

**Міністерство внутрішніх справ України
Одеський державний університет внутрішніх справ**



**КРИМІНАЛЬНИЙ АНАЛІЗ
І КІБЕРБЕЗПЕКА:
ОБ'ЄДНАННЯ ЗУСИЛЬ ДЛЯ НОВИХ
ВИКЛИКІВ**

**матеріали науково-практичної
конференції**

23 травня 2025 року

**м. Одеса
2025**

Міністерство внутрішніх справ України
Одеський державний університет внутрішніх справ
Науково-дослідна лабораторія з проблемних питань
кримінального аналізу
Одеського державного університету внутрішніх справ

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ
«Кримінальний аналіз і кібербезпека: об'єднання
зусиль для нових викликів»

23 травня 2025 р.

м. Одеса – 2025

УДК 343.9(477)

Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів: збірник тез Міжнародної науково-практичної конференції (23 травня 2025 р.). Одеса : ОДУВС, 2025. 216 с.

Збірник містить тези доповідей учасників Міжнародної науково-практичної конференції «Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів» , яка відбулася 23 травня 2025 року в Одеському державному університеті внутрішніх справ.

Матеріали подано в авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, галузевої термінології, інших відомостей.

УДК 343.9(477)

© Автори, 2025

© Одеський державний університет
внутрішніх справ, 2025

ШАНОВНІ УЧАСНИКИ КОНФЕРЕНЦІЇ!

Щиро вітаю вас на відкритті науково-практичної конференції, присвяченої надзвичайно важливим питанням - розвитку кримінального аналізу та зміцненню кібербезпеки в Україні. Це не просто актуальні напрямки наукової та прикладної діяльності - це стратегічна потреба нашої держави в умовах військового стану, інформаційних атак та зростаючої цифрової загрози.

У сучасному світі кіберзагрози стають все більш складними, багатошаровими та руйнівними. Вони здатні паралізувати функціонування ключових державних структур, дестабілізувати економіку та завдати шкоди правам громадян. У цьому контексті кримінальний аналіз, побудований на основі сучасних даних, аналітичних інструментів та міждисциплінарного підходу, є необхідною умовою для ефективного протистояння цим викликам.

Формування дієвих стандартів, впровадження інноваційних інструментів OSINT, використання штучного інтелекту та аналітики Big Data - це саме ті напрями, які потребують нашої фахової уваги й спільної роботи. Саме на таких платформах, як сьогоднішня конференція, ми маємо унікальну можливість об'єднати знання, обговорити ідеї та спільно сформуванати ефективну систему реагування на нові загрози.

Одеський державний університет внутрішніх справ пишається тим, що є майданчиком для професійного діалогу між наукою, освітою та практикою. Ми впевнені, що результати вашої роботи матимуть практичне значення та сприятимуть підвищенню рівня безпеки в нашій країні.

Бажаю всім учасникам конференції продуктивної роботи, цікавих дискусій, конструктивних рішень і нових звершень у науковій та професійній діяльності.

ДАВИДЕНКО В'ячеслав Віталійович
ректор Одеського державного університету внутрішніх справ
кандидат юридичних наук, доцент, полковник поліції

АНАЛІТИЧНА ДІЯЛЬНІСТЬ ЯК СКЛАДОВА КРИМІНАЛЬНОЇ РОЗВІДКИ

Албул Сергій Володимирович

кандидат юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції НПУ ОДУВС

Правова регламентація оперативно-розшукової діяльності, розроблення, обґрунтування та формування основних правових концептів розвивалися одночасно з процесами державотворення сучасної України. Орієнтуючись на досвід провідних країн світу, теоретичні положення суміжних галузей знань, напрацювання науковців, вперше в історії України 18 лютого 1992 року був прийнятий Закон «Про оперативно-розшукову діяльність», який на довгі роки став базовим щодо її регламентації. Легітимізація оперативно-розшукової діяльності шляхом прийняття відповідного Закону закріпила її правовий статус та вивела на новий рівень, позбавивши таємні відомчі нормативні акти функції основного регулятора. Разом із тим, Закон України «Про оперативно-розшукову діяльність» не є сталим правовим актом і за час свого існування неодноразово піддавався змінам та доповненням [1, с. 3].

На сьогодні, з метою реалізації завдань, визначених у п. 1.7.1. Плану заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки, затвердженого розпорядженням Кабінету Міністрів України від 23 серпня 2024 року № 792-р. міжвідомчою робочою групою здійснюється опрацювання проекту Закону України «Про кримінальну розвідку», який концептуально замінить Закон України «Про оперативно-розшукову діяльність» [2].

В проекті визначено, що кримінально-розвідувальна діяльність (кримінальна розвідка) – це особливий вид діяльності спеціально уповноважених державних органів, що здійснюється за наявності визначених законодавством підстав з метою профілактики кримінальних правопорушень, їх виявлення, припинення та розкриття, сприяння реалізації завдань кримінального провадження, виявлення та нейтралізації реальних та потенційних загроз національним інтересам України, а також забезпечення національної, державної, воєнної, економічної, громадської безпеки та правопорядку [3]. При цьому, наголошується, що кримінально-розвідувальна діяльність здійснюється шляхом організації та проведення заходів кримінальної розвідки, *аналітичної діяльності* (курсив наш – С.А.) та негласного співробітництва [4].

Визначаючи аналітичну діяльність як обов'язкову складову кримінальної

розвідки, передбачено, що така діяльність – це системний інтелектуальний процес обробки, систематизації, перевірки, аналізу інформації, отриманої з різних джерел, моделювання та прогнозування, що здійснюється суб'єктами кримінально-розвідувальної діяльності з метою виявлення загроз, установлення зв'язків, ідентифікації осіб, фактів та об'єктів, профілактики кримінальних правопорушень, їх виявлення, припинення та розкриття, сприяння реалізації завдань кримінального провадження, а також забезпечення національної, державної, воєнної, економічної, громадської безпеки та правопорядку [3]. Органи та підрозділи, які уповноважені здійснювати кримінально-розвідувальну діяльність здійснюють аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим законом.

У свою чергу, кримінальний аналіз – це специфічний вид інформаційно-аналітичної діяльності в кримінально-розвідувальній діяльності, що спрямований на встановлення та припущення взаємозв'язків між інформацією (відомостями, даними) про злочинну чи протиправну діяльність та потенційно з нею пов'язаною інформацією, отриманою з різних джерел, її оцінювання, інтерпретацію та прогнозування розвитку досліджуваних подій, ситуацій і фактів з метою їх використання під час здійснення кримінально-розвідувальної діяльності, розроблення тактичних і стратегічних заходів з протидії злочинності. Одночасно зазначається, що інформаційно-аналітичне забезпечення кримінально-розвідувальної діяльності – це комплекс заходів організаційно-методичного характеру щодо пошуку, збору, накопичення, документального оформлення, структурування, систематизації, зберігання, її аналізу, перетворенню, та охорони інформації, що здійснюється уповноваженими суб'єктами з метою створення та ефективного використання інформаційних ресурсів в процесі виконання завдань кримінально-розвідувальної діяльності [4].

Примітно, що серед значної кількості завдань кримінальної розвідки проектом окремо передбачено контроль, відслідкування, аналіз, оцінка та прогнозування криміногенної обстановки; збирання та аналіз інформації про правопорушення, що впливають на національну, економічну, публічну безпеку і порядок держави, та визначення способів запобігання їх виникненню в майбутньому; оцінювання ризиків і загроз у сферах безпеки суспільства і держави шляхом аналізу структурованих і неструктурованих даних, сукупних висновків та результатів проведених оперативних, тактичних, стратегічних аналітичних досліджень та прийняття управлінських рішень щодо усунення передумов виникнення зон ризиків та схем протиправної діяльності [4]. Крім цього, норми проекту передбачають, що суб'єкти кримінально-розвідувальної діяльності уповноважені, зокрема:

створювати, застосовувати та захищати інформаційні, автоматизовані інформаційні та інформаційно-комунікаційні системи для забезпечення кримінально-розвідувальної діяльності;

мати безпосередній, у тому числі автоматизований, доступ до автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є державні органи або органи місцевого самоврядування;

збирати публічно доступну інформації з будь-яких джерел, у тому числі здійснювати розвідку з відкритих джерел (OSINT) з метою пошуку інформації, її фіксації, обліку та аналізу, аналітико-синтетичної переробки та відображення її в видових аналітичних продуктах;

створювати аналітичні продукти та інформаційні документи, у тому числі з оцінки загроз і ризиків тяжких злочинів та організованої злочинності (SOCTA); безпосередньо проводити або ініціювати проведення кримінального аналізу [3].

Слід зазначити, що окремі норми проекту деталізують питання аналітичної діяльності та використання її результатів. Зокрема, зазначено, що аналітична діяльність може здійснюватися з використанням аналітичних інструментів – спеціального програмного забезпечення з обробки інформації та перетворення її у форму, прийнятну для розуміння та використання. Результатом аналітичної роботи – є висновок та рекомендації, які створюються в електронному та/або письмовому вигляді, з обов'язковим зазначенням використаних аналітичних інструментів, баз даних, ухвал слідчого суді, судді апеляційного суду, дозволів прокурора або слідчого, якщо досліджувана інформація отримана в результаті проведення кримінально-розвідувальних заходів, слідчих (розшукових) та інших процесуальних дій. При цьому, результати кримінального аналізу та рекомендації, які створюються в електронному або письмовому вигляді, з обов'язковим зазначенням використаних аналітичних інструментів, баз даних, ухвал слідчого суді, дозволів прокурора або слідчого, якщо досліджувана інформація отримана в результаті проведення кримінально-розвідувальних заходів, слідчих (розшукових) та інших процесуальних дій у випадках, визначених Кримінальним процесуальним кодексом України, можуть бути визнані доказом у кримінальному провадженні [4].

Підсумовуючи викладене, слід зазначити, що розроблення та прийняття Закону України «Про кримінальну розвідку» сприятиме подальшому вдосконаленню правового регулювання протидії кримінальним правопорушенням, реалізації завдань кримінального провадження, виявлення та нейтралізації реальних та потенційних загроз національним інтересам України, а також забезпечення національної, державної, військової, економічної, громадської безпеки та правопорядку в умовах нових викликів. І особливе місце в цьому, безсумнівно, належить аналітичній діяльності як складової кримінальної розвідки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Албул С.В. Оперативно-розшукова діяльність: сучасні доктринальні та праксеологічні концепти. *Воєнний стан: теоретико-праксеологічні*

проблеми юриспруденції : колективна монографія. Lviv-Torun : Liha-Pres, 2024. С. 1–24. DOI <https://doi.org/10.36059/978-966-397-421-7-1>

2. План заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки: затверджений розпорядженням Кабінету Міністрів України від 23 серпня 2024 року № 792-р (зі змінами, внесеними згідно з Постановою Кабінету Міністрів України від 07.03.2025 р. № 272) [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/792-2024-%D1%80/print> (дата звернення 25.04.2025 р.).
3. Про кримінальну розвідку: проєкт Закону України. К.: МВС України, 2025. – 33 с.
4. Албул С.В. Пропозиції до проєкту Закону України «Про кримінальну розвідку». Одеса: ОДУВС, 2025. – 14 с. (вих. ОДУВС від 07.02.2025 р. № 1/389-2025).

ОКРЕМІ ПИТАННЯ ПОШУКУ ВІДЕОКОНТЕНТУ ТА ФОТОМАТЕРІАЛІВ У DARK WEB: РИЗИКИ ТА ПРАВОВІ АСПЕКТИ

Афонін Дмитро Сергійович

кандидат юридичних наук, доцент,
завідувач науково-дослідної лабораторії з актуальних питань
кримінального аналізу навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції НПУ ОДУВС

В умовах стрімкого розвитку цифрових технологій та зростання обсягів інформації в мережі Інтернет, Open-Source Intelligence (OSINT) стає критично важливим інструментом для правоохоронних органів у боротьбі зі злочинністю, забезпеченні національної безпеки та проведенні різноманітних досліджень. Проте, значна частина протиправної діяльності, включаючи торгівлю забороненими речовинами, зброєю, дитячу порнографію та координацію терористичних актів, зосереджена у прихованих сегментах Dark Net.

Пошук та аналіз відповідного відеоконтенту та фотоматеріалів у цих специфічних середовищах є надзвичайно складним, пов'язаний з високими ризиками та невизначеністю, а також перебуває на межі правового поля. Це робить OSINT-дослідження відеоконтенту та фотоматеріалів на Dark Web ресурсах вкрай актуальним для розробки ефективних методик та інструментів, що відповідають вимогам законності та етики.

Dark Web середовище вже давно стало предметом наукового інтересу багатьох вчених як українських, так і іноземних. Вони охоплюють широкий спектр тем, включаючи мережеву безпеку, шкідливе програмне забезпечення,

кібератаки, кіберзлочинність, конфіденційність даних, криптографію, машинне навчання, соціальні мережі, штучний інтелект та незаконний обіг наркотиків. Хсінчун Чен та AI Lab Університету Арізони провели значні дослідження Dark Web, зосереджуючись на інформатиці тероризму та розробці інструментів для збору даних, аналізу зв'язків, контенту, мультимедіа та авторства [1]. Майк Макгвайр з Університету Суррея досліджував кіберзлочинну економіку в Dark Web та соціальних мережах, включаючи продаж хакерських послуг, шкідливого програмного забезпечення та викрадених даних [2]. Жан-Лу Ріше вивчав онлайн-відмивання грошей та методи кіберзлочинців, включаючи ті, що використовуються в Dark Web [3].

Наукові роботи також обговорюють труднощі зі збором та аналізом даних отриманих з Dark Web ресурсів через анонімність, шифрування та динамічний характер контенту. Методи пошуку в Dark Web включають використання спеціалізованих пошукових систем, таких як Ahmia, Torch та Duck Duck Go (версія для Dark Web), а також каталогів на кшталт Onion Links [4]. Етичні аспекти є надзвичайно важливими при дослідженні Dark Web, особливо щодо дотримання законодавства та уникнення незаконної діяльності. У деяких дослідженнях використовуються штучний інтелект та машинне навчання для аналізу та класифікації контенту Dark Web, включаючи обробку зображень для виявлення незаконного контенту.

Відповідного зробленого аналізу наукових досліджень, можна виділити наступні ключові проблемні питання, пов'язані з пошуком та аналізом відеоконтенту та фотоматеріалів у Dark Web за допомогою інструментів OSINT:

- відсутність чіткого законодавчого регулювання доступу до прихованих сегментів мережі та використання отриманих звідти матеріалів як доказів;

- перетин межі між законним збором публічної інформації та порушенням приватності, особливо при використанні технік, що можуть включати елементи обману;

- анонімність Dark Web ускладнює пошук, ідентифікацію джерел та суб'єктів;

- високий ризик зіткнутися з неправдивою або сфабрикованою інформацією (включаючи Deepfake), що вимагає складних методів верифікації;

- необхідність обробки значних масивів даних низької якості, що вимагає потужних аналітичних інструментів та кваліфікованих фахівців [5].

- доступ до Dark Web може наражати дослідника на ризики інфікування шкідливим програмним забезпеченням або зіткнення з протиправним контентом.

Шляхами вирішення зазначених проблем можна вважати:

- вдосконалення нормативно-правової бази (розробка чіткого законодавства, що регулює порядок доступу до прихованих сегментів мережі для OSINT-досліджень, процедури збору та закріплення доказів, отриманих з таких джерел, з урахуванням захисту прав людини);

- розробка етичних кодексів та стандартів (формування професійних етичних норм для фахівців, що займаються OSINT-дослідженнями, особливо при роботі з чутливою інформацією та в прихованих сегментах мережі);

- розвиток спеціалізованих інструментів (створення та впровадження вдосконалених інструментів для автоматизованого пошуку, збору, аналізу та верифікації відеоконтенту та фотоматеріалів у Dark Web, включаючи інструменти на основі машинного навчання для виявлення маніпуляцій);

- підвищення кваліфікації фахівців (навчання OSINT-аналітиків правоохоронних органів специфіці роботи в прихованих сегментах мережі, методам безпечного доступу, технікам верифікації даних та правовим аспектам їх використання);

- міжнародна співпраця (обмін досвідом та найкращими практиками між країнами у сфері OSINT-досліджень прихованих сегментів мережі).

Пошук та аналіз відеоконтенту та фотоматеріалів у сегментах Dark Web є перспективним, але водночас надзвичайно складним та ризикованим напрямком OSINT-досліджень. Правова невизначеність, етичні дилеми, технічні перешкоди та низька достовірність даних створюють значні виклики. Для ефективного використання потенціалу відеоаналітики в цих середовищах необхідні комплексні заходи, що включають вдосконалення законодавства, розробку етичних стандартів, розвиток спеціалізованих технологій та підвищення професійного рівня фахівців. Лише за умови вирішення цих проблемних питань OSINT-дослідження у Dark Web зможуть стати повноцінним та легітимним інструментом у системі забезпечення безпеки та боротьби зі злочинністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hribar, G., Podbregar, I., Ivanuša, T. OSINT: A "Grey Zone"? *International Journal of Intelligence and CounterIntelligence*. 2014. Vol. 27, № 3. P. 529–549
2. Herrera-Cubides, J. F., Gaona-García, P. A., Sánchez-Alonso, S. Open-Source Intelligence Educational Resources: A Visual Perspective Analysis. *Applied Sciences*. 2020. Vol. 10, № 21. 7617. P. 1–25
3. Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., Martinez Perez, G. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*. 2020. Vol. 8. P. 10282–10304
4. Ferreira, S., Antunes, M., Correia, M. E. Exposing Manipulated Photos and Videos in Digital Forensics Analysis. *Journal of Imaging*. 2021. Vol. 7, № 7. 102. P. 1–23

ЗАСТОСУВАННЯ АРІ ДЛЯ ОТРИМАННЯ ДАНИХ З СОЦІАЛЬНИХ МЕРЕЖ

Бажура Вікторія Вікторівна

студентка 2 курсу другого (магістерського)
рівня вищої освіти ОПП «Кримінальний аналіз»
спеціальність 124 «Системний аналіз»
інституту права та безпеки

Інтерфейс програмування застосунків (прикладний програмний інтерфейс, АРІ) (англ. application programming interface) — це спосіб взаємодії комп'ютерних програм між собою. Набір визначень підпрограм, протоколів взаємодії та засобів для створення програмного забезпечення[1]. це набір чітко визначених методів для взаємодії різних компонентів. АРІ надає розробнику засоби для швидкої розробки програмного забезпечення. АРІ може бути для веб-базованих систем, операційних систем, баз даних, апаратного забезпечення, програмних бібліотек. АРІ дозволяють автоматизувати процес збору великих обсягів даних з різних онлайн-платформ.

Замість ручного пошуку інформації, аналітики можуть використовувати АРІ з метою:

- публікації в соціальних мережах, новини, дані про місцезнаходження тощо;
- надають доступ до даних у структурованому форматі (наприклад, JSON або XML), що полегшує їх обробку та аналіз;
- швидко виявляти закономірності, зв'язки та тенденції в даних.

АРІ можна інтегрувати з іншими інструментами OSINT, такими як платформи для візуалізації даних, інструменти для аналізу соціальних мереж та бази даних, що дозволяє створювати комплексні аналітичні системи, які об'єднують дані з різних джерел. АРІ дозволяють налаштовувати моніторинг певних тем або подій в реальному часі.

Використання АРІ розширює можливості OSINT, дозволяючи отримувати доступ до даних, які можуть бути недоступні через звичайний веб-пошук. Наприклад, АРІ можуть надавати доступ до історичних даних, даних про місцезнаходження або даних з платформ, які вимагають авторизації з соціальних мереж (Twitter, Facebook, Instagram) для аналізу громадської думки або виявлення дезінформації, про місцезнаходження з геолокаційних сервісів для відстеження переміщень об'єктів, новинних статей з різних джерел для аналізу інформаційного простору, з відкритих баз даних (наприклад, баз даних компаній або державних реєстрів) для аналізу зв'язків між організаціями.

Слід зазначити, що не завжди отримання необхідної інформації за допомогою текстових запитів є прийнятним. Тому доволі часто виникає

потреба пошуку зображень та перевірки їх достовірності, оскільки вони можуть зловмисно або випадково вводити в оману, поширюючи неправдиві відомості. Верифікація фотографії передбачає, головним чином, встановлення першоджерела такої світлини, її автора, місця, дати й часу зйомки, обставин появи в глобальній мережі, наявності модифікованих елементів тощо.

Перевірка походження фото (дослідження цифрового сліду того, хто та яким чином його виклав) передбачає аналіз джерела, його онлайн-історії чи пов'язаних ресурсів/профілів, часу появи, характеру взаємодії з іншими користувачами, попередньо/додатково розміщеного контенту тощо. Також зображення можуть супроводжувати теги, коментарі або інші фрагменти тексту, що здатні допомогти при ідентифікації – спробуйте «втягнути» з них потенційні ключові слова (приміром, акроніми, назви місць чи їх опис, сленг тощо). Звертайте увагу на підозрілі моменти – нещодавно створений акаунт, профіль з невеликою кількістю записів/підписників/підписок, раптову зміну географічного розташування автора, чи не є він ботом (наприклад, шляхом порівняння підписників особи з тими, на кого підписаний він сам) та ін;

Метадані EXIF (Exchangeable Image File Format) – це додаткова інформація про фотознімок, що зберігається на самому початку такого файлу до даних фактичного зображення (наприклад, марка та модель камери, її налаштування, дата, час і координати зйомки, назва програми, де здійснювалась обробка тощо). Дізнатися EXIF-відомості можна за допомогою: вкладки «Властивості» контекстного меню файлу; софту для перегляду або редагування фото/метаданих – ExifTool, Exiv2, GIMP, GeoSetter, IrfanView) вебсервісів. [12]

Визначенню достовірності зображення допоможе: його критичний огляд; дослідження сцени з різних ракурсів; визначення змін ландшафту, контент-аналіз знімку разом із супроводжуваним текстом, іншими світлинами, зробленими раніше/пізніше; додатковий зворотний пошук оригіналу зображення.

Щодня в глобальну мережу користувачі викладають величезну кількість відеоконтенту. Але його покадрова індексація пошуковими системами вимагала б значної кількості часу та ресурсів. Саме тому зворотний пошук відео, на відміну від зображень, на цей час не став базовим функціоналом вказаних систем. Bing, DuckDuckGo, Google Video, Yahoo Video Search, обмежуються відшукуванням відео за ключовими словами.

Під час визначення достовірності відео необхідно звертати увагу на деталі: невідповідність аудіодоріжки зображенню, сліди його монтування, відзеркалення відео, штучне збільшення/зменшення, додавання нових елементів (часу та дати, яскравих логотипів), зміна кольорової схеми на чорно-білу та ін.

Геолокаційний аналіз – це встановлення місцезнаходження об'єкта (стаціонарного чи рухомого) на карті, що подано у вигляді географічних

координат, поштової адреси або маршруту переміщення. Визначення локації, де була зроблена світлина (чи знято відео), зазвичай, відбувається шляхом перегляду наявності геопросторових метаданих.

Здійснення зворотного пошуку за фото (або за скриншотом з відео) для встановлення ймовірного збігу з вже відомими об'єктами чи місцинами, в тому числі за допомогою спеціалізованих сервісів – EarthKit, Geolocation Estimation, GeoSpy, GVision, Landmark Recognition, Picarta [31]

Гарною практикою є видалення з кадру неважливих елементів, що можуть заважати релевантному пошуку (люди, тварини, транспортні засоби, меблі тощо), або їх пікселізацію або розмиття з метою зосередження роботи алгоритмів пошуковиків на фоні – місцевості чи інтер'єрі. Додатково проаналізуйте назву фото (відео), дописи до нього та іншу супутню інформацію. Якщо зображене на світлині можна описати словами (приміром, готель, гора, церква), спробуйте їх віднайти мовою країни потенційного знаходження;

Детального вивчення знімку – вид з вікна, особливості будинків навколо, їх адреси, помітні елементи, зовнішня реклама, вуличні вивіски та ліхтарі, дорожні знаки та розмітка, лінії електропередач, конфігурація доріг, написи або малюнки, номерні знаки, маршрути транспорту, характерний рельєф, погодні умови, сонячні тіні, сузір'я, предмети інтер'єру, деталі одягу тощо.

API картографічних сервісів дозволяють отримувати інформацію про місцезнаходження об'єктів. Це може використовуватися для визначення маршрутів пересування осіб, локацій подій чи спостереження за географічним розташуванням об'єктів інтересу. Веб-скрапінг: API веб-скрапінгу дозволяють отримувати дані з веб- сайтів шляхом автоматизованого звертання до їхніх ресурсів. Це може бути корисно для отримання інформації про компанію, організації або події. [30]

СЕКСУАЛЬНЕ НАСИЛЬСТВО ЯК ВОЄННИЙ ЗЛОЧИН

Березовська Вероніка В'ячеславівна

студентка 3 курсу

відділення підготовки студентів

денної форми навчання інституту права та безпеки

Одеського державного університету внутрішніх справ

Науковий керівник:

Резніченко Г.С

Сексуальне насильство, яке відбувається під час збройних конфліктів, є одним із найважчих порушень міжнародного гуманітарного права та основних прав людини. Ця форма насильства стає ще більш небезпечною,

коли мова йде про дітей, оскільки вони є особливо вразливими до таких кримінальних правопорушень. Під час війни діти можуть бути використані як інструменти насильства, що призводить до їх фізичного, психічного та соціального розбиття. Ситуація стає ще складнішою в умовах сучасних збройних конфліктів, таких як війна в Україні, де сексуальне насильство над дітьми є не лише порушенням законодавства, а й серйозним гуманітарним викликом для міжнародної спільноти.

Сексуальне насильство в умовах війни підпадає під категорію воєнних кримінальних правопорушень, згідно з Римським статутом Міжнародного кримінального суду. Воно включає звалтування, примусове сексуальне рабство, примусові стерилізації та інші форми насильства, які здійснюються як щодо цивільних осіб, так і щодо військовополонених. Ці кримінальні правопорушення не лише порушують фізичну недоторканість жертв, а й наносять незліченні психологічні травми, що мають довготривалий вплив на психічний та емоційний стан постраждалих [5].

Однією з найбільших проблем є сексуальне насильство, спрямоване проти дітей. Вони, через свою безпорадність і вразливість, стають мішенями для такого насильства. Діти під час воєн можуть бути змушені ставати сексуальними рабами, а також використовуватись у бойових діях чи стати об'єктами сексуальної експлуатації. Це порушує основні права дітей, такі як право на безпеку, на розвиток, на захист від насильства та дискримінації, що є неприязними до загальноприйнятих норм гуманності [1].

Для захисту дітей від сексуального насильства міжнародне право передбачає низку важливих інструментів. Серед них важливе місце займають Конвенція ООН про права дитини, Протокол Гаазької конвенції 1999 року, що стосується захисту дітей під час збройних конфліктів, а також Римський статут, який закріплює правові норми для криміналізації сексуальних кримінальних правопорушень під час війни. Ці документи мають за мету забезпечити правовий захист дітей та відновлення їхніх прав після конфліктів [4, с.93].

Міжнародні організації відіграють важливу роль у боротьбі з сексуальним насильством в умовах воєн. ООН, ЮНІСЕФ, Міжнародний комітет Червоного Хреста та правозахисні НУО активно працюють над зниженням рівня насильства, надаючи гуманітарну допомогу, здійснюючи моніторинг ситуації в зонах конфлікту та сприяючи притягненню винних до відповідальності. Їхня діяльність включає в себе підтримку постраждалих дітей, а також роботу із забезпеченням справедливості для тих, хто скоїв ці кримінальні правопорушення.

Однак, розслідування сексуального насильства в умовах збройних конфліктів стикається з численними викликами. Відсутність доступу до постраждалих, загроза помсти свідкам, відсутність достатньої кількості доказів і політичні бар'єри значно ускладнюють здійснення правосуддя. Ці обставини дозволяють злочинцям уникати відповідальності, що додає

складнощів у боротьбі з цією проблемою на міжнародному рівні [2, с.62].

Національні ініціативи та законодавчі реформи також відіграють важливу роль у боротьбі з сексуальним насильством, особливо коли йдеться про захист дітей під час воєн. В Україні після 2014 року було ухвалено ряд законів, що криміналізують сексуальні кримінальні правопорушення, створено спеціалізовані підрозділи поліції та суддів, які займаються такими справами, а також запроваджено програми реабілітації для постраждалих. Це дозволяє створити правову основу для ефективного захисту та надання допомоги дітям, які стали жертвами насильства [5].

Діти, які пережили сексуальне насильство під час війни, часто стикаються з важкими психологічними та соціальними наслідками. Посттравматичний стресовий розлад, депресія, соціальна ізоляція, а також труднощі в реінтеграції в суспільство усе це є результатами пережитих травм. Важливо надавати дітям не лише медичну допомогу, а й психологічну підтримку, щоб мінімізувати негативні наслідки та сприяти їхньому відновленню [3, с.81].

Отже, необхідно підкреслити важливість посилення міжнародної співпраці для ефективного вирішення проблеми сексуального насильства щодо дітей під час збройних конфліктів. Це включає покращення правового регулювання, забезпечення належних умов для розслідування та притягнення до відповідальності винних, а також надання належної психологічної та соціальної допомоги дітям, які пережили ці жахливі кримінальні правопорушення. Такий підхід дозволить не лише зменшити масштаби сексуального насильства, але й сприяти відновленню постраждалих осіб у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Вік постраждалих від сексуального насильства – від 4 до 85 років», – прокурорка Діденко. LB.Ua. 24 жовтня 2022 р. URL : https://lb.ua/news/2022/10/24/533571_vik_postrazhdalih_vid_seksualnog_o.html.
2. Вознюк А. А., Жук І. В. Порушення законів і звичаїв війни : безпосередні об'єкти, предмети та потерпілі від злочину. Загальні положення «*ius in bello*». Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка. 2022. Вип. 4. С. 57–74.
3. Дудоров О. О., Задоя К. П. «Вік сексуальної згоди» у міжнародному праві, кримінально-правовій доктрині та Кримінальному кодексі України. Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка. 2019. Вип. 1. С. 75–94.
4. Задоя К. П., Дудоров, О. О. Сексуальне насильство як воєнний злочин: особливості криміналізації та кваліфікації за законодавством України. *Вісник Луганського навчально-наукового інституту імені Е.О. Дідоренка*, (2), 2023р. 90–110с.

5. Харитонова О. Сексуальне насильство, пов'язане з конфліктом, у війні рф проти України : можливості правового реагування. URL : <http://jurfem.com.ua/sexu-alne-nasylstvo-povyazane-z-konfliktom-u-viyini-rosii-proty-ukrainy>.

OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ

Богдан Віталій Петрович

курсант 202 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС

Науковий керівник:

Свинаренко Ю. П.

