МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ НАФТИ І ГАЗУ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ ІМ. М. Є. ЖУКОВСЬКОГО «ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Матеріали

VII Всеукраїнської дистанційної науково-практичної конференції

«ІНФОРМАЦІЯ ТА ДОКУМЕНТ У СУЧАСНОМУ НАУКОВОМУ ДИСКУРСІ»

20 травня 2022 р.
м. Івано-Франківськ, Україна

УДК 316.77: 002 (063)

Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. 175 с.

У збірнику представлені тези доповідей учасників VII Всеукраїнської дистанційної науково-практичної конференції «Інформація та документ у сучасному науковому дискурсі». Висвітлюються актуальні проблеми документознавства, професійного інформаційного середовища, документаційного забезпечення установ, освітніх комунікативних технологій у навчальному процесі тощо. Увага акцентується на пріоритетних напрямах документознавства та інформаційної діяльності у площині сучасних проблем комунікації та освіти.

Збірник призначений для науковців, викладачів, здобувачів вищої освіти, аспірантів, а також для широкого кола читачів.

Відповідальність за зміст і достовірність публікацій несуть автори наукових доповідей.

УДК 316.77: 002 (063)

РОЗДІЛ 1
СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ДОКУМЕНТОЗНАВСТВА ТА СОЦІАЛЬНИХ КОМУНІКАЦІЙ

Оксана Дуфенюк,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
та криміналістики факультету №1
ІПФПНП Львівського державного
університету внутрішніх справ

ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ЦИФРОВОЇ ІНФОРМАЦІЇ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

Останніми десятиліттями обсяги даних у кіберпросторі зростають у геометричній прогресії і малоймовірно, що ця тенденція ближчим часом уповільниться. Мільярди людей мають профілі у соціальних мережах і щодня публікують свій контент. Засоби масової інформації, комунікація держави із суспільством значною мірою перемістилися у віртуальний простір. У багатьох розвинених країнах створено спеціальні підрозділи для аналітичної роботи з такими даними, проводяться тренінги, конференції, курси для усіх бажаючих опанувати роботу з відкритими джерелами. Помітною є тенденція появи команд приватних, громадських, журналістських «розслідувачів», які досить ефективно виконують аналітичні завдання, пов’язані із документуванням злочинної діяльності. Прикладом може слугувати діяльність групи дослідників Bellingcat, які вивчають відкриті джерела та публікують результати розслідувань, зокрема, щодо діяльності наркобаронів, вчинення злочинів проти людства, воєнних злочинів у всьому світі.

Цілком логічно, що така сила силенна інформації стала цікавою і для правоохоронних органів. Аналітична робота з такими джерелами еволюціонувала від епізодичного використання до своєрідної моделі інформаційно-цифрового розслідування події через відкриті джерела у кіберпросторі. На відміну від «розвідки відкритих джерел» (OSINT), яка більшою мірою концентрується на виявленні загроз, оцінці ризиків, трендів з

метою інформування уповноважених осіб для прийняття політичних, безпекових, військових рішень, поняття «розслідування відкритих джерел» розглядається у контексті кримінального процесу і має прямою метою збір доказів кримінальних правопорушень, тобто виявлення, аналіз, дослідження, систематизацію, збереження, оцінку даних з відкритих джерел цифрової інформації з метою їх подальшого використання в рамках досудового та судового процесів [5, с. 7-8]. Не зважаючи на відмінності у кінцевій меті, засади діяльності розслідування відкритих джерел та розвідки відкритих джерел суттєво не відрізняються. Водночас варто підкреслити, що надання цифровим відомостям з відкритих джерел статусу доказу та перспективи їх використання у судовій залі детермінує особливі підходи до формування кінцевого звіту такої аналітичної діяльності, належної процесуальної фіксації та збереження даних. Такі цифрові докази мають відповідати критеріям достовірності, правдивості, надійності, релевантності, переконливості, належності та допустимості.

Відкритим вважається таке джерело інформації, яке є публічно доступним, тобто будь-хто з представників громадськості може моніторити, запитувати, купувати, колекціонувати таку інформацію без обмежень. Щоправда інколи така інформація може бути доступна тільки фахівцям, які мають спеціальні навички користування певним програмним забезпеченням, певними браузерами. Існує явище «темної павутини», «темної мережі», в межах якої користувачі користуються анонімністю, що робить її особливо привабливим місцем для незаконної діяльності [5, с. 6]. Типові відкриті джерела цифрової інформації демонструє Таблиця 1.

Таблиця 1 – Типові відкриті джерела цифрової інформації

Публічні веб-сайти	Бази даних (реєстри)	Соціальні мережі
• офіційні сторінки органів державної влади, державних підприємств, установ, організацій, органів місцевого самоврядування • офіційні сторінки неурядових громадських організацій, асоціацій, спілок • засоби масової інформації (сайти газет, журналів) • особисті блоги, влоги, конференції, виступи, звіти, інформаційні бюлетені і т.д.	• публічні бази даних • приватні бази даних • бази даних рішень • база персональних даних • бази даних контактів (зв'язків) • бази логістичних даних • бази картографічних даних • бази мультимедійних даних • бази текстових даних • бази комерційних даних • бази фінансових даних і т.д.	• YouTube • Facebook • Instagram • WhatsApp • Twitter • Snapchat • Telegram • TikTok • Viber і т.д.

