УДК [343.1+355.40]:004(477)
DOI: https://doi.org/10.24144/2307-3322.2026.94.3.44

ВИКОРИСТАННЯ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ OSINT У ПРОТИДІЇ КОЛАБОРАЦІЙНІЙ ДІЯЛЬНОСТІ: ОКРЕМІ АСПЕКТИ

Рибка Д.,
доктор філософії,
старший викладач НА СБУ
ORCID: 0000-0002-8824-0089

Рибка Д. Використання Службою безпеки України OSINT у протидії колабораційній діяльності: окремі аспекти.

В науковій статті розглядаються актуальні питання використання методів та інструментів OSINT для отримання доказів у кримінальних провадженнях щодо колабораційної діяльності як одного з напрямів протидії Службою безпеки України цьому кримінальному правопорушенню.

Відзначено, що суб'єкти колабораційної діяльності досить часто залишають сліди своєї кримінально-протиправної діяльності у цифровому середовищі (соціальних мережах, групових чатах месенджерів, веб-сайтах тощо). Тому сучасні технології OSINT надають широкі можливості уповноваженим державним органам виявляти та накопичувати великий обсяг фактичних даних про особу колаборанта та обставини вчинення ним колабораційної діяльності, які матимуть доказове значення у кримінальному провадженні.

Привернено увагу на складнощі використання OSINT-даних у доказуванні, обумовлені вразливістю цифрової інформації до фальсифікації і нестабільністю доступності інформації в Інтернеті. Наголошено на тому, що при роботі з цифровою інформацією з відкритих джерел необхідно обирати вірний підхід до фіксування та збереження OSINT-даних, який дозволить суду безпосередньо дослідити такі дані під час судового розгляду. Підкреслено важливість використання уповноваженими державними органами новітніх цифрових технологій, придатних для перевірки, інтерпретації, аналізу та збереження OSINT-даних. Зазначено, що є потреба у підвищенні обізнаності оперативних співробітників, слідчих, прокурорів, суддів як щодо юридичних, так й інформаційно-технологічних аспектів використання цифрової інформації у доказуванні.

Висловлена думка, що для підвищення ефективності використання технології OSINT у доказуванні існує нагальна потреба у впровадженні якісної правової моделі електронних (цифрових) доказів та процесуального порядку поводження з ними. Ця модель має ґрунтуватися на узгоджених доктринальних положеннях кримінального процесу, відповідати потребам юридичної практики та водночас враховувати як сучасний рівень, так і потенційні можливості інформаційних технологій.

Ключові слова: протидія колабораційній діяльності, OSINT, електронні докази, доказування, Протокол Берклі, розслідування, національна безпека.

Rybka D. Use of OSINT by the Security Service of Ukraine in collaborationist activities countering: certain aspects.

This scientific article examines current issues regarding the use of Open Source Intelligence (OSINT) methods and tools to obtain evidence in criminal proceedings related to collaborative activities, as one of the areas of the Security Service of Ukraine's counteraction to this criminal offense.

It is noted that subjects of collaborative activities frequently leave traces of their criminal conduct in the digital environment (social networks, group chats in messengers, websites, etc.). Therefore, modern OSINT technologies provide extensive opportunities for authorized state bodies to identify and accumulate a vast amount of factual data regarding the collaborator's identity and the circumstances of their collaborative activities, which will have evidentiary value in criminal proceedings.

Attention is drawn to the difficulties of using OSINT data in the process of proving, caused by the vulnerability of digital information to falsification and the instability of information accessibility on the Internet. It is emphasized that when working with digital information from open sources, it is necessary to choose the correct approach for recording and preserving OSINT data, which would allow

the court to directly examine such data during trial. The importance of the use of state-of-the-art digital technologies by authorized state bodies for the verification, interpretation, analysis, and preservation of OSINT data is highlighted. It is noted that there is a need to increase the awareness of operational officers, investigators, prosecutors, and judges regarding both the legal and information-technology aspects of using digital information in proving.

The opinion is expressed that to improve the efficiency of using OSINT technology in proving, there is an urgent need to implement a high-quality legal model for electronic (digital) evidence and the procedural order for its handling. This model should be based on consistent doctrinal provisions of the criminal process, meet the needs of legal practice, and simultaneously account for both the current state and potential capabilities of information technologies.