доктор філософії, завідувач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

З початку повномасштабного вторгнення Російської Федерації в Україну 24 лютого 2022 року світ став свідком численних воєнних злочинів, скоєних на території України. У відповідь на ці події виникла нагальна потреба у швидкому та ефективному документуванні злочинів для подальшого притягнення винних до відповідальності. У цьому контексті технології відкритої розвідки (OSINT) стали незамінним інструментом для збору, аналізу та верифікації доказів воєнних злочинів.

OSINT (Open Source Intelligence) - це метод збору та аналізу інформації з відкритих джерел, таких як соціальні мережі, новинні ресурси, супутникові знімки, відео та фотографії, опубліковані в Інтернеті. У контексті війни в Україні OSINT став ключовим інструментом для документування воєнних злочинів, особливо в умовах обмеженого доступу до окупованих територій [3, с. 149].

Одним із прикладів ефективного використання OSINT є діяльність міжнародної волонтерської спільноти InformNapalm, яка з 2014 року займається збором та аналізом відкритої інформації про участь російських військових у конфлікті на Донбасі. Зокрема, за допомогою аналізу фотографій та відео з соціальних мереж волонтери ідентифікували російських військовослужбовців, їхню техніку та місця дислокації, що стало важливим доказом присутності регулярних військ РФ на території України [7, с. 207].

Іншим прикладом є використання супутникових знімків для виявлення масових поховань та руйнувань цивільної інфраструктури. Так, у місті Буча

Київської області, де були зафіксовані масові вбивства мирних жителів, супутникові знімки допомогли підтвердити наявність братських могил та зафіксувати переміщення військової техніки [6, с. 258].

Крім того, український уряд активно використовує цифрові інструменти для збору доказів воєнних злочинів. Зокрема, було створено чат-бот «eВорог», який дозволяє громадянам надсилати фото- та відеодокази злочинів, що автоматично фіксуються з геолокацією та часовими мітками. Ці дані передаються до Офісу Генерального прокурора та можуть бути використані в міжнародних судових процесах [2, с. 318].

Важливу роль у документуванні злочинів відіграють також міжнародні організації, такі як Bellingcat та OSINT for Ukraine, які спеціалізуються на аналізі відкритих джерел для виявлення та верифікації фактів порушення міжнародного гуманітарного права. Наприклад, Bellingcat опублікувала розслідування щодо обстрілів цивільних об'єктів у Маріуполі, використовуючи відео з соціальних мереж, супутникові знімки та інші відкриті джерела для підтвердження фактів злочинів [1, с. 18].

Застосування OSINT-технологій також дозволяє протидіяти дезінформації та пропаганді. Шляхом аналізу та спростування фейкових новин, що поширюються через проросійські медіа, OSINT-спільноти сприяють формуванню об'єктивної картини подій та забезпечують прозорість інформаційного простору [5, с. 253].

Проте використання OSINT має свої обмеження. Зокрема, виникають питання щодо автентичності та достовірності зібраної інформації, необхідності верифікації даних та дотримання етичних норм при роботі з чутливими матеріалами. Також існує ризик використання фальсифікованих матеріалів або маніпуляцій з боку недобросовісних акторів.

Застосування OSINT-технологій у документуванні воєнних злочинів під час війни в Україні продемонструвало їхню ефективність та значущість у сучасному інформаційному середовищі. Завдяки відкритим джерелам вдалося зібрати значну кількість доказів злочинів, скоєних російськими військами, що стало основою для розслідувань як на національному, так і на міжнародному рівнях.

Однак для забезпечення надійності та легітимності зібраних даних необхідно розробити стандартизовані методики верифікації та зберігання інформації, а також забезпечити навчання фахівців у сфері OSINT. Крім того, важливо враховувати етичні аспекти роботи з чутливими даними та забезпечити захист прав осіб, які надають інформацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний poradnik / Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Х.: ІПЮК для СБУ, 2023. 36 с.
2. Кисельов А.О. Досвід використання підрозділами Національної поліції технологій «OSINT» у протидії кримінальним правопорушенням / А.

- Кисельов // Міжнародна та національна безпека: теоретичні і прикладні аспекти: матеріали VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 березня 2022 р.). Дніпро, 2022. С. 318-319.
3. Одерій О.В., Кожевніков О.А. отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. Правовий часопис Донбасу. 2020. № 4 (73) 2020. С. 144 –155.
 4. Панченко І. В. Цифрові технології в роботі з джерелами інформації / І. В. Панченко. Одеса: Університет Ушинського. 2023. 27 с.
 5. Пчеліна О. В., Фоміна Т. Г. Особливості проведення огляду місця події під час досудового розслідування злочинів, пов'язаних зі збройною агресією проти України. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2023. № 2. С. 251–259.
 6. Сидоренко Д. В. Поняття спеціальних знань у кримінальному провадженні. Право і суспільство. 2022. № 6. С. 253–260.
 7. Яровий Т. С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. Експерт: парадигми юридичних наук і державного управління. 2019. № 4(6). С. 201 – 208.

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT

Бойченко Вікторія Юрївна

курсантка 2-го курсу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Науковий керівник:

Поляков С. В.

доцент кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
к.ю.н., доцент, полковник поліції

У сучасному світі, де обсяг відкритої інформації швидко зростає, ефективне використання OSINT (Open-Source Intelligence) стає ключовим фактором для отримання цінних інсайтів у різних сферах діяльності. Здатність швидко та якісно збирати, обробляти та аналізувати публічно доступні дані є надзвичайно важливою. Розвиток практичних інструментів та алгоритмів для роботи з OSINT-даними відіграє вирішальну роль у підвищенні ефективності цього процесу.

Теоретичні основи та ключові поняття OSINT. Розвідка з відкритих джерел (OSINT - Open Source Intelligence) представляє собою методологію збору, аналізу та використання даних и публічно доступних джерел інформації для прийняття рішень та проведення досліджень.

Специфіка роботи з відкритими джерелами вимагає розуміння основних категорій інформації та їх характеристик. Процес збору даних потребує систематичного підходу та використання спеціалізованих інструментів для автоматизації пошуку та обробки інформації. Принципи OSINT передбачають постійне оновлення методів роботи та адаптацію до нових джерел інформації

Процес аналізу інформації OSINT вимагає використання різних технічних інструментів та програмного забезпечення. Інструменти OSINT включають спеціалізовані пошукові системи, програмне забезпечення для моніторингу соціальних мереж, інструменти візуалізації даних та аналітичні платформи.

Практичні інструменти для збору OSINT-інформації повинні відповідати вимогам законності, оперативності та можливості використання отриманих даних як доказів у кримінальних провадженнях. Категорії та конкретні інструменти, які можуть бути корисними:

1. Інструменти для ідентифікації та верифікації осіб:
державні реєстри України (з офіційним доступом);

єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань (ЄДР);

державний реєстр речових прав на нерухоме майно;

реєстр транспортних засобів МВС;

бази даних Державної міграційної служби.

Інструменти для аналізу соціальних мереж (з урахуванням публічних даних):

спеціалізовані платформи для аналізу соціальних мереж, які дозволяють ідентифікувати профілі, встановлювати зв'язки, аналізувати публікації;

інструменти для пошуку за зображеннями (Google Images, TinEye);

інструменти для аналізу відео (InVID WeVerify).

3. Інструменти для відстеження цифрових слідів:

Інструменти аналізу веб-сайтів та інтернет-інфраструктури;

Інструменти для моніторингу онлайн-активності.

4. Інструменти для геолокації та аналізу картографічних даних:

Google Earth Pro;

OpenStreetMap.

5. Інструменти для аналізу великих обсягів даних:

інструменти для роботи з табличними даними (наприклад, Microsoft Excel, Google Sheets);

прості інструменти для візуалізації даних (наприклад, Google Charts).

Алгоритм аналізу OSINT-даних - це систематизований набір кроків та процедур, які використовуються для збору, обробки, аналізу та інтерпретації інформації, отриманої з відкритих джерел, з метою отримання цінних інсайтів та відповідей на конкретні дослідницькі питання.

Розвідка на основі відкритих джерел включає чітку послідовність етапів для отримання та обробки даних:

Збір даних. Визначте мету дослідження та збирайте якомога більше даних. Уникайте зайвих відгалужень, які не сприяють вашому OSINT розслідуванню.

Організація інформації. Перетворіть хаотичні дані на структуровану систему, яка дозволить виявляти патерни.

Інтерпретація знахідок. Критично оцініть отримані дані, аналізуйте їх об'єктивно і робіть логічні висновки.

Перевірка надійності. Фактчекінг і перевірка надійності джерел є ключовими для OSINT розслідувань.

Зробіть висновки. Використовуйте отриману інформацію для прийняття рішень або запобігання ризикам.

Методи OSINT - це комплексна система технічних рішень і методологічних підходів для ефективного збору й аналізу інформації з відкритих джерел. До цих методів відноситься: розпізнавання об'єктів, що використовує алгоритми комп'ютерного зору, зокрема глибоке навчання (deep learning), для автоматичної ідентифікації та локалізації різних об'єктів

на зображеннях. Технології, такі як CNN, YOLO та R-CNN, є передовими в цій галузі, дозволяючи точно визначати, що саме зображено на фотографії або відео; аналіз метаданих: метадані - це прихована інформація, вбудована у файли зображень. Їхній аналіз дозволяє отримати важливий контекст, такий як час і місце створення знімка, технічні характеристики камери, що може бути корисним для розслідувань, верифікації або просто для розуміння походження зображення; геолокація зображень: визначення точного місця зйомки може бути критично важливим у багатьох ситуаціях, від журналістських розслідувань до правоохоронної діяльності. Використання GPS-координат є найточнішим методом, але якщо вони відсутні, можуть застосовуватися методи аналізу зображення на наявність відомих орієнтирів або триангуляція на основі кількох зображень однієї місцевості; перевірка автентичності: в епоху цифрових маніпуляцій надзвичайно важливо мати методи для перевірки справжності візуального контенту. ELA аналізує рівень стиснення різних частин зображення для виявлення нерівномірностей, DCT є основою для багатьох алгоритмів стиснення і його аналіз може виявити артефакти редагування, а шумовий аналіз досліджує статистичні характеристики шуму на зображенні, які можуть змінюватися при маніпуляціях; пошук за зображенням: замість текстового опису цей метод дозволяє знайти візуально схожі зображення. CBIR використовує алгоритми для порівняння низькорівневих (колір, текстура, форма) або високорівневих (семантичний зміст) ознак зображень. Перцептивні хеші генерують унікальний «відбиток» зображення, що дозволяє швидко знаходити візуально подібні, навіть якщо вони були незначно змінені.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Юридичний науковий електронний журнал http://www.lsej.org.ua/9_2021/85.pdf
2. Кваліфікаційна робота; Західноукраїнський національний університет; Факультет комп'ютерних інформаційних технологій “Алгоритми розвідки з відкритих джерел в задачах кібербезпеки / Intelligence Algorithms for Open Sources in Cyber Security Tasks” - П.Я.Билень
3. Що Таке OSINT у 2025: Гайд від Molfar. <https://molfar.com/blog/shcho-take-osint-u-2024-gaid-vid-molfar>

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ТА НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Бойчук Олександра Олександрівна

курсант 201 взводу навчально-наукового інституту підготовки фахівців підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ

Тригуб С. М.

доктор філософії, викладач кафедри оперативного-розшукової діяльності навчально-наукового інституту підготовки фахівців підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ

У сучасному світі, де цифрові технології стрімко розвиваються та проникають у всі сфери життя – від особистого спілкування до державного управління, – правоохоронні органи стикаються з новими, все більш складними викликами. Одними з найактуальніших серед них є кіберзлочинність, а також необхідність оперативного й ефективного кримінального аналізу великих обсягів інформації. Такі виклики вимагають від правоохоронної системи не лише високого рівня технічної підготовки персоналу, але й постійного вдосконалення нормативно-правової бази. Лише за умови належного правового регулювання та впровадження сучасних технологій можна забезпечити дієву протидію злочинності у цифровому середовищі та захист прав громадян. Актуальність дослідження визначеної теми зумовлена також науковими дискусіями щодо доцільності та меж використання штучного інтелекту у сфері безпеки, які активізувалися після затвердження Кабінетом Міністрів України «Концепції розвитку штучного інтелекту в Україні» від 2 грудня 2020 року № 1556-р. [1].

Так, цифрова криміналістика стала невід'ємною частиною сучасної криміналістики, спрямованою на виявлення, збирання, фіксацію, збереження, аналіз та інтерпретацію електронних доказів, що мають значення для кримінального провадження. Її завданням є дослідження цифрових слідів, які виникають у результаті злочинної діяльності в інформаційному просторі, зокрема в мережі Інтернет, на електронних носіях, у мобільних пристроях і в хмарних сховищах даних. У період воєнного стану в Україні актуальність цифрової криміналістики зростає. Н. Братішко зазначає, що цифрова криміналістика – це новітній напрям криміналістики, що являє собою прикладну науку, зосереджену на розкритті кримінальних правопорушень, пов'язаних із комп'ютерною інформацією. Вона вивчає цифрові докази, а

також методи їх виявлення, вилучення, фіксації та дослідження [2, с. 286].

У сучасних умовах зростає як науковий, так і практичний інтерес до цифрових криміналістичних інструментів, які відіграють надзвичайну роль у виявленні та розслідуванні воєнних злочинів, сприяючи не лише розкриттю злочинів, а й забезпеченню неминучості покарання для осіб, причетних до таких дій. К. Латиш зазначає, що в умовах війни, де традиційні методи збору доказів можуть бути ускладнені, цифрові інструменти надають слідчим нові можливості для збору та аналізу даних. Особливу увагу приділяється пошуку та аналізу інформації за заздалегідь підготовленими списками ключових слів і хештегів, що можуть вказувати на планування або здійснення злочинів, а також на визначення місця та часу подій. Значним елементом розслідування є також аналіз супутникових знімків, які дають змогу відстежувати зміни на місцевості, виявляти масштаби руйнувань або рухи військової техніки [3, с. 32].

Крім того, застосування технологій обробки великих обсягів даних (Big Data) дозволяє виявляти приховані зв'язки між подіями, особами і навіть державами, що можуть бути критичними для розкриття складних воєнних злочинів. Геолокаційні мітки, що містяться у фото- та відеоматеріалах, здатні не лише підтвердити або спростувати факти, але й надати точну інформацію про місце події, час її виникнення та особи, що були до неї причетні. Використання відкритих джерел та тих, що надаються слідством, дозволяє ефективно відслідковувати зміни в інформаційному полі та ідентифікувати осіб, які могли брати участь у злочинах. Великого значення набувають також програмні засоби для обробки цифрових зображень та аналізу телефонних розмов, електронних пристроїв, ігрових платформ. Використовуються також системи розпізнавання облич, що допомагають ідентифікувати підозрюваних або загиблих за допомогою зображень, отриманих з камер спостереження або соціальних мереж. В Україні для ідентифікації підозрюваних і загиблих застосовується додаток Clearview AI, що здійснює розпізнавання облич з бази даних відкритих зображень і відео, наданих слідчим органам.

Кримінальний аналіз кіберзлочинності вимагає врахування специфіки цифрових злочинів, які характеризуються високою динамікою та складністю. Дослідження Д. Войтенка, А. Шрама та А. Кисельова підкреслює необхідність адаптації методів кримінального аналізу до особливостей кіберзлочинності, зокрема, врахування нових способів вчинення злочинів та використання сучасних технологій. Кіберзлочинність нині становить одну з найсерйозніших загроз для безпеки й стабільності процесів як у суспільному, так і в державному житті. Збройна агресія Росії проти України лише загострила цю проблему, спричинивши активний пошук нових, більш ефективних механізмів протидії кіберзагрозам. У результаті питання правового регулювання у сфері боротьби з кіберзлочинністю набуло особливої актуальності та стало пріоритетним напрямом державної політики у сфері національної безпеки [4, с. 203].

Крім того, І. Рафальський, С. Соха, С. Савчук та Р. Здибель

стверджують на необхідності вдосконалення державної кримінально-правової політики протидії кіберзлочинності, що включає аналіз наукових досліджень та розробку ефективних стратегій боротьби з кіберзагрозами. Основна увага дослідників зосереджена на фундаментальних аспектах кібербезпеки, зокрема на захисті критичної інфраструктури, протидії кібератакам та запобіганні кіберзлочинності. При цьому спостерігається виражений міждисциплінарний підхід, що охоплює елементи інформаційної безпеки, інтелектуальних технологій і соціально-економічного аналізу [5, с. 114].

Захист прав людини у кіберпросторі є значним аспектом нормативно-правового регулювання. Н. Сперкач та В. Ковбасюк вказують на необхідність вдосконалення правового регулювання для забезпечення захисту користувачів в Інтернеті та зміцнення довіри громадян до цифрового середовища. Автори вважають, що необхідною є реалізація освітніх ініціатив та методів захисту в Інтернет-просторі. Крім того, необхідно розробити, активно впроваджувати та реалізовувати Стратегію цифрового громадянства, що допоможе зміцнити правову свідомість громадян у цифровому середовищі [6, с. 789].

Інтеграція штучного інтелекту (ШІ) у правоохоронну діяльність відкриває нові можливості для протидії кримінальним правопорушенням. О. Герасименко вказує, що об'єкти критичної інфраструктури – зокрема енергетичні системи, транспортні мережі, системи водопостачання та зв'язку – є ключовими для стабільного функціонування держави та гарантування безпеки її громадян. В умовах воєнного стану ці об'єкти дедалі частіше стають мішенню для кримінальних правопорушень, що здійснюються із застосуванням сучасних цифрових технологій. Зокрема, загрозу становлять кіберзлочинність, терористичні атаки, диверсії та інші форми протиправної діяльності. У зв'язку з цим виникає нагальна потреба у впровадженні новітніх інформаційно-аналітичних інструментів та технологій штучного інтелекту для ефективного виявлення, запобігання та протидії таким загрозам. Інформаційно-аналітичне забезпечення дає змогу оперативного збирати, обробляти та аналізувати великі масиви даних з різноманітних джерел, виявляти закономірності та формувати прогнози щодо потенційних ризиків. Застосування штучного інтелекту, зокрема в автоматизованому аналізі інформації, розпізнаванні образів та підтримці прийняття рішень, істотно підвищує ефективність заходів із захисту критичної інфраструктури [7, с. 686].

Отже, сучасні виклики у сфері кібербезпеки та кримінального аналізу вимагають комплексного підходу, що включає розвиток цифрової криміналістики, адаптацію кримінального аналізу до специфіки кіберзлочинності, вдосконалення нормативно-правового регулювання та інтеграцію новітніх технологій, таких як штучний інтелект, у правоохоронну діяльність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р.

- Кабінет Міністрів України : офіц. сайт. URL: <https://www.kmu.gov.ua/pras/pro-shvalennya-koncepciyi-rozvitkushtchnogo-intelektu-v-ukrayini-s21220> (дата звернення: 10.05.2025).
2. Братішко Н. Напрями використання цифрової криміналістики в умовах воєнного стану. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2024. № 2. С. 282–288. URL: <https://doi.org/10.31733/2078-3566-2023-6-282-288>. (дата звернення: 10.05.2025).
 3. Латиш К. В. 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.
 4. Войтенко Д., Шрам А., Кисельов А. Кримінальний аналіз кіберзлочинності: специфіка та сучасні виклики. *Universum*. 2024. № 8. С. 201–204. URL: <https://archive.liga.science/index.php/universum/article/view/1002> (дата звернення: 10.05.2025).
 5. Рафальський І., Соха С., Савчук С., Здибель Р. Сучасний стан наукових досліджень з проблем державної кримінально-правової політики протидії кіберзлочинності. *Society and Security*. 2024. № 6(6). С. 103–115. URL: [https://doi.org/10.26642/sas-2024-6\(6\)-103-115](https://doi.org/10.26642/sas-2024-6(6)-103-115) (дата звернення: 10.05.2025).
 6. Сперкач Н. А., Ковбасюк В. С. Напрями запобігання кіберзлочинності та вдосконалення правового регулювання захисту прав людини у кіберпросторі. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 785–790.
 7. Герасименко О. М. Проблеми та перспективи застосування штучного інтелекту у протидії Службою безпеки України кримінальним правопорушенням на об'єктах критичної інфраструктури. *Аналітично-порівняльне правознавство* / редкол.: Ю. М. Бисага (голов. ред.), В. В. Заборовський, Д. М. Белов, С. Б. Булеца та ін. Ужгород : ДВНЗ «УжНУ», 2024. № 5. С. 680–687. URL: <http://journal-app.uzhnu.edu.ua/article/view/313148/304189> (дата звернення: 10.05.2025).

ІНСТИТУЦІЙНЕ СТАНОВЛЕННЯ ТА ФОРМУВАННЯ СТАНДАРТІВ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Боцу Тетяна Петрівна

курсант 212 взводу навчально-наукового інституту
підготовки фахівців підрозділів кримінальної поліції
Національної поліції України Одеського
державного університету внутрішніх справ

Тригуб С. М.

доктор філософії, викладач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України Одеського
державного університету внутрішніх справ

У сучасних умовах глобальної цифровізації суспільства питання кримінального аналізу та кібербезпеки набули особливої актуальності в системі забезпечення національної безпеки України. Інституційне становлення цих напрямів правоохоронної діяльності є відповіддю на зростання кіберзагроз, транснаціональної злочинності, гібридних форм агресії та інформаційних впливів, що набувають все більш складних і технічно досконалих форм.

Кримінальний аналіз як інструмент стратегічного управління безпекою формувався в Україні поступово, під впливом європейських стандартів та рекомендацій Інтерполу, Європолу і ОБСЄ. Уперше потребу в систематичному зборі, обробці, класифікації й прогнозуванні інформації про злочинність та її динаміку було офіційно визнано після реформування органів внутрішніх справ у 2015–2016 роках. Національна поліція України створила підрозділи аналітичного забезпечення, які займаються розробкою профілів злочинної поведінки, просторово-часовою візуалізацією правопорушень, ідентифікацією кримінальних трендів та оцінкою ризиків. Таким чином, інституційне становлення кримінального аналізу стало складовою частиною переходу до сучасної моделі «інтелектуальної поліції» [1, с. 76].

Законодавчі передумови для формування стандартів кримінального аналізу базуються, зокрема, на Законах України «Про Національну поліцію», «Про оперативно-розшукову діяльність», а також підзаконних актах Міністерства внутрішніх справ. У 2019 році було ухвалено Концепцію розвитку кримінального аналізу в системі Національної поліції, яка передбачає адаптацію до стандартів Європейського кримінального розвідувального моделювання (EUCRIM). Особлива увага надається розбудові кримінальної аналітики у сфері організованої

злочинності, тероризму, торгівлі людьми, наркотрафіку та злочинів, пов'язаних із корупцією [3].

У свою чергу, кібербезпека як частина національної безпеки України почала інституційно оформлюватися після ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» (2017 р.). Цей нормативний акт визначив суб'єктів кібербезпеки (СБУ, Державну службу спеціального зв'язку та захисту інформації, Національну поліцію тощо) і окреслив ключові принципи кіберзахисту. Водночас у 2021 році було затверджено оновлену Кібербезпекову стратегію України, що передбачає впровадження проактивного підходу до виявлення, нейтралізації та попередження кіберзагроз, з особливим акцентом на захист критичної інфраструктури, державних інформаційних систем та персональних даних громадян [3].

Особливістю формування стандартів у сфері кібербезпеки в Україні є орієнтація на міжнародні рекомендації: ISO/IEC 27001, NIST, стандарти НАТО та директиви Європейського Союзу. Впровадження систем управління інформаційною безпекою (СУІБ) у державному секторі, сертифікація фахівців із кіберзахисту, створення Національного координаційного центру кібербезпеки при РНБОУ стали важливими етапами у становленні інституційного середовища. Крім того, Україна активно співпрацює з Європейським агентством з кібербезпеки (ENISA) та іншими міжнародними партнерами в межах програм Twinning та Horizon Europe.

Для вирішення цих проблем доцільно вжити комплексних заходів. Насамперед необхідно оновити законодавство в частині кримінальної аналітики, запровадивши єдині національні стандарти, розроблені відповідно до міжнародних рекомендацій (зокрема Європолу та ENISA). Важливим кроком є створення централізованої аналітичної платформи на базі Національної поліції, що дозволить об'єднати різні джерела оперативної інформації в єдиний масив даних. Також слід забезпечити системну підготовку кадрів – аналітиків, кіберекспертів, операторів інформаційних систем – у співпраці з вітчизняними університетами та закордонними партнерами.

У сфері кібербезпеки одним із пріоритетів має стати посилення кіберзахисту критичної інфраструктури, зокрема енергетичного сектору, телекомунікацій та урядових порталів. Для цього необхідне не лише вдосконалення технічної бази, а й розбудова ефективного механізму кібермоніторингу, швидкого реагування на інциденти та обміну інформацією між державою та приватним сектором. Крім того, важливо створити стабільну фінансову основу для кібербезпеки, передбачивши окреме бюджетне фінансування як на національному рівні, так і в регіонах [4, с. 32].

Узагальнюючи, можна стверджувати, що інституційне становлення кримінального аналізу та кібербезпеки в Україні перебуває на етапі активного формування, однак потребує подальшого поглиблення. Проблеми

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 переосмисленні 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 нарративу, 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, балансує 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

1. 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>.
2. 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 напрямку 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

спеціалізовані центри в межах Міністерства внутрішніх справ, Державного бюро розслідувань, Служби безпеки України, використовуються інструменти просторового аналізу (наприклад, Stime Mapping), аналізу соціальних зв'язків, побудови профілів злочинних груп.

Проте цей напрям залишається ще не до кінця розвиненим. Існують проблеми з кадровим забезпеченням, відсутністю єдиних стандартів кримінального аналізу, а також із міжвідомчою координацією.

Україна з 2014 року перебуває в стані гібридної війни, де кіберпростір є одним з головних полів битви. У зв'язку з цим питання кібербезпеки стало одним із пріоритетів національної безпекової політики.

До основних кроків держави у цьому напрямі можна віднести:

1) прийняття Закону України «Про основні засади забезпечення кібербезпеки», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки;

2) створення Державного центру кіберзахисту Держспецзв'язку, який входить до загальної структури Державної служби спеціального зв'язку та захисту інформації України. Основними завданнями Державного центру кіберзахисту Держспецзв'язку є:

- провадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки;
- забезпечення створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет;
- забезпечення створення та функціонування системи антивірусного захисту національних інформаційних ресурсів;
- аудит інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури;
- забезпечення створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту;
- забезпечення створення та функціонування системи взаємодії команд реагування на комп'ютерні надзвичайні події;
- у взаємодії з іншими суб'єктами забезпечення кібербезпеки, розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм та методик проведення кібернавчачь;
- створення та забезпечення функціонування Національного центру резервування державних інформаційних ресурсів.

3) посилення підрозділів кіберполіції, які займаються розслідуванням кіберзлочинів, включаючи фінансові шахрайства, фішинг, злам систем та

розповсюдження шкідливого програмного забезпечення.

Кібербезпека також охоплює захист критичної інфраструктури – енергетичних систем, транспортних мереж, медичних установ, банківської сфери.

Попри значний прогрес, існує низка проблем, які стримують розвиток кримінального аналізу та посилення кібербезпеки:

- відсутність єдиної державної стратегії розвитку кримінального аналізу;

- не визначені стандарти збору, обробки й обміну аналітичними даними між відомствами;

- відсутність системної вищої освіти за цим напрямом;

- обмежене впровадження автоматизованих систем обробки великих даних;

- нестача фахівців з аналітичних та кібербезпекових компетенцій;

- низька цифрова обізнаність пересічного населення, що робить його вразливим до соціальної інженерії;

- недостатня взаємодія між державними структурами, приватним сектором та академічною спільнотою.

Розвиток кримінального аналізу та кібербезпеки в Україні стримується як об'єктивними (війна, ресурсні обмеження), так і системними (недостатня координація, відставання у підготовці кадрів, правова неврегульованість) чинниками. Усунення цих бар'єрів є критично важливим для ефективної безпекової політики держави у найближчі роки.

З огляду на поточні виклики, перспективи розвитку кримінального аналізу та кібербезпеки в Україні мають спиратися на: інституціоналізацію кримінального аналізу – створення Національного центру або платформи для міжвідомчої аналітики; інвестиції у кіберосвіту - навчання нових фахівців, програми з перекваліфікації; розвиток державно-приватного партнерства у сфері кібербезпеки; міжнародну інтеграцію – участь у глобальних кіберальянсах, обмін інформацією про кіберінциденти.

Кримінальний аналіз та кібербезпека є взаємопов'язаними інструментами у сучасній системі безпеки. Їхній розвиток в Україні потребує стратегічного підходу, міжвідомчої координації, кадрового зміцнення та інтеграції найкращих світових практик.

Системний підхід до цих питань дозволить Україні не лише ефективно протидіяти загрозам, але й стати повноцінним учасником міжнародної кіберспільноти, здатним протистояти найскладнішим викликам ХХІ століття.

КРИМІНАЛЬНИЙ АНАЛІЗ У ПРОТИДІІ КІБЕРЗЛОЧИННОСТІ: СПЕЦИФІКА ТА СУЧАСНІ ВИКЛИКИ

Григор'єва Валерія Михайлівна

*студентка 3 курсу 4 групи
відділення підготовки студентів денної
форми навчання інституту права та безпеки
спеціальності 081 «Право»*

*Одеського державного університету внутрішніх справ
Науковий керівник:*

Албул С. В.

*кандидат юридичних наук, професор, професор кафедри
оперативно-розшукової діяльності навчально-наукового
інституту підготовки фахівців для підрозділів
кримінальної поліції НПУ ОДУВС*

Кримінальний аналіз як окремий напрямок діяльності поліції почав активно розвиватися у 60–70-х роках ХХ століття, коли у США різко підвищився рівень злочинності, що стимулювало ухвалення спеціального закону для боротьби з нею. У рамках цих змін було створено розвідувальні підрозділи з аналітичними командами, засновано Агентство фінансової допомоги правоохоронним органам і розроблено методичні матеріали для кримінальних аналітиків. Наприкінці 1970-х років впровадили Комплексну програму кримінального попередження ІСАР, яка сприяла підвищенню професійного рівня в цій галузі. У середині 1990-х запровадження картографічних методів дозволило створювати тривимірні моделі злочинів, додаючи новий вимір до аналізу даних. Протягом 1990-х років, зі становленням інформаційного суспільства, поліція змінила стратегії протидії злочинності, що привело до створення Міжнародної асоціації кримінальних аналітиків (ІАСА). Унаслідок цих зрушень у структурі Генерального секретаріату Інтерполу з'явився підрозділ кримінального аналізу, а діяльність Європолу вже базується на відповідних технологіях і результатах цієї сфери [2, с. 11; 7, с. 26].