Опрацювання власне

Фахівці справедливо зазначають, що пошук значущої інформації в мережі Інтернет пов'язаний з необхідністю долати низку викликів, зумовлених великими обсягами даних, складною динамікою інформаційних потоків, багатократним дублюванням інформації, наявністю «шумової інформації», відсутністю індексації у пошукових системах значної кількості інформації (навіть такій потужній пошуковій системі Google за деякими розрахунками потрібно 300 років для індексації всієї інформації, обсяги якої, нагадаємо, далі зростають) [3, с. 309-310]. Відтак, роботу з відкритими джерелами інформації метафорично справедливо порівнюють з пошуком одного відсотка цінної інформації, «золотої крупиці», яка захована у 99 % пустого піску [4, с. 39]. Це стало приводом до активного пошуку шляхів алгоритмізації, оптимізації та автоматизації роботи з відкритими джерелами даних. Основними кроками такої діяльності є:

Крок 1. *Ідентифікація джерел* (визначення яку інформацію ми потребуємо, де і як її знайти).

Крок 2. *Колекціонування даних* (збір даних самостійно або за допомогою спеціальних програм).

Крок 3. *Обробка даних* (систематизація та фільтрація інформації, яка є важливою, яка ні, а яка потребує додаткової верифікації чи уточнення).

Крок 4. *Аналіз* (вивчення та уточнення даних, визначення їх значення для розслідування. Скажімо, якщо докази А, Б і В, що підтверджують аргумент Х, то можна переходити на наступну стадію, якщо доказів бракує, або вони не підтверджують аргумент Х, то ми повертаємося на попередній етап і проводимо додаткову обробку даних).

Крок 5. *Звітність* (оформлення даних у вигляді звітних документів, які можна згодом використати залежно від поставлених завдань [6, с. 3−4].

Дещо інший цикл роботи з відкритими даними (див. рис. 1) пропонують фахівці Берклійської школи права, Каліфорнійського університету, які підготували спеціальний протокол розслідування фактів порушень міжнародного гуманітарного права, порушень прав людини за допомогою відкритих джерел інформації [5, с. 55].

Рисунок 1 – Цикл розслідування події через відкриті джерела, *опрацьовано за матеріалами джерела [5, с. 55]*

Цей алгоритм передбачає (1) процес виявлення інформації (он-лайн запити, моніторинг); (2) процес попередньої оцінки даних; (3) процес

колекціонування даних (4) процес збереження даних, тобто фіксація і вилучення цифрової інформації з Інтернету в такий спосіб, що дозволяє підтвердити певні факти навіть тоді, коли з першоджерела інформація була видалена (резервне копіювання даних, завантаження контенту, виготовлення скрінів екрану тощо); (5) процес верифікації (перевірка надійності джерел даних та правдивості їх змісту); (6) процес слідчого аналізу, тобто інтерпретація даних, формулювання висновків, ідентифікація прогалин, з'ясування значення отриманих даних для процесу розслідування.

Під час розслідування злочинів підрозділи інформаційно-аналітичного забезпечення за аналогією із альтернативними видами розвідки у сфері забезпечення безпеки, на основі роботи з відкритими джерелами можуть сформувати об'єктно-реляційні моделі, здійснювати багатомірний аналіз інформації, зберігати мультимедійні та геопросторові дані, відновлювати використання технічного та програмного забезпечення після збоїв, проводити резервне копіювання даних та відновлення змін IP, захисту IP від несанкціонованого доступу, проводити процедури парних порівнянь тощо [1, с. 37–38].

Суттєвим кроком вперед в частині оптимізації інформаційно-цифрового розслідування є впровадження автоматизованих інноваційних продуктів, які дозволяють значно скоротити час на пошук та систематизацію даних. До таких програмних технологій можна віднести: *Maltego* (дозволяє здійснювати аналіз зв'язків між людьми в соціальних мережах); *Creepy* (працює з Windows та Linux і призначена для аналізу геолокаційних даних про користувачів); *Spokeo* (збирає демографічні дані, соціальні профілі, проводить оцінку фінансового стану та володіння нерухомістю); *Recorded Future* (допомагає виявити тенденції у великих масивах неструктурованої інформації, витягаючи необхідні факти з Інтернету); *OSINT Opsec* (здійснює моніторинг декількох найбільш важливих сайтів в Інтернеті; пошук за ключовими словами у свіжих публікаціях у соціальних мережах; пошук даних певного типу, відстеження рейтингу брендів) і т.д. [2, с. 6].

Підсумуємо сказане. Процес розслідування у цифрову епоху має свої особливості, одна з яких полягає в тенденції розширення інформаційних потоків, які містять дані про злочинну діяльність. Як наслідок, виникає потреба розвивати, алгоритмізувати, автоматизувати та оптимізувати роботу з відкритими джерелами цифрової інформації, результати якої можуть слугувати доказами у кримінальних провадженнях.

Список використаної літератури

1. Бурячок В. Л., Бурячок Л. В. Стратегія оцінювання внеску видів розвідки інформаційно-телекомунікаційних систем у рішення завдань пошуку та збору інформації з відкритих і відносно відкритих електронних джерел. *Сучасний захист інформації*. 2014. № 2. С. 35−43.

2. Віщун В. В., Омельянчук А. В. Технологія виявлення загроз інформаційній безпеці шляхом аналізу інформації з відкритих джерел. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2012. № 3. С. 5−7.

3. Гавловський В. Д. Окремі питання отримання інформації з відкритих джерел для правоохоронних органів. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2010. Вип. 23. С. 308−315.

4. Жарков Я. М., Васильєв А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 38−41.

5. Berkeley Protocol on Digital Open Source Investigations A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. United Nations. 2020. 104 p. URL: https://humanrights.berkeley.edu/programs-projects/tech-human-rights-program/berkeley-protocol-digital-open-source-investigations

6. Yong-Woon H., Im-Yeong L., Hwankuk K., Hyejung L., Donghyun K. Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*. 2022. P. 1−14. DOI: https://doi.org/10.1155/2022/1290129.