Key words: countering collaborative activity, OSINT, electronic evidence, proving, Berkeley Protocol, investigation, national security.

Постановка проблеми. З початком широкомасштабної збройної агресії проти України перед нашою країною постали нові виклики, пов'язані з наданням належної правової оцінки суспільно небезпечним проявам співпраці громадян України з державою-агресором, а також забезпеченням виявлення, припинення та розкриття такого роду діянь. Одним з перших кроків на шляху до подолання цих викликів стало прийняття Закону України від 03 березня 2022 року № 2108-IX, яким кримінальні правопорушення проти основ національної безпеки було доповнено ст. 111-1 Кримінального кодексу України (Колабораційна діяльність). Це дозволило уповноваженим державним органам надавати кримінально-правову оцінку найбільш суспільно-небезпечним формам співпраці колаборантів з ворогом. Враховуючи, що суб'єкти колабораційної діяльності досить часто залишають сліди своєї кримінально-протиправної діяльності у цифровому середовищі (соціальних мережах, групових чатах месенджерів, веб-сайтах тощо), сучасні технології OSINT надають широкі можливості з виявлення ознак колабораційної діяльності, ідентифікації осіб, які її вчинили, а також встановлення інших обставин, що мають значення для протидії цьому виду кримінальних правопорушень, у тому числі для ефективного здійснення кримінального провадження.

Проте, недосконаліть доктринальних й нормативно-правових положень з питань використання у кримінальному процесуальному доказуванні інформації, що існує у цифровій (електронній) формі, негативно позначається на ефективності притягнення колаборантів до кримінальної відповідальності.

Виходячи з викладеного, **метою наукової статті є** привернення уваги на окремі питання використання органами безпеки технології OSINT для отримання інформації, що має доказове значення у кримінальних провадженнях за ознаками колабораційної діяльності як одного з напрямів протидії цьому виду кримінальних правопорушень.

Аналіз останніх досліджень і публікацій. Проблематику документування та розслідування колабораційної діяльності досліджували А. Берташ, В. Бондар, Т. Вайда, В. Вигівський, О. Гарасимів, Б. Гарасимів, С. Головкін, Н. Гольдберг, С. Гусаров, Б. Кіщак, А. Мальгіна, А. Коваленко, Д. Лісніченко, М. Пашковський, О. Ряшко та інші.

Окремі питання, пов'язані з цифровими (електронними) доказами, а також використанням технології OSINT у кримінальному провадженні висвітлювали Н. Ахтирська, П. Антонюк, Д. Алєксєєва-Процюк, І. Басиста, Л. Гаврилюк, О. Гарасимів, Н. Глинська, А. Гутник, М. Гуцалюк, Д. Клепка, А. Коваленко, І. Крицька, О. Малахова, С. Марко, О. Метелев, В. Михайлов, М. Погорецький, А. Ратнова, Ю. Рєпіна, О. Ряшко А. Скрипник, А. Столітній, Д. Цехан, А. Хитра, М. Шумило та багато інших.

Водночас, неузгодженість доктринальних позицій щодо електронних (цифрових) доказів, в тому числі отриманих за допомогою OSINT, а також відсутність уніфікованого стандарту поводження з такими доказами у кримінальному провадженні спонукає до наукового пошуку шляхів удосконалення практики використання OSINT у протидії колабораційній діяльності.

Виклад основного матеріалу. У відповідності до визначених законом завдань, одним з обов'язків, покладених на Службу безпеки України є виявлення, припинення та розкриття кримінальних правопорушень, розслідування яких віднесено законодавством до її компетенції. Відповідно до ч. 2ст. 216 КПК України досудове розслідування кримінальних правопорушень, передбачених ст. 111-1 КК України (Колабораційна діяльність), як правило, здійснюють слідчі підрозділи органів безпеки. Зокрема, за даними Єдиного звіту про кримінальні правопорушення Офісу

Генерального прокурора у 2023 році органами безпеки за ст. 111-1 КК України здійснювалось досудове розслідування у 2320 кримінальних провадженнях, з яких 702 направлено до суду з обвинувальним актом [1], у 2024 році органи безпеки розслідували 1789 кримінальних проваджень з вказаною кваліфікацію, з яких до суду з обвинувальним актом було передано 644 [2], у першому півріччі 2025 року ці показники становили 1073 кримінальних провадження, з яких 213 направлено до суду з обвинувальним актом [3].

Тенденцію до зростання також має кількість вироків, винесених національними судами по першій інстанції щодо осіб, обвинувачених у вчиненні колабораційної діяльності: у 2022 році – 266 вироків, у 2023 році – 801 вирок, у 2024 році – 1107 вироків, за 9 місяців 2025 року – 911 вироків [4].

Під час розслідування колабораційної діяльності доволі типовою є ситуація, коли для встановлення обставин вчинення цього кримінального правопорушення слідчі складають протоколи оглядів інформації, що міститься у відкритому доступі в мережі Інтернет. В подальшому ці протоколи використовуються стороною обвинувачення у суді як доказ.

Наприклад, вироком Солом`янського районного суду м. Києва від 05.12.2024 р. громадянка України, яка "з метою впровадження стандартів освіти держави-агресора у закладах освіти на захоплених рф територіях Херсонської обл., перебуваючи на посаді директора, запровадила в Херсонському обласному училище культури та мистецтв навчальні програми держави-агресора та побудувала навчальний процес на основі підручників держави агресора, отриманих в окупаційної адміністрації держави-агресора, за стандартами освіти держави-агресора з загальним застосуванням російської мови та забезпечила видачу вказаних підручників учням для здійснення навчання за освітньою програмою рф" [5], була визнана винуватою у вчиненні кримінального правопорушення, передбаченого ч. 3 ст. 111-1 КК України (кримінальна справа № 760/29168/23 1-кп/760/3000/24). Одним з доказів вини цієї особи суд визнав дані протоколу огляду від 14.07.2022, згідно яких "в ході огляду веб-сторінки ІНФОРМАЦІЯ_2, виявлений телеграм-канал під назвою: ІНФОРМАЦІЯ_3, на якому висвітлено, що «ОСОБА_3 ІНФОРМАЦІЯ_1, назначена директором музучилища культури і мистецтва від окупаційної влади" [5].

В іншому кримінальному провадженні по обвинуваченню громадянина України у вчиненні кримінального правопорушення, передбаченого ч. 4 ст. 111 - 1 КК України, Херсонський міський суд Херсонської області одними з доказів провадження обвинуваченим господарської діяльності у взаємодії з незаконними органами влади, створеними на тимчасово окупованій території м. Херсон Херсонської області визнав: протокол огляду від 18.03.2023 зі скріншотами, відповідно до якого здійснено огляд веб-сторінок у мережі Інтернет відносно обвинуваченого; протокол огляду від 04.07.2023, відповідно до якого об`єктом огляду є посилання сайту, за яким розміщено канал з відео файлами, що підтверджують обставини вчинення обвинуваченим інкримінованого йому злочину [6].

Враховуючи реалії слідчо-судової практики розслідування колабораційної діяльності, науковцями привертається увага на те, що електронні (цифрові) сліди є характерними для колабораціонізму [7], "значна частина доказів вчинення даного злочину, як правило, представлена в електронній формі та є електронними відображеннями" [8], а "відкриті джерела є одним із інструментів збору інформації про такі кримінальні правопорушення" [9]. Погоджуємося з висловленою в наукових джерелах думкою, що дієвими методами документування та розслідування окремих форм цього кримінального правопорушення є: "аналіз та синтез інформаційної бази, що міститься у відкритій мережі Інтернет, зокрема акаунтів у соціальних сторінках осіб, яких підозрюють в участі у незаконних злочинних об'єднаннях... фіксація та систематизація доступних фактів (дій, діяльності) підозрюваних осіб у ЗМІ, в тому числі в інтернет-ресурсах, на місцевому телебаченні тощо; ... аналіз ЗМІ країни-терориста щодо висвітлення стану справ на окупованих територіях" [10, 11]. Це дозволяє встановити обставини, що можуть свідчити про вчинення конкретною особою колабораційної діяльності і стати підставою для початку досудового розслідування у порядку ст. 214 КПК України, а так само обставини, які згідно зі ст. 91 КПК України підлягатимуть доказуванню у кримінальному провадженні щодо колабораційної діяльності. Наприклад, такі, як зайняття посади в адміністративному органі окупаційної влади; здійснення особою господарської діяльності у взаємодії з державою-агресором та її незаконними органами влади; пособництво в організації та проведенні незаконних виборів на тимчасово окупованій території; здійснення інформаційної діяльності, спрямованої на підтримку рішень та/або дій держави-агресора, її зброй-