Підрозділи кримінального аналізу реалізують аналітичний процес, який складається з кількох етапів: планування та визначення напрямків роботи, збору й оцінки даних, співставлення інформації, її аналізу, поширення результатів і повторного перегляду отриманих даних щодо підозрюваних, злочинців або організацій. Основна мета полягає у формуванні ґрунтовної бази знань, що дозволяють правоохоронним органам більш проактивно реагувати на правопорушення [7, с. 28]. Це включає можливість ідентифікації та оцінки намірів злочинних угруповань у межах відповідної юрисдикції. Вивчення структури та методів їх діяльності дає змогу прогнозувати тенденції у кримінальному світі та за певних умов навіть попереджувати майбутні кримінальні правопорушення [1, с. 102].

Кримінальний аналіз передбачає встановлення зв'язків між інформацією про злочинну діяльність та іншими релевантними даними. Його завдання також охоплюють оцінку, інтерпретацію та прогнозування розвитку злочинних ситуацій для подальшого практичного застосування результатів у досудовому розслідуванні, оперативно-розшуковій роботі чи формуванні стратегічних і тактичних планів боротьби зі злочинністю [7, с. 32]. Цей вид аналізу поділяється на загальний і спеціалізований. Загальний аналіз охоплює широкий спектр видів злочинності та зазвичай використовується у невеликих відомствах або в межах обмежених юрисдикцій. Спеціалізований аналіз спрямований на окремі типи злочинних проявів чи конкретні об'єкти, наприклад, наркаторгівлю, промислове шпигунство або діяльність організованих злочинних груп [2, с. 16-17].

Поняття кіберзлочинності у досить вузькому сенсі закріплене в Законі України «Про основні засади забезпечення кібербезпеки України» [6]. Згідно з цим законом, кіберзлочин визначається як суспільно небезпечна винна дія, що здійснюється у кіберпросторі або з його використанням, за яку передбачена відповідальність відповідно до закону України про кримінальну відповідальність чи яка визнається злочином згідно з міжнародними договорами України [6]. Основними ознаками кіберзлочинності є: анонімність, здійснення у кіберпросторі, можливість значної віддаленості між жертвою та злочинцем, високий рівень прихованості та потреба у спеціалізованих знаннях і навичках [3, с. 35; 4, с. 23].

Кіберзлочинність із кожним днем набуває все більшого поширення, а кількість таких кримінальних правопорушень стрімко зростає. Регулярно з'являються нові види правопорушень, для протидії яким необхідно розробляти спеціальні методи боротьби. Це створює низку проблем, адже виявити та затримати кібершахрая набагато складніше, ніж злочинця, який діє у фізичному просторі. Протидія кіберзлочинам ускладнюється різноманітними факторами:

кіберзлочинці – це не звичайні правопорушники, а висококваліфіковані фахівці, які майстерно приховуються за моніторами своїх комп'ютерів. Їхнє виявлення є набагато складнішим завданням, ніж пошук злочинця, що діє відкрито;

співробітники правоохоронних органів, стикаючись із кіберзлочинами, часто потребують допомоги експертів у галузі програмування. Проте кваліфікованих спеціалістів у цій сфері досі недостатньо;

контроль за вже існуючими видами кіберзлочинності є складним через їхню постійну еволюцію та появу нових форм [4, с. 23].

У сучасному світі кіберзлочинність становить серйозну загрозу як для суспільства загалом, так і для його інформаційної безпеки. Вона породжує безліч соціальних проблем, які потребують негайного реагування та ефективних рішень. У значній мірі масштаб кіберзлочинності залишається поза офіційною статистикою. За деякими оцінками, до офіційних даних потрапляє лише 10%, у найкращому разі – 20% усіх скоєних правопорушень

[4, с. 24]. Саме тому, за нашим переконанням, значний потенціал у протидії кіберзлочинам притаманний саме кримінальному аналізу, який в змозі надавати постійну дієву допомогу іншим правоохоронним органам.

Підсумовуючи вищевикладене, можна дійти висновку, що зростання кіберзлочинності вимагає від правоохоронців нового підходу, заснованого на кримінальному аналізі. Це дозволяє системно вивчати злочини, визначати тенденції, встановлювати зв'язки та прогнозувати ризики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Албул С.В. Оперативно-розшукова діяльність: навчальний посібник / С. В. Албул, С. О. Єгоров, Є. В. Поляков, Т. Г. Щурат; за заг. ред. проф. С. В. Албула. Одеса : ОДУВС, 2023. 375 с.
2. Албул С.В. Основи кримінального аналізу: посібник з елементами тренінгу / Албул С.В., Користін О.Є., Заєць О.М., Ісмаїлов К.Ю., Тетерятник Г.К., Горбаньов І.М. Одеса : ОДУВС, 2016. 112 с.
3. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.
4. Любавіна В.П. Сутність кіберзлочинності та способи боротьби. *Молодий вчений*. 2022. № 8(108). С. 22–25.
5. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 р. № 2163-VIII [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 11.05.2025).
6. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: ЛьвДУВС, 2021. 228 с.

OSINT – ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ

Єйбог Олександр Ігорович

курсант 211 взводу навчально-наукового інституту підготовки фахівців підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ

Тригуб С. М.

доктор філософії, викладач кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ

У сучасних умовах збройних конфліктів, особливо на тлі війни в Україні, зростає потреба у використанні відкритих джерел інформації для фіксації, аналізу та доказування фактів скоєння воєнних злочинів. Відкриті

джерела розвідки (Open Source Intelligence — OSINT) є критично важливим інструментом у діяльності журналістів-розслідувачів, правозахисників, міжнародних трибуналів і незалежних слідчих органів. Застосування OSINT-технологій дає змогу швидко виявляти та документувати потенційні порушення міжнародного гуманітарного права, зокрема обстріли цивільної інфраструктури, катування, масові поховання, насильницькі депортації тощо.

OSINT охоплює аналіз інформації, отриманої з відкритих джерел, таких як супутникові знімки, відео з соціальних мереж (YouTube, Telegram, Twitter/X), фотоматеріали, геолокаційні дані, метадані файлів, публічні бази даних, а також повідомлення ЗМІ. За допомогою інструментів цифрової криміналістики (наприклад, Google Earth, InVID, Bellingcat Toolkit, Amnesty Evidence Lab) можливо встановити точне місце, час та обставини події, що дозволяє формувати доказову базу для подальших юридичних процесів. Крім того, OSINT-дослідження забезпечують можливість відстеження послідовності подій і верифікації інформації навіть у разі її знищення або офіційного заперечення [1, с. 65].

Суттєвою перевагою OSINT у розслідуванні воєнних злочинів є оперативність та доступність. OSINT-дослідження часто випереджають офіційні розслідування державних структур або міжнародних організацій, надаючи актуальні докази для реакції громадськості та інституцій. Наприклад, завдяки аналізу супутникових знімків та відео, активісти міжнародної спільноти змогли задокументувати факти вбивств у Бучі, руйнування Маріупольського драматичного театру та удари по цивільним об'єктам у Херсонській і Харківській областях. OSINT дозволив відстежити маршрути переміщення російських військ, встановити серійні номери техніки та зброї, а також ідентифікувати конкретних військовослужбовців [2, с. 18].

Проте ефективне застосування OSINT вимагає дотримання низки етичних і юридичних принципів. Особливу увагу слід приділяти питанням автентичності джерел, дотримання приватності осіб, які можуть бути зафіксовані на відео чи фото, уникнення маніпуляцій або фальсифікацій. Також необхідне правове закріплення використання відкритих джерел як допустимих доказів у судових процесах, особливо у справах про воєнні злочини, геноцид чи злочини проти людяності. В цьому контексті важливою є практика Міжнародного кримінального суду, яка поступово починає визнавати OSINT-матеріали як докази у провадженнях [3].

Отже, у ході дослідження було встановлено, що OSINT-технології (розвідка на основі відкритих джерел) посідають особливе місце в сучасному інструментарії документування воєнних злочинів. Їхня ефективність полягає у швидкому зборі, аналізі, верифікації та збереженні доказів, які мають суттєве значення у кримінальних провадженнях, зокрема в умовах воєнного конфлікту, коли традиційні слідчі механізми можуть бути ускладнені або тимчасово недоступні. Використання супутникових знімків, відео з соціальних мереж, геолокаційних даних і цифрових слідів дозволяє не лише встановлювати факт

злочину, але й ідентифікувати його виконавців, визначити місце, час і масштаби порушень норм міжнародного гуманітарного права.

Важливою науковою тезою є визнання OSINT як повноцінного елементу доказової бази в контексті міжнародного правосуддя. Попри виклики, пов'язані з автентичністю джерел, дотриманням стандартів приватності та необхідністю технологічної експертизи, практика міжнародних судів, таких як Міжнародний кримінальний суд (МКС) чи спеціальні трибунали, поступово схиляється до активного використання відкритих цифрових доказів. Це свідчить про еволюцію сучасної криміналістики та потребує подальшого наукового осмислення, стандартизації процедур збирання та обробки даних, а також правового регулювання застосування OSINT у національних та міжнародних правових системах.

Перспективи подальших досліджень у цьому напрямі пов'язані, передусім, із вдосконаленням алгоритмів автоматизованого аналізу інформації, розвитком етичних стандартів OSINT-досліджень, створенням міждисциплінарних навчальних програм для фахівців у сфері права, інформаційної безпеки та журналістики. Також перспективним є вивчення ефективності використання OSINT при співпраці громадянського суспільства з органами слідства, міжнародними місіями й неурядовими організаціями. Особливо актуальним є створення глобального реєстру відкритих доказів із можливістю їх архівації та незалежної верифікації — це стане дієвим інструментом не лише для забезпечення справедливості, але й для історичної пам'яті та недопущення повторення воєнних злочинів у майбутньому.

Таким чином, дослідження OSINT-технологій у документуванні воєнних злочинів відкриває нові горизонти в трансформації системи воєнної юстиції, вимагаючи комплексного підходу до формування законодавчої бази, методологічного забезпечення та технічної підготовки відповідних фахівців. У контексті глобалізованого світу та гібридних конфліктів такі дослідження стають не лише актуальними, а й необхідними для зміцнення міжнародного правопорядку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наместнік В. Соціальні мережі як середовище проведення інформаційно-психологічних операцій противника. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи: IV міжнар. наук.-практ. конф.. 2023. С. 8.
2. Лунгол О.М. Автоматизація виявлення кіберзагроз із застосуванням штучного інтелекту. MS thesis. 2025. С. 96
3. Report on the activities of the CyberPolice Department of the National Police of Ukraine in 2024 (2025). CyberPolice Department of the National Police of Ukraine. <https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-nacziionalnoyi-policziyi-ukrayiny-u--roczni-7074/>

РОЛЬ OSINT У ВИЯВЛЕННІ ДЕЗІНФОРМАЦІЇ ТА ЦИФРОВИХ ЗАГРОЗ: ІНСТРУМЕНТИ Й АНАЛІТИЧНІ ПІДХОДИ

Єфімкіна Ірина Миколаївна

здобувачка першого (бакалаврського) рівня вищої освіти спеціальності 262 «Правоохоронна діяльність»

Одеського державного університету внутрішніх справ

Моргунова Т. .І

к.т.н., доцент, доцент кафедри кримінального аналізу та інформаційних технологій

Одеського державного університету внутрішніх справ

У цифрову епоху інформація стала не лише засобом комунікації, а й інструментом впливу. Розвідка з відкритих джерел (OSINT) відіграє ключову роль у виявленні загроз і прогнозуванні ризиків. Вона передбачає систематичне збирання та аналіз публічної інформації, не порушуючи правових норм.

Отримання інформації у відкритих джерелах в інтересах розкриття і розслідування злочинів – одне з актуальних напрямків вдосконалення діяльності правоохоронних органів [1]. OSINT дозволяє відстежувати події в реальному часі й формувати цілісну картину суспільних процесів. Проте зростання обсягів даних і ускладнення інформаційного середовища поставили під сумнів ефективність традиційної аналітики.

У сферу інтересів OSINT входить добування та аналіз офіційних документів, проєктів статутів, відстеження нових наукових розробок, баз даних, комерційних і державних сайтів, мережеских щоденників і багато іншого [2].

OSINT вирізняється легальністю, швидкістю доступу та фінансовою доступністю, що робить її ефективною навіть для невеликих аналітичних груп.

Особливе значення OSINT має в превентивному виявленні загроз. Аналіз поведінки акаунтів, повторюваних повідомлень чи змін у лексичних патернах дозволяє заздалегідь ідентифікувати деструктивні впливи. У цьому сенсі OSINT стає не лише реактивним, а й проактивним інструментом безпеки.

Попри видиму відкритість цифрового простору, соціальні мережі, месенджери й відеоплатформи перетворилися на поле інформаційних маніпуляцій. Особливу небезпеку становлять бот-мережі, які створюють ілюзію масової підтримки, поширюють однакові меседжі й дискредитують достовірні джерела. Такі кампанії часто супроводжуються психологічним тиском та ретельно спланованими наративами.

Цифрові загрози, як-от фейки, атаки на інституції та кіберпровокації, діють комплексно – через контент і технологічні засоби. Їхня мета – дестабілізувати інформаційне поле. Тому OSINT стає одним із найефективніших інструментів протидії таким впливам, оскільки дозволяє системно ідентифікувати джерела загроз і схеми їх дій.

Для ефективного застосування OSINT важливі не лише джерела, а й

інструменти перевірки даних. Один із ключових – зворотний пошук зображень, що дозволяє виявити фейки, встановити оригінальність фото та відео. Аналіз метаданих надає інформацію про час, місце та пристрій створення матеріалу. Також важливою є візуальна аналітика для розпізнавання об'єктів і встановлення географічних координат.

Серед поширених OSINT-інструментів – InVID (аналіз відео), Maltego (побудова зв'язків між об'єктами), TinEye (зворотний пошук зображень), SpiderFoot (автоматизоване сканування цифрових слідів). Вони допомагають структурувати фрагментовану інформацію в цілісну аналітичну модель.

Автоматизований моніторинг на основі API-підключень до платформ на зразок Twitter або Telegram дозволяє аналізувати інформацію в реальному часі. Скрипти, боти та браузерні розширення сприяють створенню персоналізованих систем реагування: виявлення ключових слів, аномальної активності й повторюваних шаблонів.

Таким чином, OSINT – це не лише набір інструментів, а комплексна аналітична система, яка поєднує технологію, знання й стратегічне мислення. Саме її інтеграція в інформаційну політику дає змогу ефективно реагувати на цифрові виклики сучасності.

Щоб узагальнити ключові практики використання OSINT у виявленні цифрових загроз, нижче наведено систематизовану таблицю інструментів та відповідних аналітичних підходів (табл. 1).

Технічні інструменти OSINT – лише частина процесу. Вирішальне значення має те, як зібрані дані будуть осмислені. В умовах постійного оновлення інформації завдання аналітика – виявити закономірності серед хаосу. Аналітичні підходи дозволяють перетворити розрізнені дані на цілісну, обґрунтовану картину подій.

Таблиця 1

OSINT-інструменти та аналітичні підходи до виявлення цифрових загроз

Категорія	Приклади інструментів / підходів	Призначення / результат використання
Збір даних	API Telegram, Twitter, SpiderFoot	Автоматичний моніторинг цифрової активності в реальному часі
Аналіз зображень	TinEye, InVID, зворотний пошук у Google	Виявлення фейкових або маніпульованих зображень
Побудова зв'язків	Maltego, Graph Commons	Візуалізація структур бот-мереж, інформаційних кампаній
Аналіз тексту	NLP-інструменти, семантичний аналіз	Виявлення патернів, риторичних прийомів,

		тональності
Виявлення аномалій	Логічний аналіз, машинне навчання, кластеризація	Ідентифікація нетипової поведінки або поширення контенту
Класифікація контенту	Мітки ризику, ручна експертиза, автоматичні моделі	Розподіл за тематикою, ступенем загрози, джерелом

Одним із найважливіших методів є виявлення патернів – повторюваних моделей поведінки, схожих повідомлень, однотипних візуальних елементів або часових інтервалів. Такі патерни дозволяють визначити джерело походження дезінформації або виявити штучно скоординовані кампанії. Поруч із цим працює виявлення аномалій – нетипових дій, які вирізняються з-поміж загального потоку й можуть сигналізувати про спробу прихованого впливу чи підготовку цифрової провокації.

Доповнює ці підходи семантичний аналіз – методика, що дозволяє досліджувати зміст текстів не лише з погляду ключових слів, а й через аналіз смислових відтінків, інтонації, емоційного забарвлення. Це особливо важливо в умовах гібридної війни, коли вплив часто реалізується не в прямому заклик, а у завуальованому контексті або через послідовне формування потрібного тла.

Ефективна робота з відкритими даними передбачає не лише їх аналіз, а й грамотну візуалізацію. Побудова графів, часових ліній, мап зв'язків чи маршрутів дає змогу унаочнити поширення наративів та виявити ключових учасників. Паралельно контент класифікується за тематикою, ризиком і джерелами, що дозволяє створити структуровану базу для прийняття рішень. Саме так неперевірені дані перетворюються на аналітичну основу для протидії дезінформації.

Однак існує низка викликів. Один із головних – інформаційний шум: потік суперечливих, повторюваних або навмисно згенерованих повідомлень маскує реальні сигнали. Обмеження доступу до даних через нову політику платформ або технічні бар'єри ускладнює роботу. Окрема загроза – Deepfake-контент, що підриває довіру до фактів.

Застосування технології Deepfake надає безмежні можливості для створення відеоконтенту, в якому можна «примусити» будь-яку особу сказати або зробити будь-що [3].

Особливу увагу слід приділяти етиці: навіть легальне використання публічних даних може порушувати приватність. Автоматизація не замінює аналітика – лише фахівець враховує культурний і психологічний контекст, виявляючи сенси, недоступні алгоритмам.

У добу інформаційної війни OSINT набуває стратегічного значення: загрози виникають не лише на фронті, а й у цифровому просторі. Відкриті джерела допомагають виявляти ризики та захищати інформаційний простір. Це вимагає

платформ, які поєднують AI з гнучкістю OSINT і враховують українські реалії.

Ключове значення має підготовка фахівців із технічними навичками, критичним мисленням та етичною відповідальністю. Водночас важливо створити нормативну базу, яка збалансує відкритість і права людини.

Отже, у майбутньому OSINT може стати опорою державної стабільності – за умови розвитку, інституційної підтримки й поєднання технологій, експертизи та етики. Його аналітичні можливості дозволяють виявляти загрози на ранніх етапах, особливо в умовах гібридної війни. Проте ефективність OSINT залежить від людського чинника – компетентності та здатності працювати в умовах інформаційного шуму. Саме тому розвиток платформ, навчання кадрів і створення етичних стандартів критично важливі для цифрової стійкості держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.
2. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. *Противіа кіберзлочинності та торгівлі людьми* Збірник матеріалів Міжнародної науково-практичної конференції. Харків: ХНУВС, 2020. С. 135-137.
3. Юртаєва К.В. Кримінологічний аналіз використання технології Deepfake: коли фейк стає злочином. *Вісник кримінологічної асоціації України*. 2021. № 1(24). С. 31-42. URL: <https://surl.luh.ua/mrimgs>

OSINT – ТЕХНОЛОГІЇ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Журавель Андрій Владиславович

курсант 2-го курсу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Науковий керівник:

Поляков Є. В.

доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС
к.ю.н., доцент, полковник поліції

У сучасному збройному конфлікті, що триває в Україні, на перший план вийшли нові засоби збору доказової інформації про злочини, скоєні під час бойових дій. Зокрема, широкого застосування набувають технології збору даних із відкритих джерел, які в умовах гібридної війни здобувають не лише

розвідувальне, а й правове значення. Поняття OSINT (англ. Open Source Intelligence) охоплює методи аналізу інформації, яка є публічно доступною, але при цьому може нести в собі критично важливі факти для ідентифікації обставин правопорушення, встановлення осіб, причетних до його вчинення, а також формування повноцінної доказової бази. Саме тому дослідження ролі OSINT у сфері документування воєнних злочинів має особливу актуальність у контексті роботи національної системи правосуддя та міжнародних органів.

У правозастосовчій практиці вже не є рідкістю ситуації, коли матеріали з соціальних мереж, відеозаписи з особистих пристроїв, супутникові зображення, опубліковані в мережі, слугують основою для відкриття кримінальних проваджень. В умовах постійної фіксації подій цивільними громадянами, військовими, журналістами, волонтерами — зростає масив цифрових доказів, які вимагають систематизації та верифікації. Зокрема, з 2022 року в Україні діють платформи, створені спеціально для збору таких матеріалів, серед яких варто згадати урядовий проєкт «Trap Aggressor», ініціативи правозахисної групи «Truth Hounds» та діяльність Центру документування Української Гельсінської спілки з прав людини. Всі ці структури в тій чи іншій мірі базують свою роботу на принципах OSINT, які інтегруються у слідчу й аналітичну роботу [1; 2].

Важливо підкреслити, що продукти OSINT самі по собі не мають абсолютної доказової сили. Однак за належної технічної фіксації, підтвердження джерела походження, а також проведення судової експертизи, така інформація може стати допустимим доказом у кримінальному провадженні. У цьому контексті значення має як дотримання вимог Кримінального процесуального кодексу України, так і орієнтація на міжнародні стандарти, зокрема положення Римського статуту Міжнародного кримінального суду. Саме тому ефективність використання OSINT залежить не лише від технічної оснащеності слідчих та аналітиків, а й від рівня їхньої правової обізнаності та методичної підготовки.

Певну увагу слід звернути на питання цифрової гігієни та етики обробки інформації. Значна частина доказів, зібраних за допомогою OSINT, стосується персональних даних, відео- та фотоматеріалів, що можуть містити жорстокі сцени, постраждалих осіб, зруйновані цивільні об'єкти. Це вимагає відповідального підходу до збору і зберігання такої інформації, дотримання принципів конфіденційності та етичних норм при її використанні. У багатьох випадках аналітики вимушені встановлювати автентичність відео, орієнтуючись на візуальні особливості місцевості, погодні умови, положення сонця на момент зйомки тощо, що свідчить про міждисциплінарний характер такої роботи.

Упродовж останніх років в Україні спостерігається поступова інституціоналізація OSINT як напряму діяльності не лише в журналістиці чи серед активістів, але й у правоохоронній діяльності. Наприклад, згідно з інформацією правозахисних організацій, зокрема Української Гельсінської спілки з прав людини, все більше розслідувачів щодо воєнних злочинів використовують

аналітичні інструменти для ідентифікації осіб за допомогою відкритих профілів у соцмережах, вивчення цифрового сліду підозрюваних, а також відстеження переміщень військової техніки ворога. У цьому контексті тісна співпраця між державними структурами й громадянським суспільством відіграє важливу роль, оскільки саме волонтерські групи часто першими фіксують воєнні злочини, а вже потім передають інформацію в офіційні канали [3].

Однією з проблем залишається відсутність чітко унормованого алгоритму використання OSINT доказів у кримінальному процесі. Попри те, що стаття 84 КПК України дозволяє використовувати електронні докази, на практиці виникають труднощі з доведенням автентичності контенту, зокрема при відсутності метаданих чи первинного джерела. Це породжує потребу у створенні інструкцій, які регламентували б порядок збору, зберігання та оцінки доказів, здобутих із відкритих джерел. Крім того, варто враховувати міжнародний досвід, зокрема практику Міжнародного кримінального трибуналу щодо колишньої Югославії, де певні OSINT докази були використані як допоміжні елементи обвинувачення.

Таким чином, OSINT технології посідають важливе місце в системі фіксації та документування воєнних злочинів, проте потребують подальшого розвитку, зокрема на нормативному рівні. В умовах збройного конфлікту Україна стала прикладом країни, яка активно застосовує аналітику відкритих джерел для правозахисної діяльності, що може стати основою для створення цілісної моделі OSINT розслідування в інших державах. Подальше вдосконалення цієї сфери має включати навчання слідчих, аналітиків, а також налагодження сталого співпраці з неурядовими організаціями, які вже мають успішний досвід OSINT документування фактів агресії проти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Truth Hounds. Методологія документування воєнних злочинів в Україні [Електронний ресурс]. – Режим доступу: <https://truth-hounds.org/wp-content/uploads/2023/08/voyenni-zlochyny-metodologiya-rozsliduvan-dlya-gromadskyh-organizacij.pdf>.
2. Trap Aggressor: офіційна платформа фіксації воєнних злочинів [Електронний ресурс]. – Режим доступу: <https://trap.org.ua>.
3. Українська Гельсінська спілка з прав людини. [Електронний ресурс]. – Режим доступу: <https://helsinki.org.ua>.
4. Кримінальний процесуальний кодекс України. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ.

Калугін Володимир Юрійович

професор кафедри кримінального аналізу
та інформаційних технологій ОДУВС к.ю.н., доцент

Зважаючи на фундаментальні трансформації, зумовлені екстенсивним поширенням і повсюдним застосуванням цифрових технологій, результативна протидія кіберзлочинності імперативно вимагає якісної розробки розширення та суттєвого підвищення дієвості уніфікованої політики з ключових питань та інкорпоруватися в будь-яку комплексну стратегію боротьби з цим видом злочинної діяльності. На сучасному етапі в Україні протидія кіберзлочинності здійснюється на підставі низки нормативно-правових актів, серед яких Конвенція про Кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний Кодекс України та інші профільні законодавчі і підзаконні акти. Однак, слід об'єктивно констатувати наявність певних недоліків та прогалин у національному законодавстві, що регламентує сферу протидії кіберзлочинності.

Підтвердженням стратегічного наміру України інтегруватися в глобальну боротьбу з цим загрозливим явищем стала ратифікація у 2005 році Європейської Конвенції про кіберзлочинність. Ще одним значущим кроком стало інституційне оформлення у 2008 році спеціалізованого відділу боротьби з кіберзлочинністю в структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, МВС України. На цей профільний підрозділ було покладено відповідальні завдання щодо формування та практичної імплементації державної політики у сфері протидії кіберзлочинності, оптимізації чинного законодавства та налагодження ефективної міжнародної співпраці у сфері боротьби зі злочинами, що вчиняються з використанням високих технологій та телекомунікаційних систем.

Аналізуючи нормативно-правову базу, що опосередковано регулює досліджувану проблематику, першочергово слід акцентувати увагу на Законі України «Про основи національної безпеки» від 19.06.2003 року. Зазначений законодавчий акт, зокрема, артикулює розуміння комп'ютерної злочинності та кібертероризму як розголошення інформації, що становить державну та іншу таємницю, охоронювану законом, а також конфіденційних відомостей, що є власністю держави або спрямовані на забезпечення потреб і національних інтересів суспільства й держави.

Конвенція про кіберзлочинність пропонує диференціацію кіберзлочинів залежно від об'єкта посягання. Так, до категорії злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відносяться несанкціонований доступ, незаконне перехоплення, деструктивне втручання в дані, втручання в функціонування системи, а також зловживання пристроями. Окрему групу становлять злочини, пов'язані з використанням

комп'ютерів, такі як підробка та шахрайство. До злочинів, пов'язаних зі змістом інформації, належать виробництво дитячої порнографії, пропонування або надання доступу до неї, її розповсюдження, передача, отримання за допомогою комп'ютерних систем, а також володіння дитячою порнографією в комп'ютерній системі чи на електронних носіях інформації.

Ще одну категорію складають злочини, що посягають на авторські та суміжні права, включаючи правопорушення, за які передбачено кримінальну відповідальність відповідно до Паризького акту від 24.07.1971 року щодо Бернської Конвенції про охорону літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності, Угоди Всесвітньої організації інтелектуальної власності про авторське право, Міжнародної конвенції про охорону інтересів артистів-виконавців, виробників фонограм і організацій мовлення (Римська конвенція) та Угоди Всесвітньої організації інтелектуальної власності про виконання і фонограми, за винятком будь-яких моральних прав, що надаються цими конвенціями, у випадках, коли такі дії вчинені умисно, в комерційних масштабах і з використанням комп'ютерних систем.

У січні 2016 року Радою національної безпеки та оборони України було схвалено Стратегію кібербезпеки України, розроблену з урахуванням актуальних викликів, що постали перед державою, а саме: агресивних дій Російської Федерації, ескалації тенденцій використання кіберпростору розвідувальними та спеціальними військовими структурами, терористичними організаціями та кримінальними угрупованнями.

Зазначена Стратегія артикулює багаторівневу концепцію розвитку національної екосистеми кібербезпеки, що охоплює своєчасну ідентифікацію та ешелоновану нейтралізацію кібернетичних загроз, а також превентивні заходи, інтегровані з передовим досвідом і визнаними практиками держав-членів НАТО та Європейського Союзу. Крім того, у цьому стратегічному документі скрупульозно розглядаються питання міжвідомчої синергії, координації зусиль та чіткого розмежування функціональних обов'язків між ключовими суб'єктами сектору безпеки та оборони України у контексті забезпечення кібербезпеки, кіберзахисту та протидії кіберзлочинності. Фундаментальною метою Стратегії є формування стійкого та безпечного операційного середовища національного кіберпростору, його використання в інтересах особистості, суспільства та держави. У документі акцентується, що поряд із безсумнівними перевагами сучасної цифрової парадигми та експоненційним зростанням інформаційних технологій, останні можуть бути інструменталізовані для здійснення терористичних актів, зокрема через нелегітимне проникнення в штатні режими функціонування автоматизованих систем управління технологічними процесами на об'єктах критичної інфраструктури.

Окрім цього, Стратегія ініціює залучення експертного потенціалу провідних наукових установ, авторитетних професійних та впливових громадських об'єднань до процесу підготовки проєктів концептуальних документів у зазначеній сфері; підвищення рівня цифрової компетентності громадян та формування культури безпечної поведінки в кіберпросторі;

активізацію міжнародного співробітництва та підтримку глобальних ініціатив у галузі кібербезпеки, зокрема через поглиблення стратегічної взаємодії України з Європейським Союзом та НАТО.

У 2017 року прийнято Закон України «Про основні засади забезпечення кібербезпеки України», який визначає ключові цілі, стратегічні напрями та основоположні принципи державної політики у сфері кібербезпеки, окреслює повноваження державних органів, підприємств, установ, організацій, фізичних осіб та громадян у цій критично важливій сфері, а також закладає підґрунтя для ефективної координації їхньої діяльності, спрямованої на забезпечення кібербезпеки. Зокрема, Закон чітко визначає суб'єктів національної системи кібербезпеки, до яких належать Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи України та Національний банк України, на яких покладається відповідальність за протидію кібернетичним загрозам у межах їхньої компетенції, визначеної цим законодавчим актом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р., № 96/2016. URL: <http://zakon1.rada.gov.ua>.

2. Указ Президента України «Про Стратегію національної безпеки України» від 06.05.2015 № 287/2015. URL: <http://zakon.rada.gov.ua>.

3. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально - методичний посібник. Одеса: 2020. 112 с.

5. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору/ Україна: події, факти, коментарі. 2017. № 19. С.42–48.–URL:<http://nbuviap.gov.ua/images/ukraine/2017/ukr19.pdf>.

5. Форос Г.В. Правові основи захисту інформації в кіберпросторі. Правова держава. Одеса. № 30. 2018. С. 181-187.

АЛГОРИТМ ВИКОРИСТАННЯ МЕТОДОЛОГІЇ OSINT

Калугін Володимир Юрійович

професор кафедри кримінального аналізу та інформаційних технологій ОДУВС

Янковий Микола Олександрович

професор кафедри кримінального процесу та криміналістики ОДУВС

Розвідка з відкритих джерел (OSINT) охоплює широкий спектр методів та інструментів для збору, аналізу та обробки інформації. Однак використання окремих інструментів у відриві від загальної аналітичної

стратегії може призвести до обмеженого розуміння ситуації. Комплексний підхід, що поєднує різні OSINT-методи, дозволяє отримати більш точні, достовірні та релевантні дані, які можна використовувати для прийняття обґрунтованих рішень у сферах безпеки, розслідувань, кіберзахисту та інформаційної аналітики.

В епоху інформаційного вибуху, коли щодня створюються терабайти відкритих даних, зростає роль розвідки на основі відкритих джерел — OSINT (Open Source Intelligence). OSINT передбачає збір, обробку та аналіз інформації, доступної з легальних публічних джерел, таких як інтернет, соціальні мережі, ЗМІ, бази даних, урядові ресурси тощо. Використання OSINT є надзвичайно актуальним у сфері національної безпеки, боротьби зі злочинністю, журналістських розслідувань та корпоративної аналітики. Однак ефективне застосування цього інструменту неможливе без чітких алгоритмів збору та аналізу інформації.

Слід зазначити, що процес OSINT-аналітики має чітко визначену послідовність дій. Узагальнений алгоритм можна представити у вигляді шести ключових етапів:

На *першому етапі* відбувається визначення цілей розвідки, формулюється задача аналітичного дослідження: Мета цього етапу – формування замовником завдань OSINT-дослідження (приміром, ідентифікація фізичної чи юридичної особи, встановлення окремих аспектів її діяльності, близького оточення чи пов'язаних контактів, компрометуючих матеріалів, місцезнаходження об'єкта або маршруту його переміщення, верифікація наявних даних тощо), визначення необхідних для його виконання сил та засобів, доведення цієї інформації до безпосереднього виконавця. [1]

Правильно визначена ціль дає змогу: обрати релевантні джерела інформації; підібрати оптимальні методи збору та аналізу; забезпечити об'єктивність і цільову спрямованість дослідження; економити ресурси та уникати дублювання даних.

Узагальнено, етап визначення цілей є фундаментом для подальших розвідувальних дій та визначає якість усього аналітичного процесу.

На *другому етапі* відбувається пошук релевантних джерел, до яких відносяться: офіційні бази даних (державні реєстри, ЄДР, санкційні списки); публікації у ЗМІ та наукових виданнях; соціальні мережі (для OSINT); професійні форуми, блоги експертів; документи, витоки, відкриті судові реєстри; метадані файлів, зображень, відео. що є критично важливим етапом аналітичного дослідження, який безпосередньо впливає на якість, достовірність і повноту отриманих висновків. [2] Основна мета цього етапу — виявлення інформаційних ресурсів, що містять актуальні, перевірені та тематично релевантні дані для досягнення поставленої цілі розвідки. Універсальний набір інструментів і алгоритм пошукових дій визначити складно – ключові слова, джерела потенційної інформації, необхідний

інструментарій, наявність відомостей та їх достовірність залежать від вихідних даних та кінцевої мети пошуку.

Правильно обрані джерела дозволяють уникнути хибних висновків, зменшити обсяг зайвої інформації та підвищити обґрунтованість аналітичного продукту.

Третій етап збір даних в ході якого здійснюється технічний збір даних — вручну або з використанням інструментів автоматизації (парсери, API, web crawlers). Збір даних є одним із ключових етапів аналітичного дослідження, що забезпечує основу для подальшого аналізу, висновків та прийняття рішень. На цьому етапі здійснюється цілеспрямоване отримання інформації з попередньо визначених джерел — як відкритих, так і спеціалізованих.

Збір відомостей може бути *пасивним* (без взаємодії з об'єктом зацікавленості, наприклад, за допомогою пошукових систем, сервісів чи Telegram-ботів) та *активним* (наприклад, застосування елементів соціальної інженерії при роботі з поштою чи акаунтами особи в соцмережах; отримання доступу до відкритих портів його пристроїв; використання вразливостей встановлених ним програм тощо). [3]

Методи збору поділяються на ручні (традиційний пошук, моніторинг) та автоматизовані (використання скриптів, парсерів, API, краулерів).

У розвідці на основі відкритих джерел (OSINT) особливо актуальним є застосування таких інструментів, як Maltego, SpiderFoot, Shodan, Google Dorks, які дозволяють ефективно витягувати структуровані й неструктуровані дані з Інтернету.

На *четвертому етапі* відбувається перевірка інформації на актуальність, достовірність і релевантність. Використовуються крос-перевірка, пошук джерела первинної інформації, перевірка метаданих, верифікація попередньо оброблених відомостей, тобто їх зіставлення з іншими незалежними OSINT-джерелами для підтвердження або спростування достовірності даних. Якщо подібна перевірка неможлива, інформація позначається як «неперевірена». Кінцевий результат роботи формується шляхом поєднання якісного та кількісного опрацювання інформації з урахуванням релевантності запиту

На *п'ятому етапі* аналітик або аналітична система обробляє зібрані дані, виявляє зв'язки, патерни поведінки, часові закономірності. Використовуються методи кластерного аналізу, машинного навчання, графових структур.

І на *шостому етапі* відбувається візуалізація та підготовка аналітичного звіту, який полягає у створенні аналітичного продукту — звіту, візуалізацій у вигляді графіків, діаграм, карт, рекомендацій або попереджень.

Як висновок. Алгоритм використання OSINT базується на чіткій послідовності: від постановки цілей до створення аналітичного продукту.

Застосування автоматизованих інструментів значно підвищує ефективність роботи з великими обсягами відкритих даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зоренко Д. С., Кульчицька Л. О., Лех Р. В., Червяков О. І. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний poradnik. 5-те вид., переробл. та доповн. / Д.С. Зоренко, Л. О. Кульчицька, Р. В. Лех, О. І. Червяков. Харків. Видавець: О. А. Мірошніченко, 2024. 80 с.

2. Калугін В.Ю., Федоров І.В., Джерела інформаційно-аналітичної діяльності Електронне наукове видання «Аналітично-порівняльне правознавство» №1 2023 р. С 168-172

3. Кисельов А.О. Досвід використання підрозділами Національної поліції технологій «OSINT» у протидії кримінальним правопорушенням / А. Кисельов // Міжнародна та національна безпека: теоретичні і прикладні аспекти: матеріали VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 березня 2022 р.). Дніпро, 2022. С. 318-319.

ДЕЯКІ ПИТАННЯ ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ У ДІЯЛЬНОСТІ КРИМІНАЛЬНОГО АНАЛІТИКА

Кіресва Ольга Сергіївна

кандидат психологічних наук, доцент,
доцент кафедри спеціальних дисциплін,

Національна академія Державної прикордонної служби України
імені Б. Хмельницького

У сучасному цифровому середовищі, в умовах гібридної війни та стрімкого розвитку інформаційних технологій, відкриті джерела інформації (Open Source Intelligence, OSINT) перетворилися на один із найпотужніших інструментів кримінального аналізу. Розвідка з відкритих джерел використовується не лише в рамках оперативно-розшукової діяльності, а й для стратегічного аналізу, виявлення загроз, супроводу досудового розслідування, ідентифікації осіб, збору доказової бази. У діяльності аналітичних підрозділів Служби безпеки України, Національної поліції України, Державної прикордонної служби України, а також військової розвідки OSINT посідає центральне місце як частина загальної розвідувальної парадигми. Ключовим орієнтиром OSINT-дослідження є так званий розвідувальний цикл TCPED (Task - Collection - Processing - Exploitation - Dissemination), що рекомендований у стандарті AJP-2.9 НАТО. Його адаптація до національної практики дозволяє створити логічну послідовність роботи аналітика - від постановки завдання до формування звіту для замовника. Зокрема, на етапі Task формується мета дослідження, обирається об'єкт і визначаються часові рамки. Етап Collection передбачає

використання інструментів Google Dorking, соціального пошуку, ботів, пошукових систем та агрегаторів. На етапі Processing проводиться сортування, переклад, систематизація даних. Етап Exploitation включає верифікацію, порівняння, оцінку надійності джерел, а Dissemination - створення фінального звіту для користувача [1].

Кримінальний аналітик, виконуючи завдання підтримки досудового розслідування, оперативно-розшукової діяльності чи превентивного аналізу, дедалі частіше інтегрує у свою роботу OSINT-інструменти. Йдеться не лише про збір інформації з Інтернету, а й про глибокий аналіз поведінкових патернів осіб, ідентифікацію цифрових слідів, перевірку алібі, відстеження контактів та переміщень підозрюваних. Особливо ефективними є такі методи у справах, що пов'язані з кіберзлочинністю, шахрайством, злочинними угрупованнями або терористичною активністю. У контексті воєнного часу OSINT дозволяє аналітикам ідентифікувати окупантів, колаборантів, ворожу техніку, маршрути переміщення, географію влучань, інформаційні операції противника. За допомогою OSINT інструментів збираються докази для майбутніх трибуналів, а також моніториться ефективність санкцій, відстежуються трансакції пов'язаних осіб та організацій [2]. Алгоритм OSINT-аналізу, який використовується у кримінальній сфері, зазвичай складається з п'яти основних етапів: постановка задачі, пошук і збирання даних, їх фільтрація, аналітична обробка та візуалізація результатів. Початковим етапом є чітке формулювання цілі - хто або що є об'єктом дослідження, які питання потребують відповіді, в яких часових і просторових рамках необхідно діяти. Наступним кроком є безпосередній збір інформації з відкритих джерел - сайтів, соціальних мереж, баз даних, публікацій у медіа, фото- і відеоматеріалів, карт тощо. Зібрана інформація проходить етап фільтрації для усунення дублікатів, «шуму», маніпулятивних джерел. Далі відбувається аналітична інтерпретація даних – виявлення закономірностей, контактів, часових послідовностей, зіставлення з уже відомою інформацією. Завершальним етапом є створення аналітичного продукту - у вигляді довідки, графу, часової лінії, інфографіки чи презентації для слідчого, керівництва або оперативних підрозділів [3].

У процесі розслідування кримінальних правопорушень кримінальні аналітики застосовують OSINT як для підтвердження наданих слідству відомостей, так і для спростування хибних алібі. Наприклад, за фото у соцмережах фігурантів із геолокацією або тегами можна встановити, чи дійсно особа перебувала у заявленому місці в конкретний час. За метаданими файлів - виявити справжній час створення, модель пристрою, координати зйомки. За допомогою аналізу цифрового профілю можна виявити зв'язки із злочинними угрупованнями, учасниками спільних Telegram-каналів, або виявити спільне користування IP-адресами. У практичному арсеналі кримінального аналітика присутній цілий набір спеціалізованих інструментів, а саме: Google Dorking - техніка використання розширених операторів

пошукових систем для виявлення інформації, прихованої від звичайного користувача. За допомогою Dorking кримінальний аналітик може знаходити незахищені документи, списки електронних адрес, бази даних, лог-файли, конфіденційні адміністративні панелі. Застосування правильних пошукових запитів дозволяє швидко виявити витоки даних або сліди злочинної діяльності в публічному доступі. Maltego - потужний інструмент для побудови графів взаємозв'язків. Дозволяє візуалізувати складні мережі взаємодій між об'єктами: особами, IP-адресами, доменами, організаціями. Maltego особливо корисний для виявлення прихованих структур організованої злочинності або мереж відмивання коштів. TheHarvester - інструмент збору відкритої інформації про електронні адреси, субдомени, IP-адреси з різноманітних джерел, зокрема пошукових систем, соціальних мереж і баз даних Whois. theHarvester допомагає скласти цифровий профіль організації чи особи. SpiderFoot та Recon-NG - модульні фреймворки для автоматизованого збору даних із понад 100 відкритих джерел. Вони дозволяють виявити зв'язки між IP-адресами, доменами, соціальними профілями, опублікувати зібрані дані у форматі, зручному для подальшого аналізу. ExifTools - програмний інструмент для витягу метаданих із фотографій, документів та інших цифрових файлів. Кримінальні аналітики можуть отримувати інформацію про місце, час, пристрій зйомки, що має вирішальне значення для підтвердження або спростування алібі підозрюваних. Pimeyes, FindClone - сервіси для розпізнавання обличчя за фотографіями. Дозволяють шукати особу в мережі за наданим зображенням, виявляючи інші акаунти або місця появи. SunCalc, Google Earth, MapChecking - інструменти для геолокації зображень на основі аналізу положення сонця, рельєфу місцевості, співставлення місць на картах і супутникових знімках. Wayback Machine, Archive.today - сервіси архівування веб-сторінок, що дозволяють відновити раніше опубліковану інформацію, навіть якщо вона була видалена. Використовується для збору доказів маніпуляцій, приховування слідів злочинної діяльності. NameCheckup, Maigret, Sherlock - інструменти для пошуку наявності акаунтів особи у сотнях соціальних мереж та онлайн-сервісах. Це дозволяє скласти повний цифровий профіль об'єкта дослідження. Ці інструменти можуть бути інтегровані в єдину платформу OSINT-операції або використовуватися окремо залежно від завдання. У діяльності кримінального аналітика також широко застосовується візуалізація результатів - за допомогою Gephi, Graphistry, Kibana чи навіть Excel створюються соціальні графи, схеми грошових потоків, часові послідовності подій. Практичні кейси свідчать про високу ефективність OSINT-методів. Так, у розслідуванні серії крадіжок у прифронтових районах було встановлено причетність певних осіб саме завдяки цифровому сліду в соціальних мережах - фотографіям із геолокацією, які згодом вдалося зв'язати з подіями на місцях злочину. В інших випадках було розкрито шахрайські схеми через виявлення повторюваних патернів поведінки в

оголошеннях, спільних контактів у месенджерах та цифрових гаманців. У випадках планування насильницьких дій або масових заворушень OSINT дозволяє на ранньому етапі виявити загрози через моніторинг Telegram-каналів, Reddit, YouTube та інших [4].

Особливої актуальності OSINT набув після початку повномасштабної агресії РФ проти України. На основі відкритих джерел і публічних цифрових слідів аналітики встановлюють особи окупантів, маршрути ворожої техніки, місця дислокації підрозділів. Волонтерські OSINT-групи (Molfar, InformNapalm, Bellingcat) стали джерелом даних, що використовуються в кримінальних провадженнях, зокрема щодо воєнних злочинів. Значну частину даних вдалося зібрати через соцмережі, акаунти військових РФ, залишені пости та фото, які згодом архівуються та аналізуються. Одним із критичних елементів OSINT є цифрова гігієна та анонімізація аналітика. Використання sockpuppet-профілів, VPN, Tor-браузера, спеціалізованих операційних систем на кшталт Tails або Whonix, емуляторів Android-середовищ, інструментів підміни цифрових відбитків браузера є базовою умовою безпечної роботи. Водночас використання OSINT пов'язане з ризиками - юридичними (межі дозволеного збору персональних даних), інформаційними (фейки, дезінформація, маніпуляції), операційними (можливість викриття аналітика або виявлення sockpuppet-профілю). Тому кожен етап OSINT-практики потребує чіткої внутрішньої регламентації, правової оцінки та етичного контролю.

Підсумовуючи, слід зазначити, що OSINT є потужним інструментом кримінального аналітика, здатним забезпечити як стратегічний, так і оперативний рівень підтримки. Уміння працювати з відкритими джерелами, аналізувати цифрові сліди, верифікувати дані та будувати доказову лінію - це вже не додаткові навички, а базові компетенції фахівця XXI століття. Для повноцінної імплементації OSINT у практику кримінального аналізу необхідне навчання аналітиків, інтеграція інструментів у загальні інформаційні системи та закріплення методик на нормативному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OSINT Інструменти для розслідування [веб-сайт]. URL: <https://hackyourmom.com/kibervijna/osint-akademiya/osint-instrumenty-dlya-rozslid-uvannya/HackYourMom> (дата звернення: 01.05.2024).
2. Кіреєва О. С. Використання кримінальними аналітиками інноваційних технологій для виявлення проявів колабораційної діяльності // *Успіхи і досягнення у науці (Серія «Право»)*. 2024. № 3 (3). С. 46–58.
3. Купрієнко Д. А., Кіреєва О. С. Використання можливостей OSINT і штучного інтелекту для забезпечення стабілізаційних заходів прикордонного загону на деокупованій території прикордонних районів України // *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : матеріали міжсвідом. наук.-практ. конф.* (Київ, 1 листоп. 2024 р.). Київ, 2024. С. 115-117.

4. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний poradnik. 5-те вид., переробл. та доповн. / Д. С. Зоренко, Л. О. Кульчицька, Р. В. Лех, О. І. Червяков. Харків : О. А. Мірошниченко, 2024. 80с.

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Коренчук Артем Віталійович

курсант 2-го курсу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Науковий керівник:

Поляков Є. В.

доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС
к.ю.н., доцент, полковник поліції

Актуальність дослідження зумовлена глибокими трансформаціями, які переживає сучасне суспільство під впливом стрімкого розвитку інформаційних технологій. Цифровізація, проникаючи в усі сфери життя, стала каталізатором не лише соціально-економічного прогресу, але й нових форм злочинності та загроз національній безпеці. Україна, що перебуває на передовій протистояння гібридній агресії, особливо вразлива до кібератак, інформаційних операцій та зростання кіберзлочинності.

Кримінальний аналіз, як інтелектуальна діяльність, спрямована на виявлення, інтерпретацію та прогнозування злочинної діяльності на основі систематизованої інформації, набуває особливого значення в умовах зростання обсягів цифрових даних. Його здатність виявляти приховані зв'язки, патерни та тенденції у злочинній діяльності є незамінною для ефективного розслідування та запобігання злочинам, включаючи кіберзлочини. У свою чергу, кібербезпека, як комплекс заходів, спрямованих на захист кіберпростору, стає критично важливим елементом забезпечення національної стійкості, захисту критичної інфраструктури та прав громадян в умовах зростаючої залежності від цифрових технологій.

Сутність та основні концепції кримінального аналізу в цифрову епоху визначається як систематичний процес збору, обробки, аналізу та інтерпретації кримінально значущої інформації з метою виявлення закономірностей, зв'язків, тенденцій та прогнозування злочинної діяльності. В цифрову епоху сутність кримінального аналізу залишається незмінною, проте значно розширюються його об'єкт та інструментарій. До традиційних видів кримінального аналізу (тактичний, стратегічний, оперативний)

додаються нові, зумовлені специфікою цифрових даних. Принципи кримінального аналізу (системність, об'єктивність, прогностичність) набувають нового змісту при роботі з великими обсягами неструктурованої цифрової інформації. Цифровізація впливає на кримінальний аналіз через:

- **Збільшення обсягів та різноманітності даних:** Аналітики отримують доступ до величезної кількості цифрових слідів, метаданих, комунікацій, активності в соціальних мережах тощо.

- **Появу нових інструментів:** Використання технологій обробки великих даних (Big Data), штучного інтелекту (AI), машинного навчання (ML), мережевого аналізу (SNA), геоінформаційних систем (GIS) стає необхідністю для ефективного аналізу.

- **Зміну характеру злочинності:** Цифрові технології використовуються як інструмент вчинення традиційних злочинів (шахрайство, торгівля людьми, розповсюдження наркотиків) та породжують нові види кіберзлочинів.

Кібербезпека як комплексна система захисту в цифровому просторі визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави в кіберпросторі. Вона є комплексною системою, що охоплює технічні (програмно-апаратні засоби захисту), організаційні (політики, процедури, навчання) та правові (законодавство, нормативні акти) аспекти. Основними цілями кібербезпеки є забезпечення конфіденційності, цілісності та доступності інформації в цифровому просторі. Принципи кібербезпеки включають:

- **Системність:** Забезпечення безпеки на всіх рівнях та етапах життєвого циклу інформаційних систем.

- **Комплексність:** Застосування різноманітних методів та засобів захисту.

- **Безперервність:** Постійний моніторинг, аналіз та вдосконалення системи кібербезпеки.

- **Пропорційність:** Витрати на кібербезпеку повинні відповідати потенційним збиткам.

- **Відповідальність:** Чітке визначення обов'язків та відповідальності суб'єктів кібербезпеки. Еволюція загроз у кіберпросторі призвела до появи складних кібератак, кібершпигунства, кібертероризму та інформаційних операцій, що мають значний вплив на національну безпеку. Кібербезпека тісно пов'язана з інформаційною безпекою, яка є ширшим поняттям та включає захист інформації незалежно від її форми.

У цифрову епоху кримінальний аналіз та кібербезпека стають взаємодоповнюючими сферами. Кримінальний аналіз є ключовим інструментом для виявлення, розслідування та запобігання кіберзлочинам. Аналітики використовують цифрові сліди, дані трафіку, логи подій для встановлення зловмисників, їхніх методів та цілей. З іншого боку, дані, отримані в результаті аналізу кіберінцидентів та кіберзагроз (індикатори

компрометації, тактики, техніки та процедури зловмисників), є цінним джерелом інформації для кримінального аналізу, допомагаючи виявляти закономірності та прогнозувати майбутні кібератаки. Особливо важливим є застосування кримінального аналізу для протидії гібридним загрозам, які поєднують кібератаки на критичну інфраструктуру з інформаційними операціями, спрямованими на дестабілізацію суспільства. Аналіз цифрових слідів та інформаційних потоків дозволяє виявляти скоординовані дії та атрибутувати їхніх організаторів.

В Україні підрозділи кримінального аналізу існують у різних правоохоронних органах, зокрема в Національній поліції України (Департамент кримінального аналізу), Службі безпеки України (відповідні підрозділи контррозвідки та боротьби з кіберзлочинністю), Державному бюро розслідувань (Аналітичне управління) та інших відомствах. Їхня структура, функції та повноваження можуть відрізнятися залежно від специфіки діяльності органу. Аналіз їхньої взаємодії показує наявність як налагоджених каналів комунікації, так і проблем, пов'язаних з обміном інформацією та узгодженням аналітичної діяльності. Недостатня інтеграція інформаційних систем між різними відомствами ускладнює створення цілісної аналітичної картини злочинності.

Технологічне забезпечення кримінального аналізу в Україні. Рівень впровадження сучасних інформаційно-аналітичних систем, баз даних та програмного забезпечення для обробки та аналізу кримінальних даних у правоохоронних органах України є неоднорідним. Хоча спостерігаються позитивні зрушення у впровадженні окремих аналітичних платформ та інструментів, залишаються проблеми, пов'язані з інтеграцією застарілих та нових систем, якістю та повнотою даних, а також недостатнім забезпеченням аналітиків сучасними інструментами для роботи з великими обсягами цифрової інформації. Використання технологій штучного інтелекту та машинного навчання перебуває на початковому етапі впровадження.

Кадрове забезпечення та рівень кваліфікації аналітиків. Підготовка фахівців з кримінального аналізу в Україні здійснюється у профільних навчальних закладах Міністерства внутрішніх справ, Служби безпеки України та інших відомств. Проте, існує проблема недостатньої кількості спеціалізованих навчальних програм, особливо у сфері аналізу цифрових даних та кіберзлочинів. Плинність кадрів та недостатній рівень спеціалізованих знань у практикуючих аналітиків, особливо в галузі інформаційних технологій та аналізу великих даних, є серйозним викликом для ефективного розвитку кримінального аналізу.

Практичне застосування кримінального аналізу у розслідуванні різних видів злочинів. Кримінальний аналіз відіграє важливу роль у розслідуванні різних видів злочинів в Україні, включаючи резонансні вбивства, організовану злочинність, корупцію та економічні злочини. Є приклади успішного використання аналітичних методів для виявлення

злочинних схем, встановлення зв'язків між злочинцями та майном, прогнозування злочинної діяльності. Проте, ефективність застосування кримінального аналізу у розслідуванні кіберзлочинів залишається недостатньою через складність цифрових слідів та брак спеціалізованих знань у аналітиків.

Інституційна система забезпечення кібербезпеки України.

Забезпечення кібербезпеки в Україні є функцією багатьох державних органів, серед яких ключову роль відіграють Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ), Служба безпеки України (СБУ), Національний банк України (НБУ), Національна поліція України (НПУ) та інші відомства. Кожен з цих суб'єктів має свої функції, повноваження та сфери відповідальності у сфері кібербезпеки. Проблема міжвідомчої координації та обміну інформацією залишається актуальною, що ускладнює формування єдиної ефективної системи протидії кіберзагрозам.

Нормативно-правове забезпечення кібербезпеки України.

Нормативно-правова база у сфері кібербезпеки України перебуває на етапі розвитку та потребує подальшого удосконалення у відповідності до сучасних викликів та міжнародних стандартів. Закон України «Про основні засади забезпечення кібербезпеки України» є базовим, але існує потреба у прийнятті нових та оновленні існуючих підзаконних актів, що регулюють різні аспекти кібербезпеки, включаючи захист критичної інфраструктури, протидію кіберзлочинності та захист персональних даних.

Технологічний стан та рівень захищеності критичної інформаційної інфраструктури. Рівень впровадження сучасних технологій захисту інформації, систем виявлення та запобігання вторгненням, аналізу кіберзагроз на об'єктах критичної інформаційної інфраструктури України є недостатнім. Аналіз вразливостей виявляє значні ризики успішних кібератак, що можуть мати серйозні наслідки для національної безпеки та стабільності функціонування держави. Необхідна модернізація технологічної бази та впровадження сучасних стандартів кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
2. Аносов, В. М., & Шепітько, В. Ю. (2018). *Кримінальний аналіз: теоретичні та практичні аспекти*. Харків: Право.
3. Голубєв, В. О. (2019). *Кібербезпека держави: теоретико-правові засади*. Київ: Юрінком Інтер.
4. Доповіді та аналітичні матеріали Служби безпеки України, Національної поліції України, Державної служби спеціального зв'язку та захисту інформації України.
5. Статистичні дані щодо стану злочинності та кіберзлочинності в Україні.
6. Публікації міжнародних організацій (ООН, ОБСЄ, Рада Європи) з

- питань кіберзлочинності та кібербезпеки.
7. Наукові статті та публікації у фахових виданнях з питань кримінального аналізу та кібербезпеки.
 8. Інтернет-ресурси та веб-сайти профільних державних органів та міжнародних організацій.
 9. Матеріали профільних громадських організацій та аналітичних центрів України, що займаються питаннями кримінального аналізу та кібербезпеки.

МЕТОДИ ФІКСАЦІЇ ТА ЗБЕРЕЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Кочин Владислав Дмитрович

курсант Харківського національного
університету внутрішніх справ

Науковий керівник:

Онищенко Ю. М.

доцент кафедри кібербезпеки та DATA-технологій
навчально-наукового інституту № 5

Харківського національного університету внутрішніх справ
кандидат наук з державного управління, доцент

У сучасному цифровому середовищі електронні докази стали важливим елементом кримінальних розслідувань, особливо розслідувань кіберзлочинів. Розвиток інформаційних технологій призвів до значних змін у доказовій базі, де важливу роль відіграють дані, що зберігаються, обробляються та передаються в електронному вигляді. У цьому контексті питання належної фіксації та збереження електронних доказів є надзвичайно важливим, оскільки будь-яка помилка на цьому етапі може зробити докази недійсними або юридично неприйнятними.

Електронні докази – це будь-яка інформація в електронній або цифровій формі, яка може бути використана для доказування обставин кримінального правопорушення. До них належать: документи, повідомлення, електронні листи, дані серверів, файли журналів, метадані, записи дзвінків, GPS-координати, зображення, відео, дані камер спостереження, збережені паролі та цифрові підписи. Електронні докази характеризуються нестабільністю: їх легко підробити, видалити, пошкодити або зробити недоступними через втрату ключів шифрування, поломку пристрою або віддалений доступ третіх осіб. Тому одним із головних завдань слідчих, прокурорів та експертів є забезпечення автентичності, цілісності та надійного зберігання таких даних [1].

Процес фіксації електронних доказів складається з кількох важливих етапів. Першим кроком є визначення потенційних джерел цифрової

інформації. Це не лише комп'ютери, смартфони та планшети, але й хмарні сервіси, роутери, зовнішні накопичувачі, акаунти в соціальних мережах, віртуальні сервери та навіть «розумні» пристрої (Інтернет речей). Після того, як джерело інформації ідентифіковано, дані фіксуються. Це робиться за допомогою спеціальних інструментів для створення точної копії носія інформації. Цей тип копіювання називається криміналістичною візуалізацією і передбачає побітове копіювання всього накопичувача, включно з видаленими або прихованими файлами [2, с. 8]. Найпоширенішими інструментами для цього є FTK Imager, EnCase, X-Ways і dd (для Linux), які можуть копіювати дані з джерела без змін.

Окрім створення копій, важливо також контролювати автентичність отриманого матеріалу. Хеш-функція – це математичний алгоритм, який створює унікальний цифровий відбиток (хеш-суму) для кожного файлу або диска, найпоширенішими алгоритмами є MD5, SHA-1 і SHA-256. Якщо змінюється хоча б один байт файлу, змінюється загальна сума хешу, і можна визначити, чи відбулося втручання. Таким чином, хеш-функція є своєрідною «електронною печаткою», яка гарантує цілісність електронних доказів [3].

Не менш важливою є процедура документування дій, пов'язаних з доказами, тобто забезпечення ланцюга зберігання. Це формальний запис усіх дій, вчинених щодо носія інформації та даних: хто отримав доступ до даних, коли і за яких обставин, які інструменти були використані, коли і як дані були передані. Такі записи мають вирішальне значення для доведення допустимості електронних доказів у суді.

Наступним кроком є збереження цифрових доказів. На практиці доцільно зберігати як оригінальний носій даних (якщо це можливо), так і копію, на якій проводився аналіз. Носії даних повинні бути надійно захищені від несанкціонованого доступу, фізичного пошкодження та впливу електромагнітного випромінювання. Для цього використовують сховища, спеціалізовані лабораторії, ізольовані мережі і навіть зашифровані цифрові контейнери [4].

Останні тенденції показують, що значна частина електронних доказів доступна онлайн. Прикладами є інформація в хмарних сервісах (Google Drive, Dropbox), повідомлення в месенджерах (Telegram, WhatsApp) та активність у соціальних мережах (Facebook, Instagram). Доступ до таких ресурсів можливий лише за рішенням суду або каналами міжнародної правової допомоги, а тому потребує окремого правового регулювання. У зв'язку з цим правоохоронцям необхідно бути обізнаними з цифровими правами та процедурами доступу до чутливих даних, а також знати деталі зберігання метайнформації (час, місце та пристрій).

Програмні інструменти аналізу відіграють важливу роль у відновленні та захисті даних: Autopsy дозволяє відновити видалені файли, EnCase забезпечує комплексний аналіз дисків, а Magnet AXIOM виявляє сліди активності користувачів. Ці інструменти не лише записують, але й аналізують великі обсяги даних, встановлюють зв'язки між файлами, часом, місцезнаходженням і

користувачами, а також автоматично генерують звіти для судів [5, с. 131-132].

Важливими є також міжнародні стандарти у сфері цифрової криміналістики. Зокрема, керівні принципи Інтерполу (Міжнародної організації кримінальної поліції) та ENFSI (Європейської мережі судово-експертних установ) вимагають суворого дотримання процедур для забезпечення допустимості доказів у судах різних юрисдикцій. Слід також враховувати рекомендації стандарту ISO/IEC 27037:2012 щодо ідентифікації, збору, пошуку та збереження цифрових доказів.

Таким чином, методи збору та збереження електронних доказів – це не просто технічні процедури, а складний комплекс правових, організаційних та аналітичних заходів, які потребують висококваліфікованих фахівців, доступу до сучасного обладнання та повного дотримання процесуальних норм. Належне поводження з електронними доказами є запорукою ефективного розслідування кіберзлочинів та справедливого судового розгляду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. WikiLegalAid. Електронні докази в цивільному процесі. URL: <https://surl.lu/vmgbpl>.
2. Використання електронних (цифрових) доказів у кримінальних провадженнях
Гуцалюк М.В URL: <https://elar.navs.edu.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content>.
3. Криптографічні хеш-функції. Математична криптологія. URL: <https://ami.lnu.edu.ua/wp-content/uploads/2022/06/Cryptology9.pdf>.
4. Національна асоціація адвокатів України. Проблеми зберігання речових доказів стороною обвинувачення окреслили в НААУ. URL: <https://surl.li/rkncjh>.
5. Благуга Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання. URL: <https://surl.cc/zbcvrb>.

OSINT ЯК ІНСТРУМЕНТ ПОПЕРЕДЖЕННЯ КІБЕРЗАГРОЗ У ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

Кочман Костянтин Павлович

аспірант денної форми 2 курсу
кафедри кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ

OSINT (Open Source Intelligence) – це процес збору та аналізу інформації з відкритих джерел для оцінки загроз, ухвалення рішень або відповіді на конкретні питання. Такий підхід легітимно використовують як державні структури, так і приватні організації для моніторингу ризиків і виявлення вразливостей у своїх системах. При цьому слід пам'ятати: кіберзлочинці теж застосовують OSINT для соціальної інженерії, фішингу та

підготовки атак.

Джерела інформації для OSINT надзвичайно різноманітні: це і пошукові системи (Google, Bing, Yandex тощо), друковані та онлайн-ЗМІ, соціальні мережі (Facebook, X, LinkedIn, Telegram), форуми, а також спеціалізовані реєстри й бази даних, наприклад електронні державні реєстри, публічні звіти і бюджети, академічні публікації. До числа OSINT-джерел належать також технічні дані: IP-адреси, відкриті порти, API, метадані вебсторінок тощо.

Для збору та обробки відкритої інформації існує низка спеціалізованих інструментів і сервісів. Наприклад, Maltego дозволяє графічно візуалізувати зв'язки між об'єктами інформації, Shodan сканує пристрої Інтернету, theHarvester збирає доменні імена та email-адреси, SpiderFoot автоматизує OSINT-розвідку з понад 100 джерел. Є також веб-платформи (наприклад, OSINT Framework), що класифікують сотні інструментів за категоріями та напрямками. Використання цих засобів значно підвищує ефективність збору великих обсягів публічної інформації [3].

У сфері кібербезпеки OSINT широко застосовується для превентивного виявлення загроз. Зокрема, OSINT-розвідка може здійснювати:

- моніторинг витоків даних – аналіз відкритих джерел (форумів, соціальних мереж, платформ обміну файлами) дозволяє виявити випадки викрадення конфіденційної інформації та своєчасно реагувати на це;

- аналіз соціальної інженерії – вивчення активності зловмисників у соцмережах і на онлайн-форумах дає змогу прогнозувати потенційні фішингові кампанії чи інші атаки соціальної інженерії;

- виявлення фішингових ресурсів – автоматизовані інструменти OSINT дозволяють розпізнавати підроблені сайти до їхнього запуску та блокувати шкідливі домени на ранніх стадіях;

- інцидент-респонс та профілювання кіберзагроз – як зазначає Group-IB, інтеграція OSINT у процес реагування дає можливість проактивно виявляти вразливості систем і швидше локалізувати атаки. Наприклад, регулярне сканування відкритих даних системи дозволяє випереджувати атаки, удосконалювати процедури реагування та складати профілі потенційних загроз;

- аналіз власної інфраструктури – захисники використовують OSINT для збору інформації про власні організації з відкритих джерел (сайтів компаній, соцмереж співробітників, метаданих), щоб виявити потенційні уразливості та запобігти їх експлуатації [4].

Застосування OSINT стає особливо важливим в епоху сучасних гібридних конфліктів. Наприклад, у реальних кейсах війн OSINT дозволяє оперативним відстежувати рухи військ за супутниковими знімками та повідомленнями в мережі, а також розкривати агентів через дані з відкритих реєстрів. Сукупність такої інформації забезпечує органам влади «інформаційну перевагу» і допомагає протидіяти кібератакам противника.

Органи публічної влади постійно працюють в умовах інформаційної невизначеності та кіберзагроз. Використання OSINT тут дозволяє вчасно виявляти загрози, спрямовані на державні інфраструктури. Наприклад, за допомогою відкритих державних реєстрів та картографічних сервісів можна аналізувати фізичні та кібернетичні об'єкти критичної інфраструктури. Ідентифікація таких об'єктів допомагає розробити додаткові заходи безпеки.

Водночас дослідники вказують, що разом із легітимністю OSINT існує загроза зловживань. Івкова та Опірський відзначають, що зловмисники можуть використовувати відкриті дані для збору персональних відомостей про працівників влади чи виявлення уразливостей у системах державних органів. Автори підкреслюють колізію між необхідністю відкритості інформації та завданнями кібербезпеки, а також аналізують чинні норми законодавства України, що регулюють доступ до публічних даних. Згідно із Законом України «Про доступ до публічної інформації» (№2939-VI, 2023), органи влади зобов'язані публікувати визначені законом дані, а громадяни мають право на їх отримання. З іншого боку, діяльність із збору та аналізу відкритих даних має здійснюватися з урахуванням норм щодо захисту персональних даних і запобігання порушенню конфіденційності [1 с. 65].

Нормативно-правове регулювання OSINT в Україні не виділено окремим законом, тому така діяльність підпорядковується загальним правилам інформаційного та кримінального права. Зокрема, у роботі з відкритими джерелами потрібно дотримуватись Закону «Про доступ до публічної інформації», Закону «Про інформацію» та Закону «Про захист персональних даних». Це означає, що чиновники мають обмежувати пошук виключно публічними даними і не допускати збирання закритої чи забороненої інформації. Етичні норми вимагають мінімізувати шкоду для приватних осіб (не проводити незаконного «доксингу», не поширювати конфіденційні дані без підстав) і уникати маніпуляцій (наприклад, спеціально введених у оману даних).

Відповідальність за порушення під час OSINT діяльності може бути передбачена як адміністративним, так і кримінальним законодавством (за розголошення державної таємниці, недотримання захисту персональних даних тощо). Наприклад, при отриманні з відкритих джерел персональної інформації службовець має уникати ситуацій, які можуть трактуватися як порушення статті 32 Конституції України про недоторканність особистого життя чи статті 182 ККУ про порушення недоторканності приватного життя. Таким чином, хоча сам по собі збір публічно доступних даних легальний, на нього поширюються вимоги інформаційної політики держави і міжнародні стандарти права (наприклад, загальні принципи GDPR), які мають враховуватися в практиці державних службовців [2 с. 2].

Використання OSINT у публічному секторі України стикається з низкою викликів. По-перше, існує прогалина в регулюванні – бракує чітких правил та стандартів діяльності з відкритими даними саме для органів влади. Це створює

невизначеність щодо повноважень та меж використання OSINT. По-друге, стрімкий розвиток технологій кібершахрайства ставить нові виклики. Зокрема, Group-IB констатує, що у 2024 році фішинг-атаки зросли на 22% і все більше використовують можливості штучного інтелекту, ускладнюючи їх виявлення. Крім того, застосування OSINT вимагає спеціальної експертизи – держава потребує підготовлених кадрів, здатних працювати з великими обсягами відкритої інформації та аналітичними платформами.

З перспективних можливостей варто відзначити тренди на розвиток освіти й інструментів OSINT. У 2024–2025 рр. з'явилися освітні курси (наприклад, на платформі Prometheus) для підвищення компетентності публічних службовців у роботі з відкритими даними, включаючи правові та етичні аспекти. Технічною перспективою є інтеграція OSINT з інструментами штучного інтелекту для ефективного сортування і аналізу великих масивів даних. У глобальному плані багато країн розглядають OSINT як частину стратегії кібербезпеки, що може стимулювати Україну розробити аналогічні нормативні документи та кооперативні проекти в рамках міжнародної співпраці [5].

Особливе значення для ефективного використання OSINT має створення спеціалізованих аналітичних підрозділів у складі органів виконавчої влади, служб безпеки, кіберполіції та центрів реагування на інциденти. Такі структури повинні не лише технічно працювати з великими масивами даних, а й забезпечувати правову відповідність, оперативну координацію та інформаційний суверенітет. У майбутньому важливо створити систему сертифікації аналітиків з OSINT, аналогічну стандартам кібербезпеки (наприклад, CEH, OSCP), для легалізації їхнього фаху в державному секторі.

Висновок. Отже, OSINT є потужним інструментом кібербезпеки, який забезпечує органи влади додатковою інформацією для виявлення загроз та реагування на них. Головні переваги OSINT – використання легкодоступних даних і прозорість отриманої інформації – супроводжуються необхідністю дотримання законодавства і етики. Важливо, що держава організовано розвиває компетенції у сфері OSINT і розглядає його адміністративно-правові аспекти. Для ефективної протидії сучасним кібератакам необхідне поєднання розвинених технічних засобів OSINT та адекватного нормативного регулювання, яке захищатиме суспільні інтереси й конституційні права громадян.

Таким чином, OSINT доводить свою ефективність не лише як технічний, а й стратегічний інструмент кіберзахисту, що дозволяє виявляти, класифікувати та попереджати потенційні загрози у відкритому інформаційному середовищі. Його використання потребує високого рівня цифрової та правової обізнаності, адже межа між публічною та конфіденційною інформацією часто є тонкою й умовною.

Крім того, впровадження OSINT у практику державного управління

стимулює модернізацію адміністративних процедур та відкриває перспективи для міжвідомчої співпраці на основі обміну аналітичними даними. Це дає змогу формувати нову культуру інформаційної безпеки в органах публічної влади, де відкриті джерела використовуються відповідально, в інтересах суспільства та на основі прозорих і етичних підходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Івкова В. М., Опірський І. В. OSINT-технології як загроза кібербезпеці держави. Кібербезпека: освіта, наука, техніка. 2025. №27. С. 64–83.
2. Лях І. М. Сфери застосування OSINT у сучасних кіберзагрозах: тези доповіді / Житомирська політехніка, 2025. 2 с.
3. Group-IB. OSINT: Open Source Intelligence, Frameworks, and Cybersecurity Applications: веб-сайт. URL : <https://www.group-ib.com/resources/knowledge-hub/osint>.
4. Imperva Inc. Open-Source Intelligence (OSINT) — Meaning, Techniques and Tools : веб-сайт. URL : <https://www.imperva.com/learn/application-security/open-source-intelligence-osint/>.
5. Lindemulder G., Forrest A. What is open-source intelligence (OSINT)? – IBM (Think), 2024 : веб-сайт. URL : <https://www.ibm.com/think/topics/osint>.

РОЛЬ OSINT У РОЗКРИТТІ КІБЕРЗЛОЧИНІВ ТА ІДЕНТИФІКАЦІЇ КІБЕРЗЛОЧИНЦІВ

Кривошея Данило Григорович

курсант 2 курсу факультету
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України
Дніпровського державного університету внутрішніх справ
Науковий керівник:

Рижков Едуард Володимирович

професор кафедри
інформаційних технологій
кандидат юридичних наук, професор
Дніпровського державного університету внутрішніх справ

Розвиток комп'ютерних технологій, мобільного зв'язку, мережі «Інтернет» у всьому світі призвів до того, що сучасна людина вже не уявляє свого життя без використання електронних технічних засобів та тих можливостей, які вони надають. Практично кожна людина, яка живе в розвиненій країні світу, має в особистому користуванні смартфон, ноутбук, планшет з доступом до мережі Інтернет. Більшість таких людей мають особисті сторінки в соціальних мережах, акаунти на різних інтернет-сайтах,

месенджерах тощо.

Цифровізація життєдіяльності людини не могла не вплинути на таке негативне соціальне явище, як злочинність. Ряд злочинних діянь практично повністю перейшов у сегмент інформаційно-телекомунікаційних технологій, наприклад, незаконний збут наркотичних засобів у переважній більшості випадків відбувається безконтактним способом.

У зв'язку з цим зростає потреба в нових підходах до виявлення, моніторингу та аналізу інформаційних потоків, зокрема, які формуються у відкритому доступі. В умовах інформаційного перевантаження особливу цінність набувають інструменти, здатні оперативно та ефективно обробляти великі обсяги даних, доступних у мережі Інтернет.

OSINT – термін, який перекладається як Open-source intelligence, - це методи пошуку, збору, вибору та аналізу інформації, яка являє оперативний інтерес з відкритих джерел. Отримані дані таким чином використовують маркетологи, журналісти, фахівці з комп'ютерної та інтернет-безпеки та ін. [1, с. 138].

Технологія OSINT стрімко набуває популярності та вдосконалюється в органах правопорядку України відповідно до тенденцій розвитку інформаційних технологій. Завдяки здатності витягувати дані з відкритих джерел цей підхід знаходить застосування у широкому спектрі сфер – від військової розвідки до оперативно-розшукової діяльності [2, с. 85].

У правоохоронній сфері технологія OSINT використовується для виявлення, запобігання, розслідування та документування правопорушень, пов'язаних з кіберпростором. Також, вона дедалі відіграє важливу роль у боротьбі з терористичними угрупованнями, відмиванням коштів, здобутих злочинним шляхом, незаконним обігом наркотиків, зброї та інших видів транснаціональної злочинності. Пошук у соціальних мережах потенційно небезпечних груп та індивідуумів є важливою частиною роботи міжнародних правоохоронних організаціях таких як Europol чи Interpol.

Однією із переваг OSINT є можливість її використання за відсутності підстав ведення оперативно-розшукової діяльності, підставою для якої у свою чергу є тяжкість протиправного діяння. Переважна частина кіберзлочинів як раз є нетяжкими. Саме тому доцільно у таких випадках використовувати OSINT, яка демонструє здатність об'єднувати інформацію з різних відкритих джерел для створення цілісного уявлення про об'єкт дослідження або діяльність злочинців. Такий підхід дозволяє зіставляти великі обсяги інформації, виявляти закономірності, аналізувати взаємозв'язки та формувати прогнози. Наприклад, аналіз взаємодії користувачів у соціальних мережах дозволяє ідентифікувати мережі зв'язків, прогнозувати поведінку та оцінювати ризики. У сфері боротьби з кіберзлочинами цей підхід дозволяє виявляти вразливі точки у схемах злочинців і розробляти ефективні стратегії запобігання. OSINT забезпечує не лише оперативність і точність, а й дозволяє стратегічно планувати заходи

безпеки, орієнтуючись на виявлені загрози та можливості [3].

Для ефективної роботи з OSINT існує низка спеціалізованих інструментів. Наприклад, Maltego дозволяє візуалізувати зв'язки між різними об'єктами (люди, компанії, телефони, email-адреси), виявляючи приховані взаємозв'язки. Shodan використовується для пошуку пристроїв, підключених до Інтернету (веб-камери, сервери, промислові системи). Навіть просунуті методи пошуку в Google (Google Dorks) можуть дати неочікувано цінні результати. Існують також платформи, що агрегують дані з різних джерел та надають зручний інтерфейс для їх аналізу.

Особливо актуальним є використання OSINT для деанонізації кіберзлочинців, які використовують псевдоніми, VPN, TOR, криптовалюти та інші засоби приховування особистості. Систематичний збір цифрових слідів, таких як IP-адреси, часові мітки, стилістичні особливості текстів, метадані тощо, дозволяє створювати профілі підозрюваних осіб та формувати доказову базу.

Варто зазначити, що OSINT крім технології виявлення, фіксації та збору інформації є також аналітичним інструментом. У поєднанні з базами даних та внутрішніми ресурсами органів правопорядку його потенціал зростає. Проте, навіть при високому рівні автоматизації фінальні етапи OSINT беззаперечно потребують участі кваліфікованого фахівця [2, с. 88], що свідчить про необхідність якісної підготовки кадрів і збереження людського фактору в аналітичній діяльності.

Доступність інструментів OSINT значно знижує поріг входу для проведення початкових етапів розкриття злочину. Навіть без значних ресурсів чи складних технічних засобів, оперативник, володіючи відповідними навичками, може швидко зібрати первинну інформацію про об'єкт зацікавленості, його зв'язки та діяльність. Це прискорює процес збору інформації та дозволяє ефективніше планувати подальші заходи. Проте, саме ця легкість доступу створює певні ризики. Існує спокуса збору надлишкової інформації, в тому числі про осіб, які не мають прямого відношення до справи. Використання даних із соціальних мереж чи інших неперевіраних джерел без належної верифікації може призвести до помилкових висновків. Тому, навчання фахівців ОВД має включати не лише технічні аспекти роботи з OSINT-інструментами, а й глибоке розуміння правових обмежень, що надзвичайно важливо, навички критичної оцінки достовірності та релевантності інформації, отриманої з відкритих джерел. Відповідальне використання OSINT є ключем до його ефективності та законності.

Слід зазначити, що кримінальне законодавство у сфері кіберзлочинності є динамічним, реагуючи на нові виклики. Зокрема, Закон України № 2113-IX від 03.03.2022 суттєво посилив відповідальність за кіберзлочини, вчинені в умовах воєнного стану, шляхом доповнення ст. 361 новою частиною 5, яка в силу своєї тяжкості дає правові підстави для використання оперативно-розшукової діяльності у повному обсязі. Додамо,

що у необхідних випадках з вдалим поєднанням використання інструментів OSINT.

Таким чином, OSINT стає потужним інструментом у боротьбі з кіберзлочинністю. Його інтеграція в діяльність органів Національної поліції, а також розвиток спеціалізованих освітніх програм, сприяє підвищенню загальної ефективності правоохоронної системи України. У поєднанні зі штучним інтелектом OSINT має потенціал не лише виявляти кіберзлочинців, а й попереджати правопорушення, зміцнюючи інформаційну безпеку держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Михайлов В. О. Питання використання методів OSINT у криміналістиці // DICTUM FACTUM. 2021. №. 2 (10). С. 8.
2. Ryzhkov E.V. Features of utilizing artificial intelligence in OSINT by criminal police officers / E.V. Ryzhkov // Інструменти OSINT для юристів: як підвищити правову компетенцію у цифровому світі : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 20 січня – 2 березня 2025 року. – Львів – Торунь : Liha-Pres, 2025. – 85-89
3. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник / О. О. Торбас. Одеса : Видавництво «Юридика», 2024. 180 с.

ІНТЕГРАЦІЙНИЙ ПОТЕНЦІАЛ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ПРИВАТНОГО СЕКТОРУ У МЕХАНІЗМАХ ПРЕВЕНЦІЇ ТА РОЗКРИТТЯ ПРАВОПОРУШЕНЬ

Лісніченко Дмитро
старший науковий співробітник
науково-дослідної лабораторії
з актуальних питань кримінального аналізу ОДУВС
кандидат юридичних наук, доцент

На тлі перманентного зростання кримінальних проявів в Україні актуалізується потреба в імплементації інноваційних та ефективних інструментів протидії злочинності. У цьому контексті особливого значення набуває потенціал використання наявної інфраструктури приватних систем відеоспостереження. Дана доповідь присвячена поглибленому аналізу можливостей інтеграції та функціонування приватних камер відеоспостереження у спільній системі забезпечення публічної безпеки, враховуючи чинне законодавство, емпіричні дані та релевантний міжнародний досвід.

Регулювання використання приватних систем відеоспостереження в Україні здійснюється в рамках законодавства про захист персональних даних, що встановлює обмеження, зокрема, щодо прихованого візуального спостереження [8]. Легітимність відкритого відеоспостереження зумовлюється виключно за умови належного інформування суб'єктів спостереження. Доступ уповноважених представників правоохоронних органів до архівних відеозаписів регламентується встановленими процесуальними нормами, що у переважній більшості випадків вимагає наявності відповідної ухвали судових інстанцій. Прикладом інституціолізованого підходу до інтеграції різнорідних систем відеоспостереження є реалізація муніципальної програми «Безпечне місто» на території Одеської міської агломерації [6].

Результати наукових досліджень переконливо демонструють кореляцію між функціонуванням систем відеоспостереження замкненого циклу (CCTV) та зниженням рівня злочинності, зокрема стосовно майнових деліктів та неправомірного заволодіння транспортними засобами [1].

Підвищення рівня ефективності досягається шляхом інтенсифікації моніторингової діяльності та синергетичного поєднання відеоспостереження з іншими превентивними та оперативно-розшуковими заходами. Вагома роль у процесах моніторингу та надання доступу до відповідних даних належить приватним охоронним структурам.

Провідні держави світу, такі як Велика Британія, Сполучені Штати Америки, Сінгапур та Австралія, мають значний досвід двосторонньої взаємодії між приватним сектором та правоохоронними відомствами у сфері візуального моніторингу публічного простору [2; 3; 4]. Успішні моделі такої колаборації базуються на чітко артикульованих правових засадах, ефективних механізмах інформаційного обміну та посилених гарантіях захисту персональних даних.

Фундаментом для інтеграції приватних систем відеоспостереження в Одесі слугують муніципальна програма «Безпечне місто» [7] та діяльність комунальної установи «Центр-077» [5]. Технологічна можливість інтеграції IP-камер реалізується через захищені мережеві протоколи або хмарні платформи, що вимагає наявності стандартизованих протоколів передачі даних.

Експлуатація приватних систем відеоспостереження нерозривно пов'язана з комплексом етичних питань, передусім стосовно забезпечення права на приватність, мінімізації ризиків потенційних зловживань та запобігання несанкціонованому доступу до зібраної інформації. Імперативом є забезпечення абсолютної прозорості процесів збору та обробки даних, неухильне дотримання норм чинного законодавства та імплементація дієвих механізмів контролю за використанням відеоматеріалів. Суспільна думка стосовно вказаного питання характеризується вираженою амбівалентністю.

Для досягнення максимальної ефективності використання приватних систем відеоспостереження в Україні необхідна розробка комплексних

нормативно-правових актів, що регламентуватимуть чіткі протоколи взаємодії між суб'єктами права, впровадження технологічно безпечних рішень та забезпечення всебічної прозорості і підзвітності у використанні отриманих даних.

Синергія зусиль публічного та приватного секторів у сфері відеоспостереження має значний, ще не повністю реалізований потенціал для істотного підвищення рівня громадської безпеки в Україні. Успішна імплементація зазначеної можливості критично залежить від скрупульозного врахування правових, етичних та технічних аспектів, а також від імплементації найкращих міжнародних практик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Closed-circuit television (CCTV) - College of Policing, URL <https://www.college.police.uk/research/crime-reduction-toolkit/cctv>
2. EU police data plans pose «substantial security and privacy threats» - Statewatch |, URL <https://www.statewatch.org/news/2024/december/eu-police-data-plans-pose-substantial-security-and-privacy-threats/>;
3. Legal framework of EU data protection - European Commission, URL https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en
4. Privacy and Law Enforcement in the European Union: The Data Retention Directive - Scholarly Commons, URL https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1245&context=faculty_publications
5. КУ «Центр інтегрованої системи відеоспостереження та ...», URL <https://omr.gov.ua/ua/city/foundations/centr-077/>
6. МВС закликає «приватників» підключати відеокамери до системи «Безпечне місто», URL <https://www.ukrinform.ua/rubric-society/3058889-mvs-zaklikae-privatnikiv-pidklucati-videokameri-do-sistemi-bezpechne-misto.html>
7. Одеса Безпечне місто - Інженіринг – Аналітика, URL <http://engineering-a.com.ua/bezpechne-misto/item/odessa-smart-sity>
8. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL : <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ

Лозован Катерина Валеріївна

курсант 212 взводу навчально-наукового інституту
підготовки фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Науковий керівник:

Тригуб С. М.

доктор філософії, викладач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Open Source Intelligence (OSINT), або розвідка на основі відкритих джерел, є важливим інструментом для збору, аналізу та інтерпретації інформації з публічно доступних ресурсів. Її застосовують у сфері національної безпеки, правоохоронної діяльності, журналістики, бізнес-аналітики, кібербезпеки та навіть приватного сектору. OSINT дозволяє отримувати цінну інформацію без застосування засобів негласного спостереження або порушення приватності.

Розвідка на основі відкритих джерел (OSINT) — це процес збору та аналізу інформації, отриманої з відкритих джерел (тобто загальнодоступних та офіційних ресурсів), з метою формування корисної аналітичної інформації. OSINT переважно застосовується у сфері національної безпеки, правоохоронної діяльності та бізнес-аналітики, а також є цінним інструментом для аналітиків, які використовують несекретні дані для задоволення як засекречених, так і відкритих або внутрішніх інформаційних запитів у межах різних напрямів розвідки [1, с. 34].

Ключовими принципами OSINT є легальність джерел, достовірність даних, системність збору та етичність використання. Відбір даних здійснюється з відкритих вебсайтів, форумів, соціальних мереж, державних реєстрів, баз даних WHOIS, супутникових знімків, а також через зворотній пошук зображень і відео. Ефективне застосування OSINT потребує ретельного планування, знання цифрових слідів, навичок критичного мислення та технічної грамотності [2, с. 40]. Серед популярних інструментів OSINT виділяють Google Dorking для поглибленого пошуку, Shodan для виявлення підключених пристроїв, Maltego для побудови графів зв'язків, ExifTool для аналізу метаданих зображень, InVID для перевірки відео та Spiderfoot для автоматизованого збору інформації з понад 100 джерел. Також використовують сервіси для перевірки акаунтів у соцмережах, пошуку особистих даних, моніторингу новин і геолокацій.

Застосування OSINT реалізується через певний алгоритм: визначення

цілі, вибір джерел інформації, збір даних, верифікація та фільтрація отриманого, аналітична обробка, створення висновків або візуалізація результатів. Кожен із цих етапів вимагає чіткого дотримання методології та використання відповідного інструментарію.

У практичній площині OSINT використовується у журналістських розслідуваннях (наприклад, Bellingcat), аналізі репутацій (моніторинг медіа активності осіб та компаній), у криміналістиці (встановлення місцезнаходження підозрюваних), кібербезпеці (виявлення витоків даних, фішингових сайтів) та у військовій сфері (геолокація техніки, аналіз фронтних подій). У багатьох випадках OSINT виступає першим кроком до подальшого розслідування або перевірки [3, с. 91]. Разом із цим, використання OSINT пов'язане з низкою проблем. Серед них – надлишок даних, дезінформація, складність у перевірці достовірності, анонімізація користувачів та правові обмеження. Не менш важливою є проблема кваліфікованої підготовки аналітиків, які повинні не лише збирати інформацію, а й правильно інтерпретувати її контекст. OSINT є не просто технічним інструментом, а складною аналітичною системою, яка потребує глибокого знання джерел, навичок цифрової гігієни та критичного мислення. Подальший розвиток практики OSINT та її інституціоналізація в Україні мають велике значення для інформаційної безпеки, журналістської доброчесності та прозорості влади [4, с. 16].

OSINT є потужним інструментом сучасної цифрової епохи, здатним забезпечити ефективне збирання, перевірку та інтерпретацію інформації з відкритих джерел. Його успішне використання залежить від поєднання технологічних навичок, аналітичного мислення та дотримання етичних стандартів. Подальший розвиток OSINT-інструментарію та алгоритмів має велике значення для національної безпеки, протидії гібридним загрозам, забезпечення інформаційної гігієни та прозорості суспільних процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Билень П. Я. Алгоритми розвідки з відкритих джерел в задачах кібербезпеки. Тернопіль, ЗУНУ, 2024. С. 46.
2. Главацька А. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 2024. С. 19-50.
3. Думчиков М. О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. Академічні візії. 2024. С. 97
4. Пашнєв Д. В., Інструменти та методи AI та OSINT для розшуку дітей, які зникли безвісти, депортовані або примусово переміщені. Використання розвідданих на основі відкритих джерел, їх аналізу та новітніх технологій, включаючи розпізнавання облич: методичні рекомендації. 2024. С. 86

АЛГОРИТМ ОТРИМАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В УМОВАХ ПОТЕНЦІЙНОГО САМОЗНИЩЕННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) СЛІДІВ

Майданевич Леонід Олександрович

канд. філос. наук, старший викладач кафедри захисту інформації
факультету інформаційних технологій та комп'ютерної інженерії

Вінницького національного технічного університету,
адвокат (Рада адвокатів Вінницької області), м. Вінниця

Кирбят'єв Олег Олександрович

доктор юридичних наук, професор,

старший оперуповноважений з оперативного пошуку
та партнерства у сфері інформаційних технологій управління протидії
кіберзлочинам в Запорізькій області Департаменту кіберполіції

Національної поліції України, м. Запоріжжя

Тарасюк Микола Борисович

студент групи ІБС-24М кафедри захисту інформації
факультету інформаційних технологій та комп'ютерної інженерії
Вінницького національного технічного університету, м. Вінниця

Кіберзлочинність в XXI столітті є найнебезпечнішою глобальною загрозою. Це обумовлено стрімким розвитком інформаційних технологій та інформаційної інфраструктури. Власне, «кіберзлочинність ... завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поведженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо» [1].

Задля підвищення ефективності боротьби із кіберзлочинністю, найперше, необхідно дослідити закономірності побудови її як системи. Для цього ми враховуємо, що «на етапі створення в системі кіберзлочинності рівень безпеки забезпечується шляхом: 1) безпечної архітектури; 2) застосування сучасних засобів анонімності; 3) застосування технологій захисту від відстеження; 4) шифрування та безпечне зберігання даних; 5) маскуванню фінансових потоків; 6) розробки алгоритмів соціальної інженерії та тестування лояльності учасників кіберзлочинної групи; 7) впровадження засобів моніторингу та контролю доступу; 8) планування системи резервних копій та відновлення даних; 9) автоматизації процесів для уникнення

помилки через людський фактор; 10) підготовки до адаптації та швидкого реагування на загрози» [2, 11-12].

Враховуючи вказані особливості «безпеки системи кіберзлочинності» та використовуючи стандарти надані в NIST SP 800-101 Rev.1 [3], ДСТУ ISO/IEC 27037:2017 [4] ми вибудовуємо алгоритм вилучення цифрових доказів в умовах потенційного самознищення із 9 етапів: 1) підготовчий етап (попередня оцінка слідчої ситуації); 2) фіксація поточного стану; 3) ізоляція мережевих комунікацій; 4) визначення підходу до збереження стану пам'яті; 5) зняття живлення; 6) захист і вилучення носіїв інформації; 7) первинне клонування (forensic imaging); 8) аналіз копій у контрольованому середовищі; 9) документування та оформлення електронних доказів.

Таблиця 1. Алгоритм отримання електронних доказів в умовах потенційного самознищення електронних (цифрових) слідів

Етап	Зміст	Примітки
1. Підготовчий етап (попередня оцінка слідчої ситуації)	<p>На початковому етапі важливо визначити безпечність роботи на місці проведення розслідування та оцінити ризики, пов'язані з потенційним використанням механізмів самознищення. Слід здійснити ідентифікацію всіх наявних цифрових пристроїв, їхнього поточного стану (увімкнено / вимкнено), а також характеру мережевих підключень і периферійного обладнання.</p> <p>Хоча застосування вибухових пристроїв є надзвичайно радикальним засобом протидії розкриттю інформації, в окремих випадках зловмисники можуть вдаватися до такого методу, якщо втрата даних або їх потрапляння до рук правоохоронних органів може призвести до</p>	<p>Ризики: Існує ймовірність використання спеціалізованих пристроїв або механізмів, що реагують на фізичне втручання середовище (відкриття корпусу зміна температури, переміщення), що може спричинити як знищення даних так і загрозу фізичній безпеці персоналу.</p> <p>До непрямих індикаторів наявності вибухових пристроїв або підозрілих модифікацій корпусу системного блоку належать:</p> <ul style="list-style-type: none"> - сторонні елементи кріплення що не відповідають оригінальній конструкції пристрою (наприклад, додаткові шурупи, герметики, пломби); - підозрілі електронні або механічні компоненти, прикріплені до корпусу або внутрішніх елементів (наприклад, додаткові плати, дроти, які ведуть до жорсткого диска або кнопки живлення); - наявність звукових або візуальних сигналів, що не

	серйозних юридичних або матеріальних наслідків, або розкриття критично важливої інформації (наприклад, компрометація розгалужених кіберзлочинних мереж, державна зрада, промислове шпигунство тощо)	характерні для штатної роботи пристрою (клацання, тікання, миготіння індикаторів тощо); - поява сторонніх запахів (наприклад, запах пластику, що плавиться або хімікатів); - підключення до нетипових джерел живлення або батареї, які можуть свідчити про автономні тригери; - агресивна або підозріла поведінка осіб, пов'язаних із пристроєм, включно з погрозами щодо його відкриття або використання
2. Фіксація поточного стану	Необхідно виконати повну фото- та відеофіксацію усіх пристроїв, стану екранів, індикаторів живлення, підключень кабелів, типу з'єднань та інших деталей. Усі маніпуляції повинні супроводжуватись відповідною документацією з позначенням місця, часу та відповідальної особи	Ризики: Недостатня деталізація фіксації або помилки у маркуванні можуть спричинити відтворення некоректної конфігурації під час лабораторного дослідження, що своєю чергою, може активувати ворожі скрипти. Відсутність належної документації може бути підставою для відхилення доказу у суді
3. Ізоляція мережевих комунікацій	З метою запобігання дистанційному впливу на пристрій або передачі даних слід здійснити негайну ізоляцію від зовнішніх мереж: - фізично вилучити мережеві кабелі; - помістити мобільні пристрої у Faraday-бокси; - деактивувати бездротові модулі (Wi-Fi, Bluetooth) за допомогою апаратних перемикачів	Ризики: Для певного класу анти-форензичного програмного забезпечення втрата мережевого з'єднання може бути тригером для запуску процедур знищення або шифрування даних. Однак огляду на вищий пріоритет запобігання несанкціонованому дистанційному втручанням, ізоляція є необхідною
	Для увімкнених	Ризики: Завантаження

<p>4. Визначення підходу до збереження стану пам'яті</p>	<p>пристроїв: доцільним є виконання процедури live acquisition (тобто, зняття вмісту оперативної пам'яті (RAM), інформації про активні процеси, мережеві сесії, кеш браузерів тощо).</p> <p>Для вимкнених пристроїв:</p> <ul style="list-style-type: none"> - слід уникати вмикання без підготовки; - рекомендується безпосередньо вилучити носії інформації для подальшого аналізу у контрольованому середовищі (дод. див. етап б) 	<p>сторонніх програм на пристрої може активувати шкідливі скрипти. Підключення накопичувача до іншої системи без write-blocker'a може ініціювати автозапуск руйнівних процесів</p>
<p>5. Зняття живлення</p>	<p>Цей крок застосовується лише у випадках, коли live acquisition неможливий або небезпечний.</p> <p>Перевагу слід надавати апаратному відключенню (наприклад, вилучення акумулятора або кабелю живлення), попередньо переконавшись у відсутності джерел резервного живлення</p>	<p>Ризики: Втрата всіх volatile-даних, активація скриптів самознищення, що реагують на завершення роботи системи (stop-задачі, команди на вихід, системні події завершення живлення)</p>
<p>6. Захист і вилучення носіїв інформації</p>	<p>Носії слід вилучати обережно, із дотриманням вимог електростатичної безпеки, та упакувати у спеціальні антистатичні пакети</p>	<p>Ризики: SSD накопичувачі можуть автоматично виконувати команди очищення (TRIM), що унеможливає відновлення частини даних.</p> <p>Деякі USB-носії можуть бути модифіковані апаратно (BadUSB, USB Killer), що створює як інформаційні, так і фізичні загрози</p>

<p>7. Первинне клонування (forensic imaging)</p>	<p>З метою уникнення змін в оригінальному носії створюються побітові копії із застосуванням write-blocker-ів. Клонування виконується у відповідності до методичних стандартів збереження цифрових доказів</p>	<p>Ризики: Відсутність блокування запису може призвести до модифікації вмісту, зміни хеш-сум та втрати достовірності доказів</p>
<p>8. Аналіз копій у контрольованому середовищі</p>	<p>Усі процедури аналізу здійснюються в ізолюваному лабораторному середовищі, з використанням спеціалізованого ПЗ</p>	<p>Слід здійснити пошук: - ознак антифорензичних дій (wipe-utility, rootkits, приховані розділи); - тригерів самознищення (скрипти, cron-задачі, сигнали таймерів, механізми автоформатування); - змін у таблицях розділів, файлових системах або MBR/GPT</p>
<p>9. Документування і оформлення доказів</p>	<p>На всіх етапах необхідно: - фіксувати дії за допомогою відео, аудіо, журналів логів тощо; - здійснювати цифрове підписування створених копій; - використовувати хеш-функції (MD5, SHA-256) для підтвердження цілісності; - забезпечити ланцюг зберігання (chain of custody)</p>	

Запропонований алгоритм дозволяє уніфікувати підхід до обробки інформації в умовах потенційного самознищення електронних (цифрових) слідів. Запропоновані етапи є орієнтирами, та мають бути уточненні слідчим під конкретні обставини слідчої ситуації, слідчої версії. Результати дослідження можуть бути використанні для подальшого теоретичного та

практичного осмислення способів протидії анти-криміналістичним засобам, насамперед, застосовуючи трансдисциплінарний та міждисциплінарний підходи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26.08.2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/go/447/2021> (дата звернення: 11.05.2025)
2. [Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник / Л. Майданевич, О. Войтович, Г. Шелепало. Вінниця : ВНТУ, 2025. 117с.](#)
3. NIST SP 800-101 Rev.1 URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf> (дата звернення: 11.05.2025)
4. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 11.05.2025)

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ МЕРЕЖНИХ СПІВТОВАРИСТВ

Манжай Олександр Володимирович

к.ю.н., професор, завідувач кафедри протидії кіберзлочинності
ННІ № 4 Харківського національного університету внутрішніх справ

На круглому столі «Роль OSINT-досліджень у підвищенні рівня національної безпеки України», який відбувся на базі Львівського державного університету внутрішніх справ 07 травня 2025 року, нами було презентовано спосіб аналізу даних співтовариств в Telegram з використанням зв'язки програм Telegram-Desktop+Excel+Gephi. У результаті аналізу файлу в форматі JSON, який містить інформацію про групу Telegram, зокрема повідомлення та відповіді на них, нам вдалося досить швидко створити схему, на якій відображені найбільш активні учасники групи, однаковим кольором позначені користувачі, які входять до одного співтовариства, розмір вузлів відображає інтенсивність написання повідомлень в групі, товщина стрілок та їх напрями відображають кількість та напрям надсилання повідомлень (рис. 1).

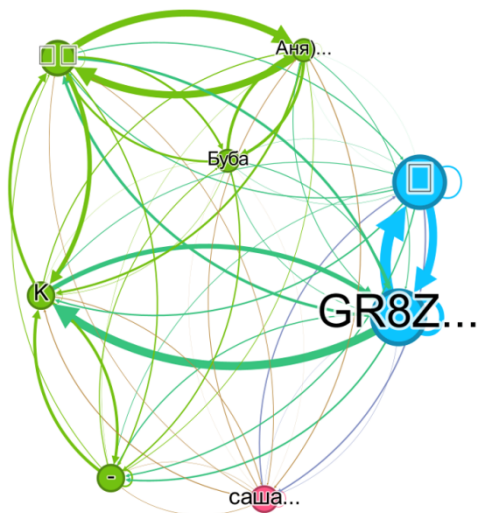


Рис. 1. Схема активності учасників співтовариства

Крім наведеного способу вельми перспективним виглядає застосування інструментів штучного інтелекту для аналізу великих структурованих даних про соціальні зв'язки [1]. Під час такого використання можна сформувавши перелік користувачів, які мали найбільшу активність, та визначати стилістичні співпадіння між акаунтами. Для отриманого переліку користувачів можна створювати часову діаграму розміщення повідомлень з позначенням кількості постів по годинах різними кольорами по аналогії з тепловою мапою. На підставі аналізу часу розміщення постів можна розрахувати, в яких країнах можуть перебувати користувачі. Крім того, з використанням засобів штучного інтелекту можна швидко будувати психологічні профілі користувачів, проводити кластерний аналіз з візуалізацією результатів тощо.

У згаданому контексті можна навести приклад аналізу вже досліджуваних раніше даних співтовариства за допомогою інструменту GPT o3, до якого було завантажено заархівований файл json з даними співтовариства. Після цього системі було поставлено низку запитань:

«У середині архіву файл в форматі json, який містить історію листування в групі Telegram:

1. Визнач перелік користувачів, які мали найбільшу активність та визнач стилістичні співпадіння між акаунтами.
2. Створи для отриманого переліку користувачів часову діаграму розміщення повідомлень. Познач кількість постів по годинах різними кольорами по аналогії з тепловою мапою.

3. На підставі аналізу часу розміщення постів розрахуй, в яких країнах можуть перебувати користувачі з переліку найбільш активних користувачів.

4. Побудуй психологічний профіль для кожного користувача з переліку найбільш активних користувачів.

5. Визнач кластери для користувачів групи та виведи їх у вигляді графу. Залиш у графі найбільш важливі вузли.

6. Виведи окремою діаграмою кожен кластер».

З першої спроби система частково виконала поставлені завдання. В результаті було отримано такі відомості, які наведені в усіченому вигляді, зокрема було видалено користувача з роллю групи, який залишав найбільше повідомлень:

Найактивніші користувачі

(підраховано ≈ 118 тис. повідомлень за всі роки)

<i>№</i>	<i>Користувач</i>	<i>Повідомлень</i>
1	□	7 418
2	GR8Z...	5 121
3	(невидимий символ)	3 183
4	□□ (невидимий символ)	3 128
5	K	2 807
6	саша ...	2 525
7	Аня)...	2 231
9	Буба	1 983
11	\ 2...	1 612
12	.	1 544
13	#Gri...	1 493
14	Таси...	1 288
15	DANT...	1 241

Стилістичні збіги

Для 15 найбільш активних акаунтів було обчислено 7 ризикомірних ознак (середня довжина, кількість токенів, частка великих літер, знаків пунктуації, «!» та «?»), тощо) і підраховано косинусну схожість.

Парами з найбільшим збігом стилю є:

<i>Схожість</i>	<i>Акаунт</i>
0,87	Буба ↔ Таси...
0,86	↔ □□
0,86	K ↔ саша...
0,86	□ ↔
0,86	Буба ↔ \ 2...

Імовірно подвійні акаунти або близькі автори:

Буба ↔ Таси..., (невидимий) ↔ □□ (невидимий).

Часова активність (UTC)

Нижче – години доби, коли кожен із топ-15 залишав найбільше повідомлень.

Користувач	Пік активності (UTC)	Коментар
□	21 :00	Прайм-тайм Європи (+2...+3)
GR8Z...	00 :00	Східна Європа (+2...+3) або Західна РФ (+3)
	00 :00	те саме, що й GR8Z
□□	22 :00	Центральна/Східна Європа
К	00 :00	як GR8Z
саша ...	00 :00	як GR8Z
Аня)...	11 :00	Півд.-Сх. Азія (+7) / Західна Австралія
Буба	19 :00	Західна Європа (+1)
\\2...	00 :00	див. GR8Z
.	23 :00	Європа (+2...+3)
#Gri...	08 :00	Близький Схід (+3...+4)
Таси...	22 :00	Центральна/Східна Європа
DANT...	23 :00	Європа (+2...+3)

Імовірні часові пояси / країни

* UTC +2 – +3 → Україна, Польща, Прибалтика, зах. частина РФ

* UTC +6 → Казахстан / Киргизстан

* UTC +7 → В'єтнам, Таїланд, Індонезія (захід)

* UTC +1 → Німеччина, Франція, Іспанія

(розрахунок: «вечірній прайм» ≈ 19-23 год місцевого часу)

Психологічні профілі (узагальнено)**Користувач Ключові риси**

□ Лаконічні короткі репліки, рідко емоційні → прагматик-модератор; високий темп відповіді.

Довші повідомлення, багато великих літер і

GR8Z... пунктуації → експресивний, домінуючий, схильний до емоційних сплесків.

/ □□ (невидимі) Дуже стислі фрази-відповіді, мінімум символів → «тінюві» боти-підтримка чи технічні акаунти.

К та саша ...	Середній розмір фраз, багато звертань-питань → комунікатори / фасилітатори дискусій.
Аня)...	Помірні тексти з частими емодзі → дружній, підтримуючий тон, високий емоційний інтелект.
Буба, Таси..., \2...	Переважно питання й жарти → «двигуни» розмов, екстраверти.
#Gri...	Ранкові меседжі, небагато емоцій → системний/утилітарний користувач, можливо адміністратор.
DANT...	Середня довжина, підвищена частка знаків оклику → схильність до імпульсивних реакцій.

Кластеризація за стилем

(агломеративний алгоритм Ward, 4 кластери)

Кластер ID	Учасники	Характеристика (спільні ознаки)
0	GR8Z..., Аня)...., Буба, \2..., .., #Gri..., Таси...	Довші репліки, багато пунктуації, емоційні.
2	□, , □□, К, саша ..., DANT...	Стислий стиль, короткі речення, багато питань.

Найважливіші вузли (центральність у графі подібності > 0,75):
, □□, К, саша..., Буба, Таси...

Як видно з наведених результатів, вони в цілому збігаються з результатами аналізу з використанням зв'язки Telegram-Desktop+Excel+Gephi. Таким чином, для аналізу відповідних співтовариств можна використовувати описані способи аналізу як окремо, так і в комплексі, зокрема для перевірки та доповнення висновків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. McGraw J. W. How I turned ChatGPT into an intelligence analyst. URL: <https://cybernews.com/editorial/chatgpt-analysis-hacktivist-pattern-recognition> (дата звернення 28.04.2025).

АНАЛІЗ ЦИФРОВИХ ПЛАТФОРМ У СФЕРІ НЕЗАКОННОГО ОБІГУ НАРКОТИКІВ ДЛЯ УДОСКОНАЛЕННЯ МЕТОДІВ ДОСЛІДЖЕННЯ НАРКОТИЧНИХ ЗАСОБІВ.

Матвєєвський Олег Володимирович

старший викладач кафедри кримінально-правових дисциплін
інституту права та безпеки Одеського
державного університету внутрішніх справ

Науковий керівник:

Афонін Д. С.

завідувач науково-дослідної лабораторії
з актуальних питань кримінального аналізу
ННІПФПКП НПУ, кандидат юридичних наук, доцент

Світовий ринок наркотиків на сьогоднішній день вступив в епоху цифрової економіки з властивою їй цифровою трансформацією: відбуваються революційні зміни традиційної бізнес-моделі вуличної торгівлі на бізнес-модель на основі використання цифрових платформ. Сучасний наркобізнес стійко набуває двох характерних рис: побудований на цифрових платформах та функціонує в мережі DarkNet (від англ. DarkNet - «прихована мережа», «темна мережа», «тіньова мережа», «темний веб»).

Разом з тим, під час воєнного стану боротьба з незаконним обігом наркотичних речовин, до яких відповідно до чинного законодавством належать наркотичні засоби, психотропні речовини та їх аналоги, прекурсори, є однією з основних напрямів діяльності правоохоронної системи України. Крім того, воєнним часом обумовлена тенденція до зміни структури підпільного ринку наркотиків у бік збільшення виробництва, збуту і споживання синтетичних і напівсинтетичних наркотичних засобів і психотропних речовин, тобто більш тих які викликають більш виражене формування наркотичної залежності (це, наприклад, стимулятори амфетамінового ряду, героїн та ін.). [1]

Виробництво експертизи такого роду засобів та речовин вимагає наявності у розпорядженні експертів не тільки сучасного аналітичного обладнання, що дозволяє використовувати різні фізико-хімічні методи дослідження, а в першу чергу розробку нових методик якісного та кількісного визначення подібних речовин у різних об'єктах. Наприклад: у сучасного наркобізнесу з'являються дивні наркотичні засоби, які включають суміші як рослинних компонентів так і синтетичні складові, а експерти не володіють прийомами та засобами їх досліджень.

Методика дослідження цих видів наркотиків об'єктивно відстає від темпів розвитку незаконного обігу наркотиків, що має на сьогоднішній день всі ознаки високотехнологічного цифрового бізнесу. Відповідно до цього ті

експертні напрацювання, які є на сьогодні основною категорією методики дослідження, не відображають об'єктивної картини.

Метою цього дослідження стало вивчення можливості доповнення традиційної емпіричної бази досліджень наркотиків, аналізом інформації з відкритим кодом (OSINT). Центральною вимогою до дослідження було визначено його здатність виявляти достовірні причинно-наслідкові зв'язки, що виводяться із спостережуваних даних.

Шляхом розробки та застосування спеціального інструменту для вилучення веб-даних ринкові дані із заданою періодичністю витягувалися з різних цифрових платформ мережі DarkNet, які пропонують рецепти виготовлення наркотиків. Дані були проаналізовані з використанням програмного забезпечення для хімічних досліджень різних речовин, що дозволяє пов'язувати різні методики досліджень. В результаті одержано якісні дані, що мають практико-орієнтоване значення для побудови нових методик досліджень.

Цифрова платформа – підприємство, що забезпечує взаємовигідні взаємодії між сторонніми виробниками (постачальниками) та споживачами. Вона дає відкриту інфраструктуру для учасників та встановлює нові правила [3]. За ступенем розвитку наданого функціоналу цифрові платформи наркобізнесу відносяться до типу торгових майданчиків (marketplace), надаючи доступ до ринку та забезпечуючи взаємодію сторін [2]. Платформи створюють цифрову інфраструктуру ринків, усуваючи посередників та ієрархічні зв'язки, знижують логістичні витрати, підвищують конкуренцію та поінформованість покупців, підвищують попит та інтенсивність торгівлі.

Шляхом розробки та застосування спеціального інструменту для отримання веб-даних із заданою періодичністю витягувалися з цифрових платформ рецептури наркотичних засобів, які перевірялися з використанням відомих методів досліджень. Дані були проаналізовані за допомогою програмного забезпечення для хімічного аналізу речовин, що дозволяє пов'язувати різні хімічні набори компонентів.

Статистика, отримана в результаті веб-сканування майданчика, дозволила виділити параметри, що дозволяють суттєво доповнити зміст стандартних методик досліджень.

Дані, отримані в результаті веб-сканування та які мають значення для доповнення елементів криміналістичного дослідження, представлені таким чином:

- хімічні інгредієнти (прекурсори), які необхідно використовувати при виготовленні наркотиків і які можуть бути відшукані при обшуку у виготовлювача;
- новітні технології виготовлення невідомих правоохоронній системі наркотичних засобів та психотропних речовин;
- вид наркотиків залежно від географії поширення;
- ймовірність джерела походження наркотика (імпортується,

вироблені на внутрішньому ринку, а також – як імпортовані, так і вироблені на внутрішньому ринку).

Викладене свідчить про допустимість нових технологій збору та аналізу інформації з відкритим вихідним кодом (OSINT) для розвитку криміналістичних досліджень, а також вимальовує перспективи їх розвитку в попередній експертній діяльності. Разом з тим, треба зазначити, що дані дослідження потребують детальної перевірки і удосконалення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Матвєєвський О.В., Афонін Д.С. Особливості організації експертних підрозділів з проведення експертиз наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів у розслідуванні кримінальних правопорушень в період воєнного стану. / Кримінально-правові, кримінологічні та кримінально-виконавчі заходи попередження злочинності в період воєнного стану: матеріали Всеукраїнської науково-практичної конференції 29 листопада 2024 р. — Одеса : ОДУВС, 2024.— стор. 131 – 134

2. Джеффрі Паркер, Маршалл ван Альстін, Санджит Чаударі. Революція платформ: як сітьові ринки змінюють економіку - і як змусити їх працювати на вас: переклад. з англійської Пономарьової Є. Київ: Манн, Іванов та Фербер, 2017.

3. Bancroft A. Research in fractured digital spaces. *International Journal of Drug Policy*. Volume 73, 2019, Pages 288–292. Адреса доступу: <https://www.sciencedirect.com/science/article/pii/S095539591930129X> (дата обращения: 18.12.2019).

OSINT ЯК ДЖЕРЕЛО ДОКАЗІВ У МІЖНАРОДНОМУ КРИМІНАЛЬНОМУ ПРОЦЕСІ

Меликов Руслан

доктор філософії в галузі права,
науковий співробітник науково-дослідної лабораторії з актуальних питань кримінального аналізу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України,
Одеський державний університет внутрішніх справ

Використання Open Source Intelligence — розвідки з відкритих джерел (далі – OSINT) як доказової бази в міжнародному кримінальному правосудді — це інноваційна практика, яка дедалі більше інтегрується в діяльність судових та слідчих органів. У випадках, коли доступ до місць злочинів обмежений (через бойові дії, окупацію або гуманітарні ризики тощо), саме цифрові відкриті джерела стають єдиним способом отримати інформацію про події. У контексті міжнародного кримінального процесу, OSINT набуває

дедалі більшого значення як інструмент збору доказів. У практиці Міжнародного кримінального суду (далі – МКС) використовуються відеозаписи з місць злочинів, геолокаційні дані, а також аналітичні звіти, створені на основі відкритих джерел. Верифікація достовірності цих матеріалів відбувається шляхом порівняння з іншими доказами та застосуванням технологій цифрової криміналістики.

Слід зазначити, що у сучасних умовах збройних конфліктів, зокрема в Україні, зростає значення OSINT у виявленні та документуванні воєнних злочинів. OSINT охоплює публічну інформацію, що доступна у відкритому доступі, включаючи соціальні мережі, фото- та відеоматеріали, супутникові знімки та інші цифрові дані. Зібрані матеріали можуть виступати в якості доказів у міжнародних судових процесах [1, с. 4].

Варто звернути увагу на те, що МКС вже неодноразово звертався до OSINT-матеріалів у справах щодо злочинів проти людяності та воєнних злочинів. Наприклад, у справі «Прокурор проти Домініка Онгвена» (угандійський повстанський командир) були використані відео, які знаходились у відкритому доступі, зокрема записи, зроблені журналістами та правозахисниками. Ці дані підтверджували як обставини конфлікту, так і конкретні дії підсудного [1, с. 23].

Крім того, у розслідуванні катастрофи MH17, яке здійснювалось Об'єднаною слідчою групою (JIT) за підтримки Bellingcat, були використані супутникові знімки, відео з соціальних мереж, геолокаційні дані. МКС визнав такі докази належними у рамках попереднього слідства [2, с. 41].

Також, необхідно звернути увагу на те, що саме Протокол Берклі (Berkeley Protocol on Digital Open Source Investigations), створений Управлінням Верховного комісара ООН з прав людини та Юридичною школою Берклі (США), є першим міжнародним методологічним документом, який надає чіткі правила та стандарти використання OSINT у судовому процесі [3]. Він окреслює принципи верифікації, ланцюга збереження цифрових доказів, захисту особистих даних та етичні обмеження.

Національні суди також поступово визнають допустимість OSINT-доказів. Наприклад, Окружний суд Гааги, розглядаючи справу MH17, детально проаналізував відео- та фотофайли, отримані з відкритих джерел, із залученням цифрових експертів. Суд визнав ці матеріали належними, оскільки вони відповідали вимогам автентичності, неперервного ланцюга зберігання та були підкріплені іншими доказами [4, с. 74].

Таким чином, практика застосування OSINT у міжнародному правосудді поступово формує новий тип доказової культури, де відкриті джерела відіграють ключову роль поряд із традиційними свідченнями, експертизами та документами. Головними умовами визнання OSINT як доказу залишаються: надійність джерела, процедура верифікації, контекст збору даних і забезпечення прав сторін на перевірку автентичності.

Разом з тим, використання OSINT має певні правові, етичні та технічні

обмеження. По-перше, важливим є питання автентичності даних — оскільки фейковий або змонтований контент може бути введений в обіг. По-друге, постає потреба захисту персональних даних свідків та жертв, що можуть бути випадково ідентифіковані [3, с. 102].

Проте, щодо правового аспекту, питання прийнятності доказів OSINT залишається відкритим. Відсутність чітких міжнародних стандартів щодо критеріїв оцінювання відкритих джерел як доказів зумовлює необхідність їх нормативного закріплення. Зокрема, потребує уніфікації порядок збирання, збереження та аналізу таких доказів [4, с. 11].

Все ж, у майбутньому роль OSINT лише зростатиме. Очікується активніше використання штучного інтелекту для автоматизованої обробки даних, розробка етичних кодексів та створення міжнародної платформи обміну OSINT-доказами. Такі кроки сприятимуть підвищенню рівня доказової цінності відкритих джерел та ефективності міжнародного кримінального правосуддя.

Університети, правоохоронні академії та міжнародні навчальні центри вже впроваджують курси з OSINT, цифрової криміналістики та цифрових прав людини. Україна також рухається в цьому напрямі — ініціативи МОН, МВС та громадських організацій спрямовані на підготовку кадрів для цифрового правосуддя [3, с. 52].

Незважаючи на зростаючу популярність OSINT у сфері розслідувань воєнних злочинів та злочинів проти людяності, цей метод має низку правових, етичних, технічних і практичних викликів, які обмежують його ефективне використання у міжнародному кримінальному процесі. Одна з ключових перешкод — це встановлення автентичності матеріалів, зібраних з відкритих джерел. У світі, де фейковий контент, дезінформація та генерація зображень за допомогою ШІ (наприклад, deepfake) стають поширеними, суди та слідчі повинні мати ефективні інструменти для перевірки достовірності цифрових доказів [1, с. 103]. Методи верифікації включають: аналіз метаданих, геолокацію, хронологічну прив'язку, перевірку на монтаж, а також перехресну перевірку з іншими джерелами. OSINT-технології вже сьогодні активно взаємодіють із алгоритмами машинного навчання, що дозволяє автоматично: виявляти збіги в обличчях (face recognition); проводити геолокацію зображень; сортувати великі обсяги відео- та фотофайлів; виявляти дезінформацію або синтетичний контент (deepfake). Це значно прискорює процес аналізу доказової бази [2, с. 87].

Все ж, наразі єдина узгоджена нормативна база, яка б регулювала процедури збору, зберігання та оцінки OSINT-доказів відсутня. Наприклад, МКС не має офіційного регламенту щодо прийнятності OSINT, а суди різних країн оцінюють подібні матеріали з різною суворістю. Хоча, Протокол Берклі [2] встановлює методичні рекомендації, він не має юридично зобов'язуючої сили.

Також, слід звернути увагу на те, що OSINT часто передбачає збір особистої або чутливої інформації без згоди особи, що може порушувати права

людини. Особливо це стосується відеозаписів із жертвами насильства, військовополоненими або цивільними. Важливо уникати повторної віктимізації таких осіб та дотримуватись принципів конфіденційності [3, с. 36].

Аналіз відкритих джерел вимагає високого рівня цифрової грамотності, знання спеціалізованих платформ, інструментів OSINT (наприклад Maltego, Hunchly, Sentinel Hub) та вміння працювати з великими масивами даних. На жаль, у багатьох країнах (в тому числі в Україні) відсутні системні програми підготовки таких фахівців у правоохоронних органах.

Також, часто OSINT-докази збираються журналістами-розслідувачами або волонтерами, а не офіційними структурами. Це створює проблему довіри до походження інформації та викликає питання щодо ланцюга збереження цифрового доказу («chain of custody»), який має бути безперервним для юридичної прийнятності.

Проте, OSINT має потенціал стати одним із найефективніших інструментів у міжнародному кримінальному правосудді, особливо в контексті розслідування воєнних злочинів, злочинів проти людяності та геноциду. Використання OSINT буде ефективнішим за умов налагодженої співпраці між: міжнародними організаціями (МКС, ООН, ЄСПЛ); державними структурами (судові органи, військові прокурори); громадянським суспільством (журналісти-розслідувачі, волонтери, правозахисники). Ця синергія дозволяє створити надійні й багатоаспектні OSINT-докази, які не підлягають спростуванню.

У перспективі можлива поява централізованих реєстрів, куди будуть вноситися верифіковані цифрові докази воєнних злочинів. Наприклад, платформи на кшталт eyewitness to atrocities (Amnesty International), Mnemonic, Bellingcat Archive можуть стати прототипами офіційних міжнародних репозиторіїв для судового використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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 Office of the High Commissioner for Human Rights; Human Rights Center, UC Berkeley School of Law. URL.: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source> (дата звернення 15.05.2025)
2. Пашковський М. Плюралістичність та системність перевірки та оцінки цифрових доказів: аналіз вироку окружного суду Гааги у справі про катастрофу рейсу МН17. Наукові дослідження у сфері протидії злочинності: матеріали наук. конф. (Харків, 6 груд. 2022 р.). URL.: https://www.academia.edu/Documents/in/Open_Source_Intelligence_OSINT (дата звернення 15.05.2025)
3. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у

розвідувальній практиці США. 2013. URL.:
<https://jrn1.nau.edu.ua/index.php/IMV/article/view/3264> (дата звернення
15.05.2025)

4. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку: Протокол Берклі. Науково-практичний poradnik. 2024. URL.:
https://www.researchgate.net/publication/385514719_Vikoristanna_elektronnih_dokaziv_pid_cas_dosudovogo_rozsliduvanna_zlociniv_protiv_miru_bezpeki_ludstva_ta_miznarodnogo_praporadku_Protokol_Berklj_naukovo-practicnij_poradnik?utm_source=chatgpt.com (дата звернення 15.05.2025)

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК СКЛАДОВА ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Михайлішина Анастасія Русланівна

студентка 3 курсу 4 групи
відділення підготовки студентів денної
форми навчання інституту права та безпеки
спеціальності 081 «Право» ОДУВС
Науковий керівник:

Албул С. В.

кандидат юридичних наук ,професор, професор
кафедри оперативно-розшукової діяльності навчально-наукового
інституту підготовки фахівців для підрозділів
кримінальної поліції НПУ ОДУВС

В умовах сьогодення підвищення рівня організованої та транснаціональної злочинності кримінальний аналіз набуває особливого значення як інструмент аналітичної підтримки діяльності правоохоронних органів, зокрема Національної поліції України. Підрозділи кримінального аналізу мають важливе значення у визначенні тенденцій злочинної діяльності, оцінці ризиків та забезпеченні ефективної підтримки оперативно-службової роботи [5, с. 13].

Сьогодні визначення кримінального аналізу є таким – це специфічний вид інформаційно-аналітичної роботи, що спрямований на виявлення та прогнозування взаємозв'язків між даними про злочини та іншими потенційно пов'язаними відомостями [4; 5, с. 14]. Його результативність значною мірою визначається якістю інформаційно-аналітичного забезпечення, яке лежить в основі ухвалення як стратегічних, так і тактичних рішень у сфері боротьби зі злочинністю [1, с. 6]. Ефективність роботи правоохоронних органів суттєво залежить від високої якості, своєчасності та достатності інформаційно-

аналітичного забезпечення.

Термін «інформаційно-аналітичне забезпечення» охоплює процеси збору інформації, її зберігання та обробки з метою подальшого аналізу та практичного використання через формулювання відповідних рішень [3, с. 141]. У діяльності підрозділів кримінального аналізу це сприяє не тільки викриттю злочинних схем, але й прогнозуванню можливих загроз громадській безпеці [2, с. 154].

На сьогодні кримінальний аналіз, як складова інформаційно-аналітичного забезпечення діяльності Національної поліції України, використовує такі ключові джерела інформації, як:

оперативні обліки, до складу яких входять оперативно-розшукові, оперативно-профілактичні та оперативно-довідкові дані;

бази даних із кримінологічною, криміналістичною, адміністративною та статистичною інформацією;

бази даних інших міністерств, відомств, підприємств, установ та організацій;

дані операторів мобільного зв'язку;

звернення громадян, депутатські запити;

інформація з медіа, зокрема з мережі Інтернет;

дані від суб'єктів, які здійснюють заходи протидії злочинності;

інформація від правоохоронних органів іноземних держав і міжнародних правоохоронних організацій;

дані від громадських (неурядових) організацій, включаючи міжнародні [5, с. 147].

Маючи дані інформаційні ресурси у своєму розпорядженні, кримінальні аналітики можуть використовувати їх під час підготовки аналітичних продуктів.

Отже, слід зазначити, що кримінальний аналіз відіграє ключову роль у належній підтримці роботи правоохоронних органів щодо протидії злочинності. Аналізуючи тенденції злочинної активності та оцінюючи потенційні ризики, підрозділи кримінального аналізу сприяють підвищенню ефективності оперативно-службової діяльності. Інформаційно-аналітичне забезпечення слугує основою для розробки дієвих стратегічних і тактичних рішень у сфері протидії злочинності. Висока якість, своєчасність і достатність інформації мають визначальне значення для успішної роботи правоохоронних структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Албул С.В. Аналітична розвідка та оперативно-розшукова діяльність : зарубіжний досвід та вітчизняні перспективи. Правові та організаційно-тактичні засади оперативно-розшукової діяльності Національної поліції України: матеріали IV Всеукраїнської науково-практичної інтернет-конференції (м. Одеса, 13 жовтня 2023 р.). Одеса: ОДУВС, 2023. С. 5–8.
2. Албул С.В. Оперативні обліки як засіб реалізації завдань оперативно-розшукової діяльності Національної поліції України. Multidisciplinary

- academic notes. Theory, methodology and practice. Proceedings of the XXVII International Scientific and Practical Conference. (July 12-15, 2022). Prague, Czech Republic. 2022. Pp. 153–155.
3. Албул С.В. Оперативно-розшукова діяльність: навчальний посібник / С. В. Албул, С. О. Єгоров, Є. В. Поляков, Т. Г. Щурат; за заг. ред. проф. С. В. Албула. Одеса : ОДУВС, 2023. 375 с.
 4. Мовчан А., Крутик Ю., Горбенко Г. Інформаційне забезпечення кримінального аналізу [Електронний ресурс]. URL: https://vaite.kiev.ua/doi/1lp/ILP_Ch_14.pdf (дата звернення 11.05.2025)
 5. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: ЛьвДУВС, 2021. 228 с.

ВИКОРИСТАННЯ OSINT ДЛЯ МОНІТОРИНГУ ДАРКНЕТУ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ

Моргунова Тетяна Іванівна

к.т.н., доцент,

доцент кафедри кримінального аналізу
та інформаційних технологій

Одеського державного університету внутрішніх справ

У цифрову епоху даркнет привертає дедалі більше уваги експертів з кібербезпеки, криміналістики та інформаційної розвідки. Це анонімне середовище, в якому процвітають нелегальні ринки, поширюється викрадена інформація та з'являються нові загрози.

За даними Top Metrics, Україна перебуває на 5 місці (4,9%) у світі за кількістю щоденних користувачів даркнету [1].

Попри ізоляцію та відсутність індексації, даркнет не є повністю прихованим – окремі його частини аналізуються завдяки інструментам відкритої розвідки (OSINT), що стають важливими в боротьбі з кіберзлочинністю.

Зростання значущості OSINT зумовлене потребою оперативного реагування на витоки даних, виявлення фішингових сайтів та діяльність злочинних угруповань. Однак ефективність таких досліджень обмежують як технічні труднощі, так і етичні та правові аспекти. У роботі розглядаються можливості OSINT для спостереження за даркнетом, аналізуються наявні інструменти та їхні обмеження.

Отримання інформації у відкритих джерелах в інтересах розкриття і розслідування злочинів – одне з актуальних напрямків вдосконалення діяльності правоохоронних органів [2].

Даркнет – це сегменти мережі, побудовані на протоколах анонімності Tor чи I2P, де трафік шифрується та маршрутизується через численні вузли.

Такі умови забезпечують високу анонімність і унеможливляють роботу стандартних пошукових систем. Проте даркнет – це не хаотичний простір, а розвинена інфраструктура з власною економікою, соціальними зв'язками й чіткою структурою контенту.

Серед найбільш розповсюджених тем – торгівля зброєю, наркотиками, підробками та краденими даними. Значну частину даркнету становлять форуми й маркетплейси, пов'язані з фішингом, зламами та продажем облікових даних. При цьому контент структурований: повторювані псевдоніми, технічні мітки й ключові слова дозволяють встановлювати зв'язки між об'єктами.

OSINT дає змогу досліджувати окремі доступні фрагменти даркнету через спеціалізовані пошукові системи, бази витоків, або канали типу Telegram. Сайти в onion-мережах часто частково індексуються (наприклад, Ahmia), що дає аналітикам змогу будувати початкові картини подій, оцінювати активність, тематику, час і структуру комунікацій.

У сферу інтересів OSINT входить добування та аналіз офіційних документів, проектів статутів, відстеження нових наукових розробок, баз даних, комерційних і державних сайтів, мережових щоденників і багато іншого [3].

Таким чином, даркнет не є повністю замкненим. Комплексне застосування OSINT-інструментів дозволяє частково зрозуміти його логіку. Водночас моніторинг даркнету – це лише один із напрямів у системі кіберзахисту, де кожен цифровий слід може стати ключем до глибшого аналізу.

Оскільки даркнет позбавлений централізованої структури, традиційні засоби пошуку тут неефективні. Замість них використовуються спеціалізовані інструменти: Ahmia – для пошуку Tor-сайтів; DarkSearch.io – для розширеного аналізу; OnionScan – для виявлення вразливостей. Інструменти як Recon-ng чи TorBot автоматизують пошук цифрових слідів – IP-адрес, хешів, ключових слів із витоків або форумів.

Щоб узагальнити основні характеристики згаданих інструментів, доцільно представити їх порівняння у табл. 1.

Особливу цінність у роботі з даркнетом становить пошук хешів, логінів, електронних адрес, цифрових підписів та ключових слів, які часто залишаються незахищеними у злитих базах даних або опублікованих dump-файлах.

Таблиця 1

Порівняльна характеристика популярних OSINT-інструментів для аналізу

Назва інструмента	Основне призначення	Тип даних / функції	Особливості використання
Ahmia	Пошукова система для Tor-	Onion-адреси, метадані	Інтуїтивний інтерфейс,

	сайтів		обмежена глибина
DarkSearch.io	Пошук по індексованим ресурсам Tor	Ключові слова, URL	Часткова індексація, API-доступ
OnionScan	Аналіз конфігурації onion-сайтів	SSL, порти, серверні помилки	Виявлення технічних вразливостей
Recon-ng	Розширена аналітика цифрових слідів	Хеші, email, логіни, домени	Автоматизовані модулі
TorBot	Моніторинг в реальному часі	Зміни на форумах, нові згадки	Може інтегруватися з Telegram-ботами

OSINT-фахівець може зіставляти ці фрагменти інформації з публічними витоками, виявляючи відповідності, які вказують на можливі компрометації акаунтів, клонування сторінок чи підготовку фішингових кампаній. Саме завдяки таким механізмам з'являється можливість виявляти структуровані схеми кіберзлочинної активності, навіть якщо первинні ресурси були приховані або знищені.

Проте справжній аналітичний ефект досягається не за рахунок одного інструмента, а шляхом інтеграції OSINT із іншими розвідувальними підходами. Зокрема, SOCMINT (Social Media Intelligence) дозволяє відстежувати обговорення даркнет-контенту в соціальних мережах, форумах чи месенджерах – наприклад, згадки про нові торговельні майданчики або інструкції з використання шкідливого ПЗ. Водночас TECHINT дає змогу оцінити технічну інфраструктуру, наприклад, сервіси доставки, криптовалютні гаманці, схеми маскуванія IP-адрес. Поєднання цих підходів дає аналітику повнішу картину – від джерела витоку до каналів поширення інформації або інструментів реалізації шахрайства.

Конкретні приклади успішного використання таких інструментів свідчать про їхню дієвість. Наприклад, через Ahmia вдалося ідентифікувати оновлений домен великого форуму з торгівлі вкраденими обліковими даними, який раніше був переміщений після блокування. За допомогою аналізу ключових слів і хешів через Recon-ng дослідники ідентифікували понад тисячу записів, які вказували на наявність повторного використання паролів у зламаних облікових записах. Подібні дані дозволяють не лише формувати карти ризиків, а й оперативно повідомляти постраждалих користувачів, банки чи компанії про потенційну загрозу.

Таким чином, інструменти OSINT, якщо вони використовуються системно та із застосуванням міждисциплінарного підходу, здатні перетворити даркнет із «чорної скриньки» на середовище, яке піддається хоча б частковому спостереженню. Це відкриває нові горизонти для

аналітики в сфері кібербезпеки, боротьби з організованою злочинністю та захисту цифрових прав.

Хоча OSINT відкриває нові шляхи дослідження даркнету, ця діяльність має чимало обмежень, що ускладнюють аналіз і ставлять під сумнів достовірність отриманої інформації. Даркнет характеризується високою анонімністю – завдяки шифруванню, маршрутизації через вузли Tor або I2P та відсутності реєстрації навіть під псевдонімами, встановити особу майже неможливо. Анонімність тут – не просто захист, а основа його привабливості.

Ще одна складність – нестабільність ресурсів. Даркнет-сайти змінюють адреси, структуру або зникають за лічені години, що унеможливує повернення до джерел для повторного аналізу. Спостереження в даркнеті – це завжди робота «в моменті», без надійної індексації чи довгострокового доступу, що ускладнює системний моніторинг.

До технічних бар'єрів додаються юридичні та етичні ризики. Навіть академічний аналіз даркнету може порушити закон – у багатьох країнах перегляд або завантаження забороненого контенту криміналізується, незалежно від намірів дослідника. Пасивне спостереження теж може мати наслідки: аналітика можуть контролювати правоохоронці, а технічні засоби стати мішенню.

Тому обережність і перевірка джерел – не порада, а обов'язкова умова. У даркнеті фейки, пастки та провокації трапляються частіше, ніж достовірна інформація. Будь-яка згадка чи файл потребують критичної верифікації з кількох джерел. Це зменшує ризик помилок і підвищує достовірність результатів.

Отже, успішне використання OSINT у даркнеті залежить не стільки від інструментів, скільки від обачності, правової обізнаності й етичної відповідальності аналітика. Це складна робота на межі технологій, права та моралі, яка потребує не лише навичок, а й внутрішньої дисципліни.

Узагальнюючи результати дослідження, слід зазначити, що даркнет, попри свою складність і високу ступінь анонімності, не є повністю недоступною зоною для OSINT-аналітики. Грамотне застосування відкритих джерел, інструментів технічного моніторингу та міждисциплінарного підходу дозволяє проливати світло на приховані аспекти діяльності в даркнеті, ідентифікувати загрози та локалізувати потенційні ризики. Водночас ефективність такої роботи потребує чіткої етичної позиції, глибокого розуміння правових меж і особливої професійної обережності. Лише поєднання технічних знань, аналітичного мислення та відповідальності дає змогу перетворити OSINT на дієвий інструмент цифрової безпеки у найменш контрольованих сегментах Інтернету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке даркнет і чи справді він такий небезпечний. *Суспільне*: офіційний вебсайт Національної суспільної телерадіокомпанії України

(НСТУ). URL: <https://suspilne.media/170190-so-take-darknet-i-ci-spravdi-vin-takij-nebezpecnij/>

2. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.

3. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. *Протидія кіберзлочинності та торгівлі людьми* Збірник матеріалів Міжнародної науково-практичної конференції. Харків: ХНУВС, 2020. С. 135-137.

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT У ВИЯВЛЕННІ, ДОКУМЕНТУВАННІ ТА РОЗСЛІДУВАННІ НЕЗАКОННОГО ЗБУТУ ПСИХОАКТИВНИХ РЕЧОВИН

Морозов Д.А.

кандидат юридичних наук, доцент,
доцент кафедри кримінального аналізу
та інформаційних технологій

ОДУВС

Бондар В.С.

кандидат юридичних наук, професор,
Національна академія Служби безпеки України

Використання аналітичних інструментів, екосистем аналітичних продуктів, банків даних різного відомчого призначення в процесі виявлення, документування та розслідування злочинів – не данина моді, а сучасна закономірність пізнавальної діяльності, здійснюваної різними суб'єктами у визначених Законами України «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про розвідку», Кримінальним процесуальним кодексом України (далі – КПК України) та іншими нормативно-правовими актами правових процедурах, орієнтованої на розв'язання наступних загальних завдань:

- встановлення осіб, причетних до вчинення злочинів, ідентифікація їх родинних, кримінальних, ділових та інших зв'язків;

- збирання, систематизацію, аналіз та узагальнення інформації, яка має значення для прийняття тактичних й процесуальних рішень у кримінальному провадженні;

- встановлення наявності та місцезнаходження носіїв та джерел потенціальної доказової інформації;

- підготовчі заходи для проведення негласних слідчих (розшукових) дій;

- підготовчі заходи для використання слідчими отриманих матеріалів у рамках кримінальних проваджень;

- формулювання висновків рекомендаційного характеру для

планування подальших слідчих (розшукових) дій, а також інших процесуальних дій.

У боротьбі держави за безпечне середовище, верховенства права, здорове суспільство, недопущення розповсюдженню наркотичних засобів та психотропних речовин - переоцінити значимість OSINT дуже важко.

Розвинені країни постійно оновлюють сучасні способи отримання оперативної та кримінально значимої інформації, у тому числі тієї інформації, яка розташована у відкритих джерелах стосовно груп та окремих осіб що причетні до незаконного виробництва, виготовлення, придбання, зберігання, перевезення чи пересилання, у тому числі через державний кордон наркотичних засобів та психотропних речовин, а також осіб причетних до «відмивання» коштів, здобутих від незаконного обігу наркотичних засобів та психотропних речовин.

Використання OSINT (Open Source Intelligence) в протидії незаконному обігу наркотичних засобів та психотропних речовин зберігає високу актуальність у сучасному світі з кількох ключових причин:

1. Інформаційна епоха та доступність даних:

Обсяг публічно доступної інформації зростає експоненціально. Інтернет, соціальні мережі, відкриті бази даних, урядові портали та інші джерела містять величезний контент, який може становити значущість для аналізу та прогнозування розвитку криміногенної ситуації в сфері незаконного обігу наркотичних засобів та психотропних речовин.

Розвиток цифрових технологій значно полегшує збирання, обробку та аналіз цих даних.

2. Широкий спектр застосування оптимізує протидію наркозлочинності у всіх сферах його проявлення (дрібний наркозбут, оптовий наркозбут, збут медичних препаратів що містять психоактивні речовини, «вуличний» наркозбут, наркозбут з використанням мережі Інтернет, незаконний обіг наркотичних засобів серед економічних, політичних та культурних еліт, а також залучення корупційних зав'язків для безпечного продовження наркообігу):

OSINT використовується в багатьох сферах які можуть перетинатися з незаконним обігом наркотичних засобів та психотропних речовин, включаючи:

Безпека: кібербезпека, виявлення загроз, розслідування наркозлочинів, боротьба з розповсюдженням наркоманії серед різних слоїв суспільства.

Бізнес: конкурентна розвідка в сфері законного та незаконного обігу психоактивних речовин, аналіз наркоринку, пошук нових можливостей для законного та незаконного наркообігу.

Журналістика: розслідування та перевірка фактів незаконного наркообігу та корупційної складової, виявлення дезінформації.

Державний сектор: Аналіз політики держав стосовно законного та незаконного наркообігу та моніторинг суспільних настроїв як реакції на цю

політику.

Наукові дослідження: перейняття позитивного досвіду боротьби з наркозалежністю, використання інструментів політології для аналізу та прогнозуванню тенденцій у сфері наркообігу, міжнародні взаємодії що до виявлення та ліквідації лабораторій що спеціалізуються на «маскуванні» старих видів психоактивних речовин засобом часткової зміни хімічної формули та створенні нових видів психоактивних речовин.

Правозахисна діяльність: документування груп та окремих осіб що причетних до незаконного виробництва, виготовлення, придбання, зберігання, перевезення чи пересилання, у тому числі через державний кордон наркотичних засобів та психотропних речовин, а також осіб причетних до «відмивання» коштів, здобутих від незаконного обігу наркотичних засобів та психотропних речовин.

3. Економічна ефективність використання OSINT протидії наркозлочинності:

OSINT використовує переважно безкоштовні або недорогі публічні джерела інформації, що робить його більш економічно вигідним порівняно з традиційними (гласними та негласними) методами збирання інформації.

4. Оперативність (одна з найважливіших рис розшукової діяльності та кримінального провадження):

Інформація з відкритих джерел часто є актуальною та оновлюється в режимі реального часу, що дозволяє швидко отримувати необхідні дані стосовно наркоспоживачів, наркозбувачів та їх корупційних зав'язків.

5. Допомога в аналізі складної інформації:

Інструменти та методи OSINT допомагають структурувати великі обсяги даних, виявляти закономірності, зв'язки та отримувати оперативно та процесуально значущі висновки (у тому числі аналізу соціальних мереж осіб, причетних до незаконного обігу наркотичних засобів та психотропних речовин разом з інформацією отриманою в інший спосіб, як гласним так і негласним).

Сучасні тенденції використання OSINT в протидії незаконному обігу психоактивних речовин та поширенню наркоманії:

Автоматизація та штучний інтелект (ШІ): Активне використання ШІ для автоматизації процесів збирання, аналізу та обробки великих даних що стосуються криміногенної ситуації в сфері обігу наркотичних засобів.

Аналіз соціальних мереж: Поглиблений аналіз соціальних мереж для отримання інформації про окремих осіб та групи, тенденції та настрої сфері обігу психоактивних речовин.

Геолокація та візуалізація даних: Використання геолокаційних даних та інструментів візуалізації для найшвидшого реагування правоохоронців що здійснюють протидію наркообігу на дії осіб які мають оперативний інтерес або є фігурантами кримінального провадження.

Розпізнавання образів та відеоаналітика: Застосування технологій

розпізнавання образів та аналізу відео для виявлення та ідентифікації об'єктів та подій що мають відношення до незаконного обігу наркотичних речовин та пошуку осіб яких викрили в незаконному обігу психоактивних речовин та які намагаються сховатися від правосуддя.

Крос-платформний аналіз: Об'єднання даних з різних відкритих джерел для отримання більш цілісної картини.

Етичні та юридичні аспекти: Інформація, яка була отримана стосовно осіб, причетних до незаконного обігу наркотичних засобів не повинна порушувати таємниці особистого життя та персональних даних фігурантів та осіб які його оточують, повинна торкатися тільки його кримінально-протиправної діяльності.

Існує багато способів застосування OSINT для отримання оперативно та криміналістично значущої інформації, але всі їх можливо умовно поділити на активні та пасивні, де розмежування між пасивним і активним дослідженням є важливим аспектом для тих, хто використовує OSINT, оскільки кожен з цих способів може мати різні результати та наслідки.

Звісно, пасивний OSINT (Open-Source Intelligence) може бути корисним для отримання інформації про осіб, причетних до незаконного збуту наркотичних засобів, шляхом аналізу їхніх соціальних мереж. Однак важливо пам'ятати про етичні та юридичні аспекти такого аналізу, а також про те, що інформація в соціальних мережах може бути неповною або неправдивою, що може суттєво вплинути на планування оперативно-розшукових заходів, слідчих (розшукових) та негласних слідчих (розшукових) дій.

Ось деякі аспекти, на які рекомендується звернути увагу в процесі аналізу соціальних мереж у контексті пасивного OSINT для виявлення осіб, ймовірно причетних до незаконного обігу наркотиків:

1. Аналіз профілю та публічної інформації:

Ім'я користувача та біографія: Чи містять вони натяки або кодові (умовності) слова, пов'язані з наркотиками?

Фотографії та відео контент: Чи є зображення, що демонструють наркотичні речовини, приладдя для їх виготовлення, вживання, відкритого чи таємного пакування? Чи є фотографії з великими сумами грошей або дорогими речами, походження яких може бути сумнівним?

Місцезнаходження: Чи часто користувач відвідує певні місця, які можуть бути пов'язані з вживанням або розповсюдженням?

Список друзів та підписок: Коло активного спілкування користувача? Чи є серед його контактів особи, які вже були помічені у наркообігу або мають підозрілу активність? На які групи та сторінки підписаний користувач? Чи є серед них спільноти, присвячені наркотикам або нелегальній діяльності?

2. Аналіз публікативної активності:

Текстові повідомлення та коментарі: Чи використовує користувач сленг, кодові слова (умовності) або емодзі, які можуть мати відношення до

наркотиків? Чи обговорює він теми, пов'язані з незаконним обігом речовин?

Репости та лайки: Який контент користувач поширює або вподобує? Чи є серед цього контенту матеріали, пов'язані з наркотиками?

Час та частота публікацій: Чи є закономірності в часі публікацій, які можуть свідчити про певний спосіб життя або діяльність?

Геолокація публікацій: Чи публікує користувач повідомлення з певних місць, які можуть бути пов'язані з вирощуванням, виготовленням, вживанням або розповсюдженням?

3. Аналіз зв'язків та мережі:

Виявлення спільних друзів та контактів: Результати Аналізу кола активного спілкування можуть допомогти виявити потенційні групи осіб, причетних до незаконного обігу психоактивних речовин.

Аналіз взаємодії між користувачами: Хто найчастіше коментує та лайкає публікації фігуранта? Який характер цієї взаємодії?

Використання інструментів для аналізу соціальних мереж: Існують спеціалізовані інструменти, які можуть допомогти візуалізувати зв'язки між користувачами та виявити закономірності в їхній активності.

Важливо пам'ятати:

Не потрібно робити необґрунтованих висновків: Інформація, отримана з соціальних мереж, потребує ретельної перевірки та підтвердження з інших джерел.

Обов'язково дотримання законодавства: Збирання та використання інформації повинні здійснюватися в рамках належної правової процедури та з повагою до персональних даних та приватного життя осіб.

Звичайно, що кримінальне процесуальне законодавство, не може швидко адаптуватися до позначених закономірностей відображення інформації у віртуальному просторі та наявних програмних засобів її збирання, в тому числі і щодо використання відомостей, отриманих за допомогою OSINT, у доказуванні (доведенні). З точки зору нормативного регулювання, всі відомості, отримані з електронних відкритих джерел, в кримінальному процесі розглядаються як документи, отже на них поширюються вимоги, які передбачені ст. 99 КПК України.

Необхідність обережного поводження з власними діями: В жодному разі не провокувати підозрюваних осіб та не розкривати методи збирання інформації.

Етичні міркування: Завжди зважувати етичні наслідки своїх дій та потенційний вплив на життя інших людей.

Пасивний OSINT в соціальних мережах є лише одним з інструментів для отримання інформації що до такого явища як наркоманія та наркозлочинність. Для більш повного та об'єктивного розуміння ситуації в сфері незаконного обігу психоактивних речовин необхідно використовувати комплексний підхід, включаючи аналіз інших відкритих джерел інформації та, за необхідності, активні методи розслідування, що проводяться органами

правопорядку, спеціальними службами та підрозділами, що протидіють незаконному обігу наркотичних засобів та психотропних речовин.

Таким чином, в умовах постійного зростання обсягів відкритої інформації та розвитку технологій, OSINT залишається надзвичайно актуальним та важливим інструментом для широкого кола правоохоронців та науковців, допомагаючи приймати обґрунтовані рішення, виявляти загрози та прогнозувати тенденції, отримувати цінну інформацію з доступних джерел.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ (OSINT) У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Мудрецька Г. В.

доцент кафедри кримінального процесу та криміналістики,

к.ю.н., доцент

ОДУВС

OSINT став невід'ємною частиною розвідувальної діяльності не лише урядових установ, а й міжнародних організацій. Завдяки швидкому розвитку інформаційних технологій та Інтернету, OSINT отримав новий поштовх, що зробило його важливим інструментом у сфері інформаційної безпеки, боротьби з тероризмом та у різних галузях комерційної діяльності [1, с.2]. Через повномасштабне вторгнення правоохоронні органи України активно використовують OSINT-технології у розслідуванні воєнних злочинів.

Однією з головних проблем, які постають в процесі проведення розслідування з використанням інформації з відкритих джерел, є «легалізація» отриманих доказів, оскільки кримінальне провадження має відбуватися в передбаченому кримінальним процесуальним законодавством порядку, а способи збирання та закріплення доказів мають відповідати встановленим законодавцем вимогам. Так, у п. 1 ч. 2. ст. 99 Кримінального процесуального кодексу України вказано що до документів, за умови наявності в них відомостей, передбачених ч.1 ч. 2 ст. 99, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) [2]. Комп'ютерні дані, як і будь-які докази що використовуються в кримінальному провадженні, повинні відповідати вимогам належності, допустимості та достовірності. Відповідно до положень ст. 85 КПК України, належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження. Обов'язок доводити зв'язок комп'ютерних даних з кримінальним провадженням покладений на сторону обвинувачення. Окрім цього, необхідним є доводити порядок отримання доказів, оскільки збирання доказів на основі відкритих джерел є складним та

багатоетапним процесом, кожна зі стадій якого повинна здійснюватися відповідно до положень закону. В іншому випадку доказ, отриманий з відкритих джерел, може бути визнаний судом недопустимим на основі доктрини плодів отруйного дерева [3, с. 106–112].

Крім того, слід враховувати достовірність доказу, а саме його відповідність дійсності. Оцінка достовірності електронних доказів супроводжується значною кількістю проблем. Так, в електронні докази досить легко вносити зміни, існує вірогідність допущення технічних помилок під час їх отримання, застосування невідповідних інструментів для збереження та доступу до них, тощо. Це значно зменшує їхню надійність [4]. Без фіксації метаданих ефективність OSINT досліджень на основі зображень і відео може знижуватись. Це пов'язано з тим, що метадані містяться у фото, відео, веб-сайтах, pdf файлах тощо, оскільки надають відомості про саме джерело інформації незалежно від її типу. Також варто пам'ятати, що певні соціальні мережі автоматично видаляють дані про координати місця, де було зроблено фото, одразу після завантаження такого фото у мережу. Однак, відомості, отримані з метаданих, не можуть використовуватися як докази в кримінальному провадженні, а тільки можуть вказувати на інші відомості, які потребують подальшої перевірки [5, с. 108]. Одним зі способів перевірки достовірності електронних доказів, який пропонує О.О. Торбас, є перевірка хеш-суми, що являє собою певне значення, обчислене на основі набору даних із застосуванням одного із математичних алгоритмів, що використовуються для перевірки цілісності даних при їхній передачі або збереженні. Так, якщо створюється копія певного файлу, то хеш-суми оригіналу та копії будуть збігатися. У разі ж заміни принаймні одного символу, хеш-сума буде відрізнятись [3, с. 112–118].

Оскільки під час OSINT-розслідувань дані збираються з відкритих джерел, постає питання про подальше збереження їх як доказів (електронних доказів) у кримінальному провадженні. Відповідно до п. 21 Протоколу Берклі, термін «докази» слід відрізнити від «інформації». Докази з відкритих джерел – це інформація у відкритому доступі із доказовою цінністю, яка може бути допущена для встановлення фактів у судовому процесі [6]. Протокол Берклі був створений спільно Школою права Каліфорнійського університету в Берклі та представниками Організації Об'єднаних Націй. У ньому сформульовано міжнародні стандарти проведення онлайн-розслідувань можливих порушень міжнародного права прав людини, міжнародного гуманітарного та кримінального права, містяться рекомендації з проведення процедур збору, аналізу та збереження цифрової інформації [7]. У главі II Протоколу наводиться перелік принципів, згідно з якими має здійснюватися розслідування. Вони поділяються на три категорії: професійні, методологічні та етичні. До професійних принципів відносяться: 1) відповідальність – необхідність несення особами, що проводять розслідування, відповідальності за свої дії; 2) компетенція - наявність

належного ступеня підготовки та навичок для проведення розслідування; 3) об'єктивність – недопустимість впливу особистих, культурних та структурних упереджень на розслідування; 4) законність - необхідність дотримання норм чинного законодавства під час проведення розслідування; 5) обізнаність у сфері безпеки - наявність базових знань у галузі оперативної безпеки, мінімізація цифрового сліду та усвідомлення потенційних ризиків [7, с. 11–13].

Отже, з метою забезпечення збереження комп'ютерних даних з відкритих джерел як доказів у кримінальному провадженні, складання протоколу огляду Інтернет-ресурсів має відбуватись за правилами КПК України з урахуванням особливостей, передбачених Протоколом Берклі, що надасть можливість не тільки зберегти відповідної інформації як доказу, а й забезпечити його достовірність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Думчиков М.О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. Академічні візії. Випуск 36.2024. С.1-6
2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17>
3. OSINT при розслідуванні кримінальних правопорушень: підручник / О.О. Торбас. – Одеса: Видавництво «Юридика», 2024. – 180 с
4. Бабаєва О.В., Авербах Д.В. Щодо питання про використання доказів, отриманих з відкритих джерел, у кримінальному провадженні. Науковий вісник Ужгородського Національного Університету. 2024. <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/28-2.pdf>
5. Коновалова Д.О. Особливості використання розвідки на основі відкритих джерел (osint) у кримінальному провадженні. Юридичний науковий електронний журнал. № 11/2024. http://www.lsej.org.ua/11_2024/108.pdf
6. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних: Пошук у відкритих джерелах. (б. д.). Організація Об'єднаних Націй. <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>
7. Berkeley Protocol on Digital Open-Source Investigations. United Nations, 2022. URL: <https://doi.org/10.18356/9789210053433>.

ІНСТРУМЕНТИ OSINT У ВИЯВЛЕННІ ФЕЙКОВИХ АКАУНТІВ І БОТ-МЕРЕЖ У СОЦІАЛЬНИХ МЕДІА

М'ясоєдова Анастасія Григорівна,
здобувачка першого (бакалаврського) рівня вищої освіти
спеціальності 081 «Право»
Одеського державного університету внутрішніх справ
Моргунова Тетяна Іванівна,
к.т.н., доцент,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету внутрішніх справ

У сучасному цифровому просторі соціальні медіа стали не лише каналом комунікації, а й інструментом маніпуляцій і психологічного тиску. Фейкові акаунти та бот-мережі, маскуючись під реальних користувачів, спотворюють громадську думку, що особливо небезпечно під час криз чи виборів. Вони технічно витончені, адаптивні до алгоритмів платформ, тому їх складно виявити.

OSINT дозволяє системно аналізувати активність у соцмережах, виявляти синхронність дій, схожі тексти та інші ознаки скоординованої поведінки. Це дає змогу будувати цілісну картину інформаційного поля без покладання лише на автоматичне блокування. Особливо актуально це в умовах гібридної війни, де бот-мережі використовуються для поширення ворожих наративів і підриву довіри до інституцій.

Використання OSINT дозволяє збирати величезні обсяги даних з різних джерел, таких як соціальні мережі, форуми, новинні сайти та інші публічні ресурси, що може порушувати приватність користувачів [1].

Фейковий акаунт – це профіль, створений для введення в оману; бот – програмний агент, що імітує людину; бот-мережа – узгоджена група таких акаунтів. У міжнародній практиці це описується терміном *coordinated inauthentic behavior* – організоване втручання в інформаційне середовище під виглядом природної активності.

Виявлення ботів базується на аналізі поведінкових патернів: схожі коментарі, синхронні реакції, однотипна активність, збіги в часі. Важливими ознаками є неповні профілі, слабкі соціальні зв'язки, а також графі взаємодій, що свідчать про централізоване управління. Візуальні OSINT-інструменти допомагають унаочнити структуру таких мереж.

Втім, чітка межа між ботами й людьми розмивається. Реальні користувачі можуть діяти механічно, а боти – бути достатньо переконливими. Саме тому OSINT-аналітик має володіти не лише технічними засобами, а й аналітичною інтуїцією.

Для ефективної роботи з динамічним потоком даних соцмереж OSINT має використовувати адаптивні інструменти. Наприклад, Botometer і

BotSentinel для Twitter (X) аналізують патерни поведінки, визначають ймовірність бот-активності, збирають статистику. Ноаху відслідковує поширення конкретних повідомлень, виявляючи джерела та візуалізуючи мережу репостів. Такі засоби дозволяють не лише виявляти фейки, а й розуміти, як саме дезінформація поширюється у цифровому просторі.

У сфері Telegram-аналітики особливо корисними є сервіси TGStat, Telemetr та TgScan, які дозволяють відстежувати зміну кількості підписників, частоту публікацій, різкі стрибки активності та аномальні взаємоз'язки між каналами. Це особливо актуально в умовах війни, коли Telegram використовується як основне джерело інформації – і дезінформації – для великої частини аудиторії. У Facebook і Instagram ефективно себе зарекомендували CrowdTangle (офіційний інструмент Meta для аналізу відкритої активності сторінок) та Graphika, яка поєднує аналітику зі штучним інтелектом, дозволяючи формувати соціальні графи, виявляти спільні джерела контенту та повторювані шаблони поведінки акаунтів.

З технічної точки зору всі ці інструменти ґрунтуються на збиранні відкритих даних – через API (інтерфейси доступу до структурованої інформації), веб-парсинг, трекінг хештегів, часових міток, геолокацій та елементів профілю. Саме зібрані у такий спосіб фрагменти дозволяють будувати аналітичну картину, розрізняти органічні та штучні інформаційні хвилі. Коли ці інструменти використовуються в сукупності, вони дозволяють не лише виявити фейкову активність, а й зрозуміти її мету, джерело та потенційний вплив на аудиторію. Це різноманіття інструментів доцільно класифікувати за сферами їх практичного застосування, що й відображено на рис. 1.

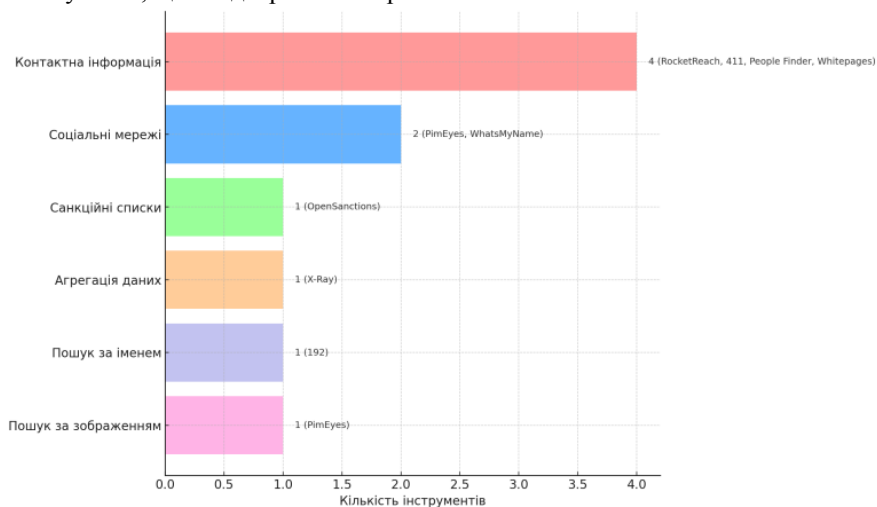


Рис. 1. Розподіл найпопулярніших OSINT-інструментів за категоріями використання (за даними OSINT-агенції Molfar, 2024) [2]

Як видно з рис.1, переважають інструменти для пошуку контактної інформації, що свідчить про високий попит на верифікацію особистостей у процесі аналітики. Таке співвідношення пояснюється потребою в точній ідентифікації джерел поширення контенту, що особливо актуально у випадках з фейковими акаунтами та маскуванню цифрового сліду. Водночас зберігається значущість платформ, орієнтованих на соціальні мережі, де відбувається основна активність ботів і координованих мереж.

Після етапу збору даних особливої ваги набуває аналітична обробка зібраної інформації. Саме в цьому полягає ключова сила OSINT: не лише побачити поверхневі сигнали активності, а й глибше проаналізувати поведінкові шаблони, виявити взаємозв'язки та синхронізацію дій. Аналіз фейкових акаунтів починається з низки базових, але показових параметрів, які у сукупності створюють індикативну картину. Зокрема, важливими ознаками підозрілих профілів є недавня дата створення акаунту, особливо у періоди інформаційної напруги, аномально висока частота публікацій, тематична одноманітність (наприклад, виключно політичні меседжі або прокремлівські наративи), а також відсутність персоналізованої аватарки чи активної взаємодії з іншими користувачами.

Узагальнені ознаки, за якими найчастіше ідентифікують фейкові акаунти, наведено в табл. 1.

Таблиця 1.

Основні індикатори фейкових акаунтів

Ознака	Опис
Дата створення акаунту	Нещодавно зареєстрований, особливо під час суспільно-важливих подій
Аватарка	Відсутня або використано стокове/згенероване зображення
Частота публікацій	Надмірна, з короткими інтервалами між постами
Тематична одноманітність	Публікації виключно на одну тему (політика, пропаганда тощо)
Повторюваність контенту	Шаблонні фрази, схожі гасла, ретвітинг одних і тих самих джерел
Взаємодія з іншими користувачами	Мінімальна або повністю відсутня
Активність	Скоординована з іншими акаунтами (час, тема, зміст)

До цього додається ще одна типова ознака – масове поширення однакового контенту: повторюваних текстів, гасел, зображень, що циркулюють із мінімальними варіаціями. На цьому етапі в аналітичний

процес активно залучаються інструменти обробки природної мови (Natural Language Processing, NLP), які дозволяють виявити повторювану лексику, шаблонні фрази, синтаксичні конструкції, не характерні для органічного користувацького спілкування.

NLP-аналіз допомагає оцінити автентичність акаунтів за риторикою, лексикою та емоційною тональністю. Виявлення мовних шаблонів дозволяє розпізнавати скоординовані кампанії з однотипним контентом. Аналіз зв'язків між акаунтами допомагає виявити бот-кластери, які діють синхронно, поширюючи повідомлення у визначені часові проміжки, зазвичай ізольовано від живих користувачів.

Фейковість визначається не лише за зовнішніми ознаками, а й за поведінковими характеристиками. OSINT поєднує мовний, мережевий і часовий аналіз, що дозволяє виявляти приховані впливи ще до їх масштабного розповсюдження.

OSINT особливо ефективний у кризових умовах. Під час війни в Україні аналіз Telegram-мереж дозволив виявити скоординовані інформаційні атаки, замасковані під свідчення очевидців. Подібні кампанії виявлялися і в період виборів: у Twitter/X тисячі ботів поширювали підготовлені меседжі, використовуючи ті самі хештеги та фальшиві геолокації. Візуалізація зв'язків дозволила простежити шлях фейкової інформації до трендів.

Міжнародні спільноти – EU DisinfoLab, Graphika, Bellingcat – поєднують OSINT з цифровою криміналістикою та соціальним аналізом. Вони викривають мережі фейкових ЗМІ, дезінформаційні операції та фабрики контенту, відновлюючи об'єктивність через аналіз структури поширення.

Отже, OSINT – це не лише інструмент реагування, а й засіб упередження загроз. У соцмережах, де фейки стали звичними, відкриті джерела дозволяють вчасно виявляти спроби маніпуляцій. Ефективна протидія потребує поєднання OSINT, кіберрозвідки та розуміння психологічного впливу – це дає змогу оцінити не лише джерело, а й силу його дії. Значення OSINT зростатиме разом із розвитком автоматизованих платформ на основі ШІ, здатних виявляти аномалії, загрози й прогнозувати їх розвиток.

На завершення відзначимо: майбутнє OSINT – це точна, відповідальна й адаптивна аналітична культура, що забезпечує інформаційну стійкість у добу гібридних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Главацька А.Л., Ангельська О.В., Опірський І.Р. Дослідження технологій використання OSINT як нової загрози з деанонізації особи в Інтернет просторі. *Кібербезпека: освіта, наука, техніка*. № 1 (25). 2024. С. 19-50.
2. Топ 10 OSINT інструментів 2024 року. Список від аналітиків Molfar: офіційний вебсайт OSINT-агенції Molfar. URL: <https://molfar.com/blog/top-10-osint-instrumentiv-2024-roku/>

ПЕРСПЕКТИВИ РОЗВИТКУ АНАЛІТИЧНОГО СУПРОВОДУ ПРОТИДІЇ НАРКОЗЛОЧИННОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Овсянюк Дмитро Іванович

підполковник поліції

Начальник аналітичного відділу

(Центр кримінальної аналітики)

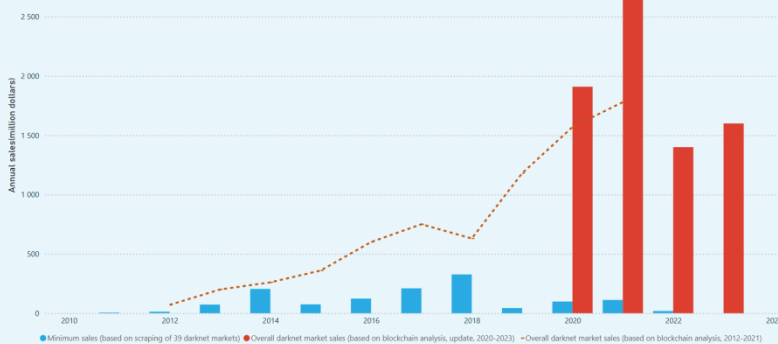
Національної академії внутрішніх справ

<https://orcid.org/0000-0002-1846-4167>

Сучасний світ характеризується інтенсивною інтеграцією інформаційних технологій у всі сфери суспільного життя, що кардинально змінило функціонування кримінального середовища. Мережа Інтернет стала невід'ємною частиною комунікації для значної частини населення, водночас відкривши нові можливості для злочинців. Вони оперативно адаптувалися до цифрових інструментів, використовуючи онлайн-платформи, такі як месенджери (зокрема, Telegram), соціальні мережі, тематичні форуми та Dark Web – прихований сегмент Інтернету, доступ до якого здійснюється через спеціалізоване програмне забезпечення (наприклад, Tor), для реалізації протиправних намірів. Особливу загрозу становить використання анонімних сегментів мережі, що ускладнює ідентифікацію правопорушників та унеможлиблює оперативне реагування з боку державних органів.

У сфері незаконного обігу наркотиків Інтернет перетворився на ефективний канал організації та координації злочинної діяльності: від вербування виконавців і логістики до реклами, маркетингу та оплати заборонених речовин. Згідно зі спільним аналізом Європолу та Європейського центру моніторингу наркотиків та наркоманії (EMCDDA), незаконний обіг наркотиків є одним із основних видів діяльності організованої злочинності [1]. Особливої уваги заслуговують Telegram-канали та торговельні майданчики в Dark Web, які перетворилися на основні джерела придбання наркотиків. За даними Управління Організації Об'єднаних Націй з питань наркотиків і злочинності (UNODC), загальний обсяг продажів у даркнеті стабільно зростає, незважаючи на тимчасові зниження після ліквідації великих ринків [2] (Рисунок 1).

Оцінка загального обсягу продажів на даркнет-ринках (переважно пов'язаних з наркотиками) на основі аналізу блокчейну та спостережень за мінімальними продажами на 39 основних даркнет-ринках (переважно пов'язаних з наркотиками), 2011-2023 рр.



Source: UNODC calculations based on Hikari Labs data and Chainalysis, Crypto Crime Report 2024 (and previous years).

Рисунок 1.

Джерело: UNODC (United Nations Office on Drugs and Crime). World Drug Report 2024. Drug market patterns and trends. 2024. URL: <https://www.unodc.org/unodc/en/data-and-analysis/wdr2024-drug-market-trends.html> (дата звернення: 15.05.2025).

Наразі правоохоронні органи стикаються зі значними труднощами через обмежені законодавчі можливості щодо ефективного блокування ресурсів та складність міжнародної правової взаємодії, що обмежує притягнення до відповідальності організаторів злочинних мереж.

Ефективна протидія складним та анонімним злочинним мережам у Dark Web вимагає не лише оперативних, а й ґрунтовних аналітичних підходів. У таких умовах надзвичайно важливим стає аналітичне супроводження розслідувань та оперативно-розшукових заходів, пов'язаних з незаконним обігом наркотиків в Інтернеті. Застосування кримінального аналізу дозволяє встановити або передбачити взаємозв'язки між накопиченими фактами, що у свою чергу допомагає побудувати, перевірити та виключити слідчі версії [3]. Кримінальний аналіз, як мультидисциплінарна інформаційно-аналітична діяльність, широко використовується провідними правоохоронними органами світу для підвищення ефективності протидії злочинності та раціонального використання ресурсів [4].

Ключовим методологічним інструментом при цьому є розвідувальний (аналітичний) цикл, який забезпечує структурований підхід до збору, аналізу й інтерпретації інформації [5]. Цей цикл включає послідовні динамічні фази: постановка завдань та планування; збір та оцінка даних (включно з інформацією з Telegram-каналів, блокчейну, фінансових операцій, форумів, honeypots); узагальнення, систематизація, обробка даних; глибокий аналіз

(формування гіпотез, ідентифікація організаторів, аналіз криптотранзакцій); підготовка звіту та зворотний зв'язок із замовником. Аналітичний супровід є важливим не лише для документування виконавців нижчої ланки, а й для встановлення ієрархічної структури злочинних спільнот, визначення ролей та виявлення їхніх організаторів. Хоча існують дискусії щодо досконалості цієї моделі, розвідувальний цикл залишається всеосяжною та гнучкою моделлю, здатною адаптуватися до специфіки діяльності, що вимагає структурованого підходу до аналізу інформації.

Для подальшого підвищення ефективності аналітичної діяльності в умовах цифрового середовища доцільно застосовувати інноваційні та проактивні методології збору інформації, зокрема системи **Honeypot** (імітовані комп'ютерні системи, що слугують «приманкою» для зловмисників). **Honeypot**, за своєю сутністю, є контрольованою інформаційною системою, що імітує потенційні цілі кіберзлочинців, створюючи ілюзію доступу до бажаних нелегальних товарів або послуг. Концептуально ця методологія ґрунтується на парадигмі превентивного збору розвідувальних даних, коли правоохоронні органи не реагують на вже скоєні злочини, а створюють умови для фіксації намірів та дій потенційних зловмисників. Впровадження **Honeypot**-систем вимагає розробки чітких стратегій щодо їхнього розміщення та безперервного моніторингу[6].

Серед перспективних різновидів **Honeypot**-систем можна виділити: системи фінансових пасток (для ідентифікації потоків криптовалют та учасників), пастки для виявлення інфраструктури виробництва наркотичних речовин (магазини-пастки обладнання та прекурсорів) та комунікаційні пастки (імітація захищених форумів для інфільтрації спільнот). Дані, отримані в межах таких пасток, після обробки можуть бути інтегровані у загальний аналітичний цикл. Також перспективним є використання методів тематичного моделювання (наприклад, **BERTopic**) та атрибуції авторства для виявлення взаємозв'язків між анонімними авторами у **Dark Web** та **Surface Web** (відкритому, загальнодоступному сегменті інтернету), що розширює можливості профілювання зловмисників.

Сучасний незаконний обіг наркотичних речовин у мережі Інтернет часто характеризується високим рівнем організації та чітко структурованими схемами злочинної діяльності з розподілом ролей (організатор, диспетчер, вербувальник, кур'єр, закладник), крім того, нерідко цією **діяльністю** займаються і «самозайняті» особи. У будь-кому форматі побудови злочинного бізнесу, його характерною рисою є відсутність безпосередньої комунікації між ієрархічними рівнями та використання засобів маскуванню електронної інформації, систем електронних платежів та активна протидія документуванню їхньої діяльності. Це призводить до того, що часто діяльність правоохоронних органів обмежується притягненням до відповідальності лише виконавців нижчої та середньої ланки.

Ефективна протидія вимагає кардинальної адаптації традиційних методів документування, акцентуючи увагу на аналізі цифрових слідів,

фінансових транзакцій (включаючи криптовалюти), моніторингу інтернет-ресурсів, а також підвищення професіоналізму правоохоронців у сфері кримінального аналізу, кібербезпеки та роботи з цифровими доказами. Важливим є використання спеціального програмного забезпечення для аналізу операцій з криптовалютами та деанонімізації транзакцій. Успішна боротьба з кібернаркозлочинністю також вимагає постійного обміну досвідом та тісної співпраці між правоохоронними органами, науковими установами та приватним сектором для спільної розробки інноваційних інструментів та стратегій. Лише комплексний підхід дозволить ефективно боротися з інтернет-торгівлею наркотиками, яка динамічно розвивається.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. EU Drug Markets: In-depth analysis
https://www.emcdda.europa.eu/publications/eu-drug-markets_en
2. UNODC (United Nations Office on Drugs and Crime). World Drug Report 2024. Drug market patterns and trends. 2024. URL: <https://www.unodc.org/unodc/en/data-and-analysis/wdr2024-drug-market-trends.html> (дата звернення: 15.05.2025).
3. Мірослав Яніцкі. Оперативний кримінальний аналіз: посібник / пер. Ігоря Родюка; за ред. Міжнародної організації з міграції (МОМ). Київ, 2009. 86 с.
4. Овсянюк Д. І. Становлення підрозділів кримінального аналізу Національної поліції України та вимоги до професійної компетентності аналітиків. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швец Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. – Київ: «ВАІТЕ», 2024. 444 с. С. 105-112
5. Ovsianiuk, D. (2024). Intelligence cycle as the basis of analytical activity in combating drug-related crime. *Law Journal of the National Academy of Internal Affairs*, 14(2), 95-104. doi: 10.56215/naia-chasopis/2.2024.95.
6. Morić, Z., Dakić, V., Regvart, D. Advancing Cybersecurity with Honey pots and Deception Strategies. *Informatics*. 2025. Vol. 12, № 1. 14. P 1-36 DOI: 10.3390/informatics12010014. URL: <https://www.mdpi.com/2227-9709/12/1/14> (дата звернення: 15.05.2025).

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ТА НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Омельян Ілля Федорович

курсант 212 взводу навчально-наукового інституту
підготовки фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Науковий керівник:

Тригуб С. М.

доктор філософії, викладач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

У сучасних умовах цифровізації суспільства регулювання кримінального аналізу та кібербезпеки набуває особливого значення у сфері правоохоронної діяльності. Ефективне використання інструментів кримінального аналізу забезпечує своєчасне виявлення, прогнозування та попередження злочинів, а належний рівень кібербезпеки — захист інформаційних систем правоохоронних органів від несанкціонованого доступу, витоку, знищення або спотворення даних. Правове регулювання цих напрямів діяльності потребує комплексного підходу, що охоплює нормативну, організаційну та технічну складові.

Кримінальний аналіз, як складова аналітичної підтримки оперативно-розшукової та слідчої роботи, регулюється низкою правових актів, серед яких центральне місце займають Кримінальний процесуальний кодекс України, Закон України «Про оперативно-розшукову діяльність», а також внутрішні інструкції та методичні рекомендації МВС, СБУ, ДБР та інших органів. Основна мета кримінального аналізу полягає у виявленні зв'язків між подіями, особами, місцями і обставинами злочинів, вивченні криміногенних факторів, а також оцінці ризиків, що загрожують суспільному порядку і безпеці. Його інструментами є як традиційні методи статистичного аналізу, так і сучасні цифрові платформи, що дозволяють обробляти великі обсяги даних (Big Data), включаючи дані соціальних мереж, банківські операції, відеоспостереження тощо [1, с. 75].

У сфері кібербезпеки особливого значення набувають такі нормативно-правові акти, як Закон України «Про основні засади забезпечення кібербезпеки України», «Стратегія кібербезпеки України», а також міжнародні стандарти (наприклад, рекомендації Європейського агентства з кібербезпеки — ENISA). Ці документи визначають підходи до захисту критичної інфраструктури, обміну інформацією між суб'єктами

кіберзахисту, розслідування кіберзлочинів і підготовки фахівців. У межах правоохоронної діяльності кібербезпека охоплює захист службових інформаційних систем, цифрових доказів, а також оперативну взаємодію з національними й міжнародними кіберцентрами [2, с. 26].

Щодо кібербезпеки, то ця сфера є більш формалізованою з огляду на її стратегічне значення для національної безпеки. Основними нормативними актами є Закон України «Про основні засади забезпечення кібербезпеки України» (2017), Указ Президента України «Про Стратегію кібербезпеки України», а також низка міжнародних документів, зокрема Будапештська конвенція про кіберзлочинність. У межах правоохоронної діяльності кібербезпека охоплює не лише технічні аспекти захисту інформаційних систем, а й кримінально-процесуальне регулювання збору та збереження цифрових доказів, кіберрозвідку, моніторинг соціальних мереж, кіберпатрулювання тощо. Попри це, на практиці виникають проблеми із законодавчим унормуванням таких понять, як «цифровий доказ», «лог-файл», «анонімна IP-адреса», «трафік даних» тощо, що ускладнює їх процесуальне використання у кримінальному провадженні [3, с. 92].

Також вкрай актуальним є питання забезпечення дотримання прав людини під час впровадження новітніх аналітичних та кіберзахисних засобів, зокрема у частині захисту персональних даних, недопущення незаконного стеження та використання цифрових доказів. Перспективи удосконалення нормативного регулювання полягають у гармонізації українського законодавства з європейськими стандартами, впровадженні уніфікованих інформаційно-аналітичних систем із захищеним доступом, а також підвищенні професійної підготовки кадрів у сфері кримінального аналізу та кіберзахисту. Створення мультиагентних міжвідомчих платформ, активна співпраця з INTERPOL, Europol, а також використання штучного інтелекту для оцінки ризиків є важливими кроками до побудови ефективної моделі інформаційної безпеки в правоохоронній системі [4, с. 10].

Таким чином, використання кримінального аналізу та кібербезпеки у правоохоронній діяльності є критично важливим для забезпечення ефективного реагування на сучасні виклики злочинності. Однак ця сфера залишається нормативно недостатньо унормованою, що створює правові та організаційні бар'єри на шляху до її повноцінного розвитку. Вирішення цих проблем передбачає прийняття спеціального законодавства про кримінальний аналіз, гармонізацію української нормативної бази з міжнародними стандартами кібербезпеки, розвиток міжвідомчої взаємодії, запровадження єдиних технічних протоколів обміну інформацією та посилення професійної підготовки кадрів. У перспективі також доцільно розробити етичний кодекс аналітика та удосконалити судову практику щодо прийнятності цифрових доказів. Це забезпечить не лише законність, а й високу ефективність правоохоронної діяльності в умовах цифрової трансформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гаруст Ю. В., Мельник В. І. Правоохоронні органи на захисті економічної безпеки України: адміністративно-правовий аспект: монографія. Суми : видавничо-виробниче підприємство «Мрія», 2019. 256 с.
2. Дерев'ягін О. О. Перспективи застосування методики кримінального аналізу у протидії кіберзлочинам. Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.). Одеса: Одеський державний університет внутрішніх справ, 2017. С. 175–176. 334
3. Мовчан А. В. Актуальні проблеми впровадження в органах Національної поліції України моделі поліцейської діяльності, керованої аналітикою. Соціально-правові студії. 2018. Вип. 1. С. 17–22.
4. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

СТВОРЕННЯ ПЕРЕДУМОВ ДЛЯ ЦИФРОВОГО ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ТА ПІДГОТОВКИ АНАЛІТИКІВ З МЕТОЮ ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ ЗАВДАНЬ З ВИЯВЛЕННЯ ТА РОЗШУКУ АКТИВІВ: АКТУАЛЬНІСТЬ І НАГАЛЬНІСТЬ СЬОГОДЕННЯ ТА ПИТАННЯ МАЙБУТЬОГО

Паламарчук Іван Васильович

к.ю.н., головний спеціаліст Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА)

Є догмою твердження - «щоб країна мала перспективи – держава зобов’язана дивитися далеко в майбутнє». Тому прийняття та підтримання такої усталеної позиції [1; 2] має свої плоди в контексті результатів розвитку Республіки Сингапур та Китайської Народної Республіки.

Крім того, зважаючи на настанови Тараса Григоровича Шевченка «І чужому навчається, й свого не цурайтесь» та переймаючи досвід і практику державного управління, у тому числі означених республік, для розвитку та укріплення України є необхідним вивчення питань майбутнього задля того, щоб не допустити входження країни в режим «надолуження».

Одним із таких питань майбутнього є питання правовідносин, що виникають із виявленням та розшуком активів в інтересах держави і в порядку визначеному законодавством, шляхом цифрового забезпечення означених заходів.

Тим паче, актуальність дослідження питання цифрового забезпечення, як приклад, кримінальних проваджень з питань виявлення та розшуку віртуальних активів в контексті забезпечення інтересів України підтверджується тим, що злочинці дедалі частіше намагаються приховати

свої активи в криптовалюти та інших віртуальних активах, вважаючи їх недосяжними для правоохоронців. Але наше спільне завдання – «Ми маємо забезпечити, щоб ці ресурси – а мова йде про мільйони і навіть мільярди доларів – активно працювали на зміцнення економіки та обороноздатності України. Кожен арештований криптоактив – це потенційні кошти для підтримки наших захисників та відбудови інфраструктури» [3].

Отже, задля реалізації визначених державою завдань, серед центральних органів виконавчої влади, що реалізують та формують різні види державних політик, які є невід’ємними складовими внутрішньої та зовнішньої політики України, функціонує Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА).

АРМА в установленому законом порядку здійснює виявлення активів (діяльність із встановлення факту існування активів, на які може бути накладено арешт у кримінальному провадженні, чи у справі про визнання необґрунтованими активів та їх стягнення в дохід держави) та їх розшук (діяльність із визначення місцезнаходження активів, на які може бути накладено арешт у кримінальному провадженні, чи у справі про визнання необґрунтованими активів та їх стягнення в дохід держави) [4].

Водночас, змістом Комплексного плану [5] впровадження такого процесуального учасника, кримінального провадження, який по суті в межах визначених повноважень забезпечував би виконання завдань цифрового забезпечення кримінального провадження, є «цифровий детектив», що на теперішній час та із урахуванням прогнозування подальшого розвитку таких правовідносин по суті є доцільним, послідовним та необхідним в таких реаліях. При цьому, виконання подібних функцій за своїми можливостями та набутою практикою можуть здійснювати відповідні структурні підрозділи АРМА (з питань виявлення та розшуку активів).

Варто зазначити, що АРМА інтенсивно впроваджує цифрові технології у сфері виявлення та розшуку активів, постійно взаємодіє в цьому напрямі з усіма правоохоронними органами, а також з компетентними структурами за кордоном. В АРМА створено ІТ-лабораторію, діяльність якої спрямована саме на аналіз даних з будь-яких цифрових носіїв інформації [6; 7; 8].

Слід зазначити, що кінцевим результатом діяльності АРМА з питань реалізації державної політики віднесеної до сфери його повноважень є подальше здійснення управління такими активами (які було виявлено та розшукано і на які було в установленому законом порядку накладено арешт та передано в управління АРМА) на умовах ефективності, а також збереження (за можливості – збільшення) їх економічної вартості [4].

Також, доречно наголосