних вироків за статтею 161 КК України. Однак практика розслідування таких злочинів залишається вибірковою та нерівномірною [15].

Так, Городищенським районним судом (справа від 17.06.2024 № 119795552) обвинувачений був визнаний винним за ч. 1 ст. 161 КК України за умисні дії, спрямовані на

розпалювання національної, расової ворожнечі й ненависті, приниження національної честі й гідності [16].

Київський окружний адміністративний суд (справа від 26.08.2024 № 640/16009/21) у рішенні зазначив, що порівняння Президента України з Гітлером у виступі є закликом до ненависті на національному ґрунті й розпалюванням ворожнечі [17].

Берегівський районний суд (справа від 09.09.2019 № 297/1874/19) визнав наявність ознак порушення рівноправності громадян залежно від їхньої расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками, що підпадає під ч. 1 ст. 161 КК України [18].

Довгинцівський районний суд міста Кривого Рогу Дніпропетровської області визнав винною особу в учиненні кримінального правопорушення, передбаченого ч. 1 ст. 161 КК України, а саме умисні дії, спрямовані на розпалювання національної, релігійної ворожнечі та ненависті, на приниження національної честі й гідності, образа почуттів громадян у зв'язку з їхніми релігійними переконаннями через розміщення дописів у «Facebook» [19].

Аналізуючи судову практику, можемо зробити висновок, що при розслідуванні злочинів цієї категорії існує низка проблем, а саме:

- труднощі в доведенні мотиву ненависті й дискримінації, що ускладнює правильну кваліфікацію злочинів за ст. 161 КК України;
- відсутність належного документування та фіксації цифрових доказів може призвести до виправдувальних вироків або закриття справ;
- суди стикаються з викликами у визначенні меж між допустимими висловлюваннями й тими, що підпадають під кримінальну відповідальність. Дослідження означених проблем стане предметом окремої наукової роботи.

Висновки. Дослідження дало змогу виявити й конкретизувати основні особливості розслідування кримінальних правопорушень, пов'язаних із використанням мови ворожнечі в цифровому просторі. Поширення мови ненависті в інтернеті, особливо в соціальних мережах, вимагає комплексного реагування правоохоронних органів із поєднанням інструментів цифрової криміналістики, судової експертизи та дієвих правових механізмів. У ході роботи ми виокремили ознаки мови ворожнечі як окремого виду мовленнєвого делікту в умовах цифрового середовища; визначили актуальні положення кримінального законодавства України щодо відповідальності за такі діяння, урахувавши практику ЄСПЛ; охарактеризували методи ідентифікації правопорушників, які діють через анонімні чи фейкові акаунти; обґрунтували роль лінгвістичної, психологічної та комп'ютерно-технічної експертизи в доведенні мотиву ворожнечі.

На основі результатів дослідження можна зробити висновок про необхідність, по-перше, удосконалення кримінально-правових норм, що встановлюють відповідальність за кримінальні правопорушення цієї категорії, по-друге, оновлення (розроблення, удосконалення) інструкцій для слідчих та експертів, які працюють із цифровими доказами; по-третє, вироблення, розвитку єдиних підходів до юридичної інтерпретації мови ворожнечі.

З огляду на визначені проблеми, подальші наукові розвідки щодо особливостей розслідування мови ворожнечі в цифровому просторі доцільно спрямувати на таке:

- розроблення стандартів судово-лінгвістичної експертизи для ідентифікації мови ненависті;
- удосконалення нормативного регулювання у сфері OSINT і цифрової розвідки;
- поглиблений аналіз взаємозв'язку між свободою слова й заборонаю мови ворожнечі з урахуванням судової практики України та ЄСПЛ.

Використані джерела:

