4. Колабораціонізм на тимчасово окупованих територіях: проблеми правової оцінки, гарантування прав і свобод людини та реінтеграції територій : монографія / [М. А. Рубащенко, І. В. Яковюк, Н. В. Шульженко, О. В. Зайцев, С. О. Харитонов] ; за наук. ред. М. А. Рубащенка ; Нац. фонд дослідж. України ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2024. 576 с.

5. Злочинна колаборація в умовах збройної агресії: практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. 312 с.

6. Дорогих С. О. Сутність та визначення понять «Інформаційна діяльність» та «Інформаційна діяльність органів влади». *Інформація і право.* 2013. № 3(9). С. 74–82. URL: https://ippi.org.ua/sites/default/files/13dsodov.pdf (дата звернення: 09.12.2025).

DOI https://doi.org/10.36059/978-966-397-582-5-44

СУТНІСТЬ І ЗМІСТ ПЕРЕВІРКИ ЯК ЕТАПУ ПРОВЕДЕННЯ РОЗСЛІДУВАННЯ З ВИКОРИСТАННЯМ ВІДКРИТИХ ЦИФРОВИХ ДАНИХ: ВИМОГИ ПРОТОКОЛУ БЕРКЛІ

Маркіна Анна Валеріївна
аспірантка кафедри кримінального процесу
Національного університету «Одеська юридична академія»
м. Одеса, Україна

Одним з етапів розслідування з використанням даних з відкритих джерел, відповідно до Протоколу Берклі, є перевірка отриманої інформації, яка становить процес визначення надійності її джерел, що існують онлайн, і змісту та може здійснюватися як під час аналізу всіх джерел, у тому числі закритих і конфіденційних (у цьому випадку вона становить частину такого аналізу), так і мати самостійний характер та проводитися виключно стосовно відкритих джерел.

Як процес визначення надійності інформації, отриманої з відкритих джерел, та її змісту, перевірка характеризується притаманною їй структурою, що знаходить відображення у Протоколі Берклі як сукупність відокремлених, але водночас взаємопов'язаних і взаємоузгоджених елементів (етапів). Так, згідно з п. 176 Протоколу Берклі, перевірка поділяється на три окремі чинники: джерело, цифровий об'єкт або файл і зміст, які потрібно розглядати сукупно та порівнювати на предмет

узгодженості [1]. Відповідно, елементами (етапами) перевірки інформації, отриманої з відкритих джерел, є: 1) аналіз джерела; 2) технічний аналіз; 3) аналіз змісту.

Для позначення вказаних чинників О.О. Торбас використовує термін «етапи» [2, с. 56], що свідчить про застосування вченим функціонального підходу до дослідження структури перевірки інформації, отриманої з відкритих джерел. Використання цього підходу дозволяє розкрити структуру перевірки зазначеної інформації в динаміці – як сукупність взаємопов'язаних етапів, які з точки зору змісту Протоколу Берклі не є послідовно змінюваними, але відображають окремі складові цього процесу. Поряд із динамічним підходом, до дослідження структури перевірки інформації, отриманої з відкритих джерел, може застосовуватися також структурний підхід. Його використання дозволяє охарактеризувати перевірку як сукупність взаємопов'язаних елементів, тобто визначити її у статиці, що забезпечує розуміння як змісту цих елементів, так і зв'язків між ними.

Аналіз джерела в п. 177 Протоколу Берклі визначається як процес оцінки його надійності та достовірності [1]. Забезпечення правильності перевірки інформації, отриманої з відкритих джерел, на цьому її етапі зумовлює необхідність правильного встановлення джерела аналізу або сукупності таких джерел з урахуванням віднесення інформації до її першоджерела, яким може бути конкретний веб-сайт, абонент або користувач певного облікового запису чи платформи, або група осіб, які склали, створили чи завантажили певний контент. Незважаючи на вагомість з'ясування авторства для встановлення автентичності цифрового об'єкта, який існує онлайн, його невстановлення може бути компенсоване за рахунок інших способів автентифікації інформації у відкритому доступі.

Під час аналізу джерела, відповідно до пунктів 178-182 Протоколу Берклі, підлягають врахуванню: 1) походження (встановлюється найбільш давня поява цифрового об'єкта в інтернеті або вихідний елемент до його завантаження в інтернет); 2) надійність (з'ясовується онлайн-активність джерела та досліджується історія його публікацій задля виявлення умисних спроб введення в оману); 3) незалежність і неупередженість (встановлюються зв'язки джерела, його взаємовідносини з іншими, фінансування, мотиви, інтереси і плани та ступінь можливого впливу цих чинників на правдивість джерела); 4) конкретність (аналіз здійснюється з урахуванням відсутності труднощів у підтвердженні або спростуванні точної інформації та тверджень і складності критичної оцінки широких та нечітких тверджень); 5) згасання (враховується більша надійність текстів, складених одночасно з описаними у них подіями, порівняно з тими, які були створені через тривалий час після подій) [1].