них формувань, окупаційної влади; участь особи в незаконних збройних чи воєнізованих формуваннях, створених на тимчасово окупованій території та ін.

Отже, з одного боку, використання технології OSINT для пошуку й вивчення інформації, розміщеної на каналах та у відкритих групах месенджерів, на веб-сайтах, сторінках в соціальних мережах, інших інформаційних інтернет-ресурсах, дозволяє уповноваженим державним органам виявляти та накопичувати великий обсяг фактичних даних про особу колаборанта, які матимуть доказове значення у кримінальних провадженнях щодо колабораційної діяльності. З іншого боку, міжнародні експерти привертають увагу на те що "нові загрози, спричинені дезінформацією та досягненнями технології діпфейку" можуть призвести до суттєвого зниження рівня довіри до доказів з відкритих джерелах, що використовуються у процедурах із притягнення до відповідальності [12]. Представники національного суддівського корпусу також зазначають, що докази, отримані з відкритих джерел мають свою специфіку [13], під час їх аналізу "можуть виникати проблеми з первинними даними, з їх дійсністю чи фальсифікацією" [12]. І оскільки "крапку в кожному кримінальному провадженні ставить суд, тому саме судді повинні розуміти походження таких доказів, наскільки їм можна довіряти і як їх перевірити" [13]. Вважаємо, що кваліфікований підхід до розуміння походження доказів з відкритих джерел має бути не тільки у суддів, але й у слідчих, прокурорів та співробітників уповноважених оперативних підрозділів органів безпеки, які в межах своєї компетенції здійснюють виявлення, припинення та розкриття колабораційної діяльності.

В більшості випадків OSINT-інформація про колабораційну діяльність та причетних до неї осіб, отримується уповноваженими оперативними підрозділами Служби безпеки України в електронній (цифровій) формі. Обов'язковою умовою використання такої інформації у кримінальному процесуальному доказуванні є її відповідність законодавчо визначеним ознакам доказів, а саме: належності, допустимості, достовірності й достатності. На відміну від цивільного, господарського та адміністративного судочинства України, в КПК України не передбачені окремі спеціальні правові норми, які б визначали поняття електронних доказів та їх джерел, а також особливості порядку їх збирання, перевірки й оцінки. При цьому, у доктрині кримінального процесу відсутня узгоджена наукова позиція щодо доцільності їх впровадження. Наприклад, А. Столітній та І. Каланча не вважають "електронні докази" новим процесуальним джерелом доказів, але допускають, що розвиток інформаційних технологій в подальшому потребуватиме внесення змін до кримінального процесуального закону щодо впровадження електронних джерел доказів, а також способу їх отримання, фіксації, зберігання та використання [14, с. 182-188]. Натомість М. Шумило, Р. Юрка Р., В. Капліна слушно наголошують, що "очевидною постає необхідність вдосконалення правового визначення поняття доказів у кримінальному провадженні із урахуванням специфіки цифрової інформації, а також нормативного закріплення спеціального режиму її використання та перевірки [15, с. 143]. Про наявність складнощів з процесуальним збором цифрової інформації, вирішення яких потребує внесення відповідних змін до кримінального процесуального законодавства, зазначають й інші науковці в галузі кримінального процесу та криміналістики [16, с. 162; 17, с. 51; 18, с. 232-238].

