нормативного, організаційного та ресурсного характеру мають бути вирішені через системні реформи, інтеграцію з європейським безпековим простором та інвестиції в людський капітал. Успішна реалізація цих завдань стане запорукою підвищення спроможності держави протидіяти сучасним загрозам у цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гнусов Ю. В., Калякін С. В. Кримінальний аналіз у роботі підрозділів Національної поліції України. Протидія кіберзагрозам та торгівлі людьми: зб. мат. міжнар. наук.-практ. конф. 26 лист. 2019, с. 61.

2. Федчак І. А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.

3. Про Національну поліцію [Текст]: Закон України від 02.07.2015 р. №580- VIII // ВВР. 2015. № 40-41. Ст. 379.

4. Школьніков В. І. Використання результатів кримінального аналізу в кримінальному процесі України. Міжвідомча науково-практична конференція «Актуальні проблеми досудового розслідування», присвячена Дню слідчого України, 2017, с. 33-35.

РОЛЬ OSINT У СТВОРЕННІ ДОКАЗОВОЇ БАЗИ ЩОДО ВОЄННИХ ЗЛОЧИНІВ

Волобоєв А. О.
доктор філософії в галузі права,
завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3
Донецького державного університету внутрішніх справ
м. Кропивницький, Україна
ORCID ID: https://orcid.org/0000-0002-7138-5847

Документування воєнних злочинів та переслідування воєнних злочинців у контексті сучасних збройних конфліктів має особливу актуальність, зокрема для міжнародного правосуддя. Відкриті джерела розвідувальних даних (Open Source Intelligence, далі – OSINT) суттєво змінили процес збору та аналізу доказів, створивши нові можливості для правосуддя перехідного періоду. Адже доказова база, сформована за допомогою OSINT, стає важливим інструментом для притягнення до відповідальності порушників міжнародного гуманітарного права.

OSINT як методологічний підхід базується на системному зборі, обробці та аналізі інформації з відкритих джерел. Такий підхід змінює традиційні методи розслідування воєнних злочинів, поєднуючи цифрові технології з юридичною практикою. Цінність досліджуваного цифрового ресурсу полягає у формуванні різнопланової доказової бази, яка висвітлює

різні аспекти протиправних діянь та обставин їх вчинення.

У правовій площині використання даних з відкритих джерел розширює доктрину допустимості доказів. Такі матеріали поєднують міждисциплінарний підхід на перетині права, технологій, соціальної психології та криміналістики, формуючи нову модель доказування в умовах цифрової екосистеми міжнародного правосуддя. Це зумовлює потребу в переосмислені основних правових концепцій, зокрема крім допустимості, ще критерії достовірності, достатності та належності доказів у світлі особливостей цифрового середовища.

Слід зазначити, що до OSINT-матеріалів, які використовуються для документування воєнних злочинів, належать:

аудіовізуальні матеріали (відеозаписи, фотографії, супутникові знімки, інфрачервоне сканування території, тепловізійні зображення);

дані соціальних мереж та комунікаційних платформ (дописи, коментарі, прямі трансляції, приватні повідомлення, що стали публічними);

геолокаційні дані та метадані цифрових файлів (координати GPS, часові мітки, ідентифікатори пристроїв, технічні характеристики фіксації);

публічні реєстри та бази даних (державні реєстри, комерційні бази даних, архіви, системи ідентифікації осіб);

цифрові сліди переміщень військової техніки та особового складу (радіоперехоплення, сигнали телеметрії, електронні комунікації, дані телеметричних систем);

цифрові економічні транзакції, що можуть свідчити про підготовку до вчинення злочинів (фінансові перекази, закупівлі специфічного обладнання);

інформаційні артефакти з архівів пошукових систем та веб-архівів, що свідчать про розвиток інформаційного наративу, тощо.

Перевірка цих матеріалів потребує багаторівневої методології, що включає хронологічну синхронізацію подій, порівняльний аналіз джерел, технічну автентифікації цифрових матеріалів, аналіз візуальних матеріалів і обставин фіксації доказів. Тут головним аспектом є підтримка неперервності ланцюга доказів від моменту виявлення до представлення в суді. Згідно з «Протоколом Берклі з ведення розслідувань з використанням відкритих цифрових даних», саме систематична крос-перевірка забезпечує точність та достовірність зібраної інформації [1]. Це критично важливо, враховуючи поширення технологій для маніпулювання цифровим контентом, зокрема deepfake та інших форм синтетичних медіа.