1. Конвенція про захист прав та основоположних свобод від 04.11.1950. *Офіційний вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 26.07.2025).
2. Recommendation CM/Rec(2022)16[1] of the Committee of Ministers to member States on combating hate speech. *Офіційний вебпортал Комітету Міністрів Ради Європи*. URL: <https://search.coe.int/cm?i=0900001680a67955> (дата звернення: 26.07.2025).
3. Рекомендація № R (97) 20 Комітету Міністрів державам-членам щодо «мови ненависті». *Офіційний вебпортал Комітету Міністрів Ради Європи*. URL: Recommendation No. R (97) 20 of the Committee of Ministers to member states on “hate speech” – Freedom of Expression (дата звернення: 26.07.2025).
4. Офіційний сайт Національної поліції України : веб-сайт. URL: <https://npu.gov.ua/> (дата звернення: 26.07.2025).
5. Коваль А. А. Толерантність онлайн: проблеми дотримання прав людини в соціальних мережах та правові шляхи їх вирішення. *Національні інтереси України*. 2025. № 5(10). С. 609–620. DOI: [https://doi.org/10.52058/3041-1793-2025-5\(10\)-609-619](https://doi.org/10.52058/3041-1793-2025-5(10)-609-619).
6. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.
7. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika*. 2022. Т. 18. С. 31–37.
8. Reedy P. Interpol review of digitalevidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520.
9. Case of Sürek v. Turkey (№ 1). *Official website of the ECHR*. URL: <https://hudoc.echr.coe.int/eng?i=001-58279> (дата звернення: 26.07.2025).
10. Case Féret v. Belgium. *Official website of the ECHR*. URL: <https://hudoc.echr.coe.int/eng?i=002-1407> (дата звернення: 26.07.2025).
11. Case Garaudy v. France. *Official website of the ECHR*. URL: <https://hudoc.echr.coe.int/eng?i=001-183928> (дата звернення: 26.07.2025).
12. Case Le Pen v. France. *Official website of the ECHR*. URL: <https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-3117124-3455760&filename=003-3117124-3455760.pdf> (дата звернення: 26.07.2025).
13. Ажнюк Л. В. Лінгвістична експертиза як юридичний інструмент. *Магістеріум. Серія «Мовознавчі студії»*. 2017. Вип. 66. С. 8–15.
14. Черняк А. М. Використання спеціальних знань при дослідженні текстів, із закликами до підриву конституційного ладу, порушення територіальної цілісності і недоторканості України. *Вісник кримінального судочинства*. 2022. № 3–4. С. 101–111.
15. Єдиний державний реєстр судових рішень : веб-сайт. URL: <https://reyestr.court.gov.ua/> (дата звернення: 26.07.2025).
16. Вирок № 119795552, 17.06.2024, Городищенський районний суд Черкаської області : веб-сайт. URL: <https://youcontrol.com.ua/catalog/court-document/119795552/> (дата звернення: 26.07.2025).
17. Рішення від 26.08.2024 по справі № 640/16009/21, Київський окружний адміністративний суд : веб-сайт. URL: <https://zakononline.com.ua/court-decisions/show/121199659> (дата звернення: 26.07.2025).
18. Ухвала від 08.09.2019 № 297/1874/19 Березівського районного суду : веб-сайт. URL: <https://verdictum.ligazakon.net/document/84309628> (дата звернення: 26.07.2025).
19. Справа № 211/3238/24. Провадження № 1-кп/211/482/24 від 29 травня 2024 року : веб-сайт. URL: <https://opendatobot.ua/court/119345418-814bd40113be14599d53c3906686da8d> (дата звернення: 26.07.2025).

References:

1. Konventsiiia pro zakhyst prav ta osnovopolozhnykh svobod [Convention for the Protection of Human Rights and Fundamental Freedoms] (1950, November, 4). Retrieved from: https://zakon.rada.gov.ua/laws/show/995_004#Text [in Ukrainian].
2. Recommendation CM/Rec(2022)16[1] of the Committee of Ministers to member States on combating hate speech. Retrieved from: <https://search.coe.int/cm?i=0900001680a67955> [in English].

3. Rekomendatsiia № R (97) 20 Komitetu Ministriv derzhavam-chlenam shchodo «movy nenavy-sti» [Recommendation № R (97) 20 of the Committee of Ministers to member states on «hate speech»]. Retrieved from Recommendation No. R (97) 20 of the Committee of Ministers to member states on «hate speech» – Freedom of Expression.
4. Ofitsiyni sait Natsionalnoi politzii Ukrainy. [Official website of the National Police of Ukraine]. npu.gov.ua/. Retrieved from: <https://npu.gov.ua/>.
5. Koval, A. A. (2025). Tolerantnist onlain: problemy dotrymannia prav liudyny v sotsialnykh merezhakh ta pravovi shliakhy yikh vyryshennia. [Tolerance online: problems of human rights obser-vance in social media and legal solutions]. *Natsionalni interesy Ukrainy – National Interests of Ukraine*. № 5(10). 609–620 [in Ukrainian].
6. Kryminalnyi kodeks Ukrainy pryiniaty 05.04.2001 r. № 2341-III. [Criminal Code of Ukraine from 05.04.2001 № 2341-III]. Vidomosti Verkhovnoi Rady Ukrainy – Info from the Verkhovna Rada of Ukraine. № 25–26. St. 131.
7. Latysh, K. (2022) Tsyfrova kryminalistyka u period viiny v Ukraini: mozhlyvosti vykorystannia spetsialnykh znan u sferi informatsiynykh tekhnolohii. [Digital forensics during the war in Ukraine: opportunities for using specialised knowledge in the field of information technology]. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika – Criminalistics and forensic science: science, studies, practice*. XVIII. T. 18. 31–37 [in Ukrainian].
8. Reedy P. (2020). Interpol review of digital evidence 2016–2019. *Forensic Science International: Synergy*. Vol. 2. 489–520 [in English].
9. Case of Sürek v. Turkey (№ 1). Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-58279> [in English].
10. Case Féret v. Belgium. Retrieved from: <https://hudoc.echr.coe.int/eng?i=002-1407> [in Eng-lish].
11. Case Garaudy v. France. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-183928> [in English].
12. Case Le Pen v. France. Retrieved from: [https://hudoc.echr.coe.int/app/conversion/pdf/?li-brary=ECHR&id=003-3117124-3455760&filename=003-3117124-3455760.pdf](https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-3117124-3455760&filename=003-3117124-3455760.pdf) [in English].
13. Azhniuk, L. (2017). Linhvistychna ekspertyza yak yurydychnyi instrument [Linguistic expertise as a legal tool]. *Mahisterium. Movoznavochi studii – Magisterium. Linguistic Studies*. № 66. 8 [in Ukrainian].
14. Cherniak, A. M. (2022). Vykorystannia spetsialnykh znan pry doslidzhenni tekstiv, iz zak-lykamy do pidryvu konstytutsiinoho ladu, porushennia terytorialnoi tsilisnosti i nedotorkanosti Ukrainy. [Use of special knowledge in the investigation of texts containing calls to undermine the constitutional order, violate the territorial integrity and sovereignty of Ukraine]. *Visnyk kryminalnoho sudochynstva – Criminal Justice Bulletin*. № 3–4. 101–111 [in Ukrainian].
15. Yedynyi derzhavnyi reistr sudovykh rishen. [The Unified State Register of Court Decisions]. Reyestr.court.gov.ua. Retrieved from: <https://reyestr.court.gov.ua/> [in Ukrainian].
16. Vyrok № 119795552, 17.06.2024, Horodyschenskyi raionnyi sud Cherkaskoi oblasti. 16. [Judg-ment № 119795552, 17 June 2024, Gorodishche District Court of Cherkasy Region]. Retrieved from: <https://youcontrol.com.ua/catalog/court-document/119795552/> [in Ukrainian].
17. Rishennia vid 26.08.2024 po spravi № 640/16009/21 Kyivskiy okruzhnyi administratyvnyi sud. [Decision of 26 August 2024 in case No. 640/16009/21 Kyiv District Administrative Court]. Retrieved from: <https://zakononline.com.ua/court-decisions/show/121199659> [in Ukrainian].
18. Ukhvala vid 08.09.2019 № 297/1874/19 Berehivskoho raionnoho sudu. [Decision No. 297/1874/19 of 08.09.2019 of the Berehove District Court]. Retrieved from: <https://verdictum.ligazakon.net/document/84309628> [in Ukrainian].
19. Sprava № 211/3238/24. Provadzhennia № 1-kp/211/482/24 vid 29 travnia 2024 roku. [Case № 211/3238/24. Proceedings № 1-kp/211/482/24 dated 29 May 2024]. Retrieved from: <https://opendatabot.ua/court/119345418-814bd40113be14599d53c3906686da8d> [in Ukrainian].

Стаття надійшла до редколегії 29.07.2025
Стаття рекомендована до друку 20.08.2025
Опублікована 12.11.2025

Koval A., Doctor of Law, Professor, Head of the Department of Constitutional and Administrative Law and Procedure, Petro Mohyla Black Sea National University (Mykolaiv, Ukraine)

Petrenko K., Attorney, Attorney Association "Aktum" (Lviv, Ukraine)

HATE SPEECH IN DIGITAL SPACE: SPECIFIC FEATURES OF THE INVESTIGATION

The article analyzes the specific features of investigating criminal offenses related to the dissemination of hate speech in the digital environment, particularly on social media platforms. It defines hate speech online as public expressions aimed at humiliating human dignity, inciting discrimination, or stirring hatred against individuals or groups based on race, nationality, language, religion, gender, and other characteristics. The article emphasizes that the prevention and counteraction of hate speech and incitement to hatred on social networks is a complex and multifaceted task. Special attention is given to the investigation of such criminal offenses, with the primary goal of bringing perpetrators to justice.

Given the digital nature of these offenses, the study highlights the evidentiary challenges, the necessity of employing tools of digital forensics, and the importance of an interdisciplinary approach. The article examines the legal classification of such acts under the Criminal Code of Ukraine and presents examples of judicial practice. Particular focus is placed on the role of forensic examinations – linguistic, psychological, and computer-technical – in establishing the motive of hatred and identifying offenders. It further explores methods of detecting digital traces, collecting evidence, and addressing issues of anonymity and limited access to social media servers.

The article also outlines key areas of digital forensics applied in such investigations, including the analysis of mobile devices, cloud storage, messaging applications, social media platforms, geolocation data, and patterns of digital behavior. The author stresses the importance of involving digital analysts and OSINT specialists, whose expertise significantly enhances the detection of offenses within the context of information threats. The article also presents relevant case law of the European Court of Human Rights (ECtHR) concerning the boundaries between freedom of expression and hate speech. Approaches for improving forensic and investigative practices are proposed.

Keywords: hate speech, discrimination, liability, criminal offenses, investigation, forensic examination, expert, digital forensics.