В цілому підтримуючи наведені наукові позиції, вважаємо, що є нагальна потреба у впровадженні якісної правової моделі електронних (цифрових) доказів та процесуального порядку поводження з ними, яка б ґрунтувалася на узгоджених доктринальних положеннях кримінального процесу, відповідала потребам юридичної практики та водночас враховувала як сучасний рівень, так і потенційні можливості інформаційних технологій.

Недосконаліть доктринальної та правової моделей використання у кримінальному процесуальному доказуванні цифрової інформації на практиці здебільшого компенсується застосуванням принципів та стандартів, визначених у Протоколі Берклі. Цей документ має рекомендаційний характер, не є джерелом кримінального процесуального права і не підміняє собою норми КПК України. Викладені у ньому положення про методи й процедури збирання, зберігання, аналізу і перевірки цифрової інформації не розкривають конкретний інструментарій пошуку й формування доказів (назви технічних засобів, програмних продуктів, конкретних процесуальних дій тощо), проте враховують, що кримінальне розслідування відрізняється "більш високим стандартом доказування та більш жорсткими правилами процедури та доказування, включаючи допустимість, з метою захисту належного процесу та прав на справедливий судовий розгляд будь-яких обвинувачених" [19, с. 47]. Отже, дотримання викладених у Протоколі Берклі принципів та стандартів

проведення розслідувань дозволяє мінімізувати процесуальний ризик визнання недопустимим доказом цифрової інформації, отриманої з відкритих джерел. Це слід враховувати співробітникам уповноважених оперативних підрозділів Служби безпеки України, які здійснюють пошукову діяльність із використанням відкритих інтернет-джерел, адже прогнозованим результатом OSINT є отримання процесуально значимих відомостей, що в подальшому можуть бути використані для прийняття рішення про початок кримінального провадження та/або формування доказів.

Окремо слід привернути увагу на складнощі використання OSINT-даних у доказуванні, викликані вразливістю цифрової інформації до фальсифікації і нестабільністю доступності інформації в Інтернеті. Зазначене обумовлює потребу у застосуванні сучасного програмного забезпечення для розпізнавання обличчя, голосу, встановлення геолокації, а також інших новітніх цифрових технологій, придатних для перевірки, інтерпретації, аналізу та збереження OSINT-даних, які не завжди є на озброєнні у правоохоронних органів, а крім цього можуть потребувати від співробітників оперативних та слідчих підрозділів спеціальних знань для їх ефективного використання. При цьому, не менш важливим є й обрання OSINT-шукачем вірного підходу до роботи із відкритим ітернет-джерелом, який забезпечить дотримання вимог ст. 23 КПК України під час судового провадження, а саме дозволить суду безпосередньо дослідити джерело цифрових фактичних даних для встановлення його придатності бути судовим доказом.

Науковці та судді вже привернули увагу на існування проблеми неналежної архівації даних, що містяться у відкритих джерелах, наслідком якої є неможливість здійснити перехід за зазначеним в процесуальних документах інтернет-посиланням або неможливість ознайомитися з тією версією інформації, яка була зафіксована під час досудового розслідування в процесуальних документах (наприклад, протоколах оглядів та додатках до них) [18, с. 234-235].

Зважаючи на це, міжнародні експерти слушно наголошують на тому, що “важливо отримати відповідне програмне забезпечення, необхідне для перевірки та автентифікації цифрових доказів” [20, с. 4], а також встановити робочі відносини “з компаніями соціальних мереж з метою відновлення цифрових доказів, які в іншому випадку можуть бути видалені на підставі видалення вмісту, що сприяє екстремізму” [20, с. 4].

У зв’язку з викладеним вище, в контексті досліджуваної авторами проблематики актуалізується питання підвищення кваліфікації суддів, слідчих, прокурорів та оперативних співробітників не тільки щодо юридичних особливостей використання цифрової інформації у кримінальних провадженнях, але й за напрямом застосування ними сучасних інформаційних технологій для роботи з такою інформацію.

Висновок. Підсумовуючи викладене, слід зазначити: виконання Службою безпеки України завдання з протидії колаборaційній діяльності потребує застосування комплексу сучасних методів і інструментів для пошуку, збереження та аналізу цифрової інформації з відкритих джерел.

Вразливість цифрової інформації до фальсифікацій, нестабільність її доступності в Інтернеті ускладнюють перевірку, інтерпретацію, аналіз і збереження OSINT-даних, що обумовлює необхідність застосування уповноваженими державними органами сучасного програмного забезпечення та потребує розуміння слідчими, прокурорами, оперативними співробітниками та суддями як юридичних, так і інформаційно-технологічних аспектів використання цифрової інформації у доказуванні.

Використання OSINT-даних у кримінальному провадженні має специфіку, яка не повною мірою врахована у нормах чинного КПК України. Удосконалення правової регламентації використання у кримінальному процесуальному доказуванні цифрової інформації дозволить мінімізувати процесуальні ризики визнання OSINT-даних недопустимими доказами, що у свою чергу сприятиме протидії органами безпеки колаборaційній діяльності.

Впровадження якісної правової моделі використання цифрової інформації у кримінальному провадженні має ґрунтуватися на узгоджених доктринальних положеннях теорії доказів, відповідати потребам сучасної юридичної практики та водночас враховувати сучасний рівень і потенційні можливості інформаційних технологій.

Враховуючи, що сучасні технології OSINT надають широкі можливості для збирання, зберігання та використання інформації про особисте життя людини, актуальним напрямом подальших наукових розвідок може стати дослідження стану дотримання права на приватність та ризиків для захисту персональних даних під час використання інструментів та методів OSINT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Єдиний звіт про кримінальні правопорушення. Січень – грудень 2023. *Офіс Генерального прокурора.* URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=241804.
2. Єдиний звіт про кримінальні правопорушення. Січень – грудень 2024. *Офіс Генерального прокурора.* URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=260042.
3. Єдиний звіт про кримінальні правопорушення. Січень – серпень 2025. *Офіс Генерального прокурора.* URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=272911.
4. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua.
5. Вирок Солом`янського районного суду м. Києва від 05.12.2024 у справі № 760/29168/23 1-кп/760/3000/24. *Єдиний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/124253478.
6. Вирок Херсонського міського суду Херсонської області від 14.01.2025 у справі № 766/6653/23 н/п 1-кп/766/773/25. *Єдиний реєстр судових рішень. URL:* https://reyestr.court.gov.ua/Review/124455855.
7. Гусаров С.М. Використання інформації з відкритих джерел при розслідуванні колабораційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму в період воєнного стану:* матеріали Всеукраїнської науково-практичної конференції, м. Одеса, 09 серпня 2024 р. Одеса: ОДУВС, 2024. С. 198-200. URL: https://www.researchgate.net/profile/Anna-Politova-2/publication/383158882_Politova_AS_Kriminalna_vidpovidalnist_za_kolaboracijnu_dialnist_zdobuvaciv_osviti_Aktualni_pitanna_kriminalno-pravovoi_kvalifikacii_dokumentuvanna_ta_rozsliduvanna_kolaboracionizmu_v_period_voennogo_s/links/66bf4cdd8d007355925978d4/Politova-AS-Kriminalna-vidpovidalnist-za-kolaboracijnu-dialnist-zdobuvaciv-osviti-Aktualni-pitanna-kriminalno-pravovoi-kvalifikacii-dokumentuvanna-ta-rozsliduvanna-kolaboracionizmu-v-period-voennogo.pdf.
8. Янковий М.О. До питання про слідову картину колабораційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму в період воєнного стану:* матеріали Всеукраїнської науково-практичної конференції, м. Одеса, 09 серпня 2024 р. Одеса: ОДУВС, 2024. С. 175-177. URL: https://www.researchgate.net/profile/Anna-Politova-2/publication/383158882_Politova_AS_Kriminalna_vidpovidalnist_za_kolaboracijnu_dialnist_zdobuvaciv_osviti_Aktualni_pitanna_kriminalno-pravovoi_kvalifikacii_dokumentuvanna_ta_rozsliduvanna_kolaboracionizmu_v_period_voennogo_s/links/66bf4cdd8d007355925978d4/Politova-AS-Kriminalna-vidpovidalnist-za-kolaboracijnu-dialnist-zdobuvaciv-osviti-Aktualni-pitanna-kriminalno-pravovoi-kvalifikacii-dokumentuvanna-ta-rozsliduvanna-kolaboracionizmu-v-period-voennogo.pdf.
9. Кобко Є.В. Організаційні аспекти документування колабораціонізму в Україні. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму в період воєнного стану:* матеріали Всеукраїнської науково-практичної конференції, м. Одеса, 09 серпня 2024 р. Одеса: ОДУВС, 2024. С. 217-220. URL: https://www.researchgate.net/profile/Anna-Politova-2/publication/383158882_Politova_AS_Kriminalna_vidpovidalnist_za_kolaboracijnu_dialnist_zdobuvaciv_osviti_Aktualni_pitanna_kriminalno-pravovoi_kvalifikacii_dokumentuvanna_ta_rozsliduvanna_kolaboracionizmu_v_period_voennogo_s/links/66bf4cdd8d007355925978d4/Politova-AS-Kriminalna-vidpovidalnist-za-kolaboracijnu-dialnist-zdobuvaciv-osviti-Aktualni-pitanna-kriminalno-pravovoi-kvalifikacii-dokumentuvanna-ta-rozsliduvanna-kolaboracionizmu-v-period-voennogo.pdf.
10. Гарасимів О.І., Гарасимів Б.Т., Ряшко О.В. Колаборційна діяльність: проблемні аспекти доказування. Правове забезпечення євроінтеграції: загальноправовий та галузевий аспекти: колективна монографія. Рига, Латвійська Республіка, 2024. С. 105-117. DOI https://doi.org/10.30525/978-9934-26-424-5-6.
11. Гольдберг Н.О., Берташ А.П. Складнощі доведення вини у кримінальних провадженнях, пов'язаних з колабораціонізмом: технічні та юридичні аспекти. *Науковий вісник Ужгородського Національного Університету.* 2024. Вип. 86, ч. 5. С. 46-52. (Серія Право). DOI https://doi.org/10.24144/2307-3322.2024.86.5.6.

12. Війна та правосуддя: як слідчим ефективно використовувати OSINT та що робити із рішеннями “судів” на непідконтрольних територіях. Новина 11.05.2021. *Українська Гельсінська спілка з прав людини.* URL: https://www.helsinki.org.ua/articles/viyna-ta-pravosuddia-iak-slidchym-efektyvno-vykorystovuvaty-osint-ta-shcho-robyty-iz-rishenniamy-sudiv-na-nepidkontrolnykh-terytoriiakh.
13. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. 24 вересня 2025. *Судова влада України.* URL: https://court.gov.ua/archive/1883704/ (дата звернення 25.09.2025).
14. Столітній А.В., Каланча І.Г., Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності.* 2019. № 146. С. 179-191. DOI https://doi.org/10.21564/2414-990x.146.171218.
15. Шумило М.Є., Юрка Р., Капліна В.А. Інформаційна теорія доказів та проблеми використання електронних засобів доказування у кримінальному провадженні. *Вісник Національної академії правових наук України.* 2019. Том 26. № 2. С. 137-152. DOI https://doi.org/10.31359/1993-0909-2019-26-2-118.
16. Гарасимів О.І., Марко С.І., Ряшко О.В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського Національного Університету.* 2023. Вип. 75, ч. 2. С. 158-162. (Серія Право). DOI https://doi.org/10.24144/2307-3322.2022.75.2.25.
17. Метелев О.П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинств*а. 2023. № 1-2. С. 42-53. URL: https://vkslaw.knu.ua/images/verstka/3_2019_METELEV.pdf (дата звернення: 17.07.2025).
18. Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. 2024. вип. 17 (29). С. 227–243. (Серія Право). DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243.
19. Протокол Берклі з ведення розслідувань із використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права. Нью-Йорк і Женева. 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.
20. Аксамітовська К. Підрозділи з воєнних злочинів: законодавчі, організаційні та технічні уроки. Серпень 2021 р. Гаага. URL: https://www.asser.nl/media/795288/karolina-aksamitowska-war-crimes-units-legislative-organisational-and-technical-lessons-ukr.pdf.

Дата першого надходження рукопису до видання: 20.03.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026