Крім того, застосування методології OSINT у системі міжнародного кримінального судочинства породжує низку складних юридичних проблем. Основні з яких, це:

філософсько-правове розуміння допустимості цифрових доказів у контексті традиційних стандартів доказування;

перевірка достовірності (верифікації) даних з відкритих джерел, включаючи встановлення їх автентичності, походження та цілісності;

юрисдикційні питання транскордонного збору доказів у віртуальному середовищі;

етико-правові аспекти використання даних з особистих цифрових профілів, балансуючи між приватністю та суспільними інтересами;

переосмислення доказової цінності інтегрованих масивів даних замість окремих доказів, що впливає на класичну теорію доказів;

виклики інтерпретації контекстуально залежних цифрових даних, зокрема при міжкультурних та міжмовних бар'єрах;

правові аспекти інтеграції алгоритмічних систем аналізу даних у доказування, тощо.

Серйозним завданням сьогодення залишається й формування єдиних стандартів обробки цифрових доказів для різних міжнародних судів.

Між тим, OSINT змінює підходи міжнародного правосуддя, розширюючи інструментарій розслідування воєнних злочинів. Використання цифрових доказів дозволяє проводити розслідування навіть без безпосереднього доступу до місць скоєння злочинів.

На нашу думку, розвиток методології OSINT у документуванні воєнних злочинів визначається через такі тенденції, як:

застосування штучного інтелекту та машинного навчання для аналізу великих обсягів даних;

розвиток методів цифрової криміналістики для перевірки мультимедійних матеріалів;

формування єдиних стандартів і протоколів обробки цифрових доказів;

розвиток транснаціональних мереж документування порушень міжнародного гуманітарного права;

розробка методик інтерпретації культурно-контекстуальних аспектів цифрових даних;

створення захищених систем зберігання та архівації цифрових доказів, тощо.

Ці тенденції сприяють трансформації міжнародного правосуддя у бік більшої доступності та ефективності. Важливим інструментом для розкриття воєнних злочинів є OSINT Framework [2], що охоплює весь процес роботи з публічно доступною інформацією.

Отже, OSINT відіграє важливу роль у документуванні воєнних злочинів та переслідуванні воєнних злочинців, формуючи новий вимір міжнародного правосуддя. Цифровізація доказів розширює можливості притягнення до відповідальності порушників міжнародного гуманітарного права навіть за умов обмеженого доступу до місць злочинів.

Подальший розвиток OSINT як інструменту міжнародного правосуддя потребує теоретичного осмислення та практичного впровадження через розробку правових механізмів та методологічних підходів. Впровадження OSINT у процесуальну практику міжнародних судів становить важливий

крок до забезпечення невідворотності покарання за найтяжчі міжнародні злочини, сприяючи утвердженню принципів верховенства права у міжнародних відносинах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. Нью-Йорк і Женева, 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

OSINT Framework. *Цифрова платформа OSINT-ресурсів.* URL: https://osintframework.com.

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ: ВИКЛИКИ, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ

Головкін Сергій Вікторович,
кандидат юридичних наук,
старший науковий співробітник, доцент,
доцент кафедри кримінального процесу
та криміналістики факультету № 1
Донецького державного університету внутрішніх справ

Сьогодні ми живемо в умовах стрімкої цифрової трансформації, яка впливає не лише на економіку та соціальну сферу, але й суттєво змінює безпекові виклики, з якими стикається наша держава. Зростання кіберзлочинності, інформаційних атак, а також використання цифрових технологій у традиційній злочинній діяльності вимагають нових інструментів для аналізу, попередження й розслідування кримінальних правопорушень.

З огляду на це доцільно зосередитися на двох ключових складових сучасної системи безпеки – кримінальному аналізі та кібербезпеці й проаналізувати, як ці напрями розвиваються в Україні.

Сучасний стан кримінального аналізу в Україні характеризується поступовим становленням і розвитком як інституційного, так і технологічного напряму аналітичної діяльності у сфері безпеки. Цей процес відбувається в умовах гібридних загроз, воєнного конфлікту та активної цифровізації.

Кримінальний аналіз – це систематичне збирання, оцінювання та інтерпретація інформації з метою попередження злочинності, виявлення злочинних тенденцій і підтримки правоохоронної діяльності. В Україні останні роки спостерігається поступове впровадження кримінального аналізу в діяльність органів правопорядку, зокрема в системі Національної поліції України функціонують підрозділи аналітичної підтримки, створено