Технічний аналіз у п. 183 Протоколу Берклі характеризується як аналіз самого цифрового об'єкта – документа, зображення чи відео [1]. Задля перевірки цілісності файлу (встановлення змін або модифікацій) технічний аналіз здійснюється під час проведення експертизи. Зміст технічного аналізу розкрито в пунктах 184-186 Протоколу Берклі, згідно з якими його елементами є: 1) метадані – вбудовані у файл, відображені на вебсторінці або у вихідному коді дані, що містять інформацію про інші дані (опис цифрового об'єкта та обставин його створення, розповсюдження або зміни, у тому числі інформація про автора файлу, дату його створення, дані завантаження, зміни, розмір файлу та геодані); 2) дані формату обмінних файлів зображень – тип метаданих, що визначає формати зображень, звуку та допоміжних тегів, які використовуються цифровими камерами, сканерами та іншими системами, що обробляють файли зображень і звуку, записані цифровими камерами; 3) вихідний код – програмування за будь-якою вебсторінкою або програмним забезпеченням [1].

Аналіз змісту в п. 187 Протоколу Берклі визначається як процес, за допомогою якого інформація, що міститься у цифровому об'єкті (відео, зображенні, аудіозаписі, документі, заяві або неструктурованому тексті), оцінюється на предмет її автентичності та достовірності [1]. Аналіз змісту здійснюється з урахуванням візуальних підказок і може передбачати підтвердження цифрового об'єкта за допомогою метаданих.

Під час аналізу змісту, відповідно до пунктів 188–194 Протоколу Берклі, підлягають урахуванню: 1) унікальні ідентифікатори (у ході перевірки візуального контенту здійснюється пошук унікальних або ідентифікуючих ознак, якими можуть бути будівлі, флора та фауна, люди, символи і знаки розрізнення, із тим уточненням, що ідентифікація зазвичай вимагає спеціальних навичок і, відповідно, здійснюється експертом); 2) інформація, яка об'єктивно перевіряється (аналіз доречно починати із визначення такої інформації та перевіряти інформацію, отриману з відкритих джерел, на відповідність їй); 3) геолокація (здійснюється ідентифікація або оцінка місця розташування об'єкта, діяльності чи місця, з якого було створено об'єкт); 4) хронолокація (передбачає підтвердження дат і часу подій, зображених в інформації, зазвичай у вигляді візуальних зображень); 5) повнота (встановлюється повнота цифрового об'єкта та враховується вплив прогалин на його доказове значення); 6) внутрішня узгодженість (перевірка проводиться стосовно окремого фрагмента інформації з відкритого онлайн-джерела або стосовно сукупності інформації з певного джерела та/або джерел з однаковим походженням чи авторством і має на меті встановлення внутрішньої узгодженості та послідовності цієї інформації); 7) зовнішнє підтвердження (забезпечується інформацією, яка знаходиться поза

межами самого цифрового об’єкта, але збігається з його змістом і, таким чином, підтверджує достовірність його змісту) [1].

Підсумовуючи викладене, потрібно зазначити, що вимоги Протоколу Берклі містять детальну характеристику перевірки інформації як етапу розслідування з використанням даних з відкритих джерел. Із урахуванням впровадження Протоколу Берклі у практичну діяльність прокурорів і працівників слідчих підрозділів правоохоронних органів на підставі листа-орієнтування Офісу Генерального прокурора «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел» від 28.08.2021 р. № 18/1 [3] та широке використання його рекомендацій у судовій практиці, використання наведених у ньому вимог під час перевірки електронних доказів, отриманих з відкритих джерел, у кримінальному провадженні спрятиме встановленню їх достовірності та, відповідно, визначенню придатності для використання в доказуванні.

Література:

1. Berkeley Protocol on Digital Open Source Investigations. New York and Geneva : Office of the United Nations High Commissioner for Human Rights, and the Human Rights Center at the University of California, Berkeley, School of Law, 2022. 87 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

2. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса : Видавництво «Юридика», 2024. 180 с.

3. Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел: лист-орієнтування Офісу Генерального прокурора від 28.08.2021 р. № 18/1. Київ : Офіс Генерального прокурора, 2021. 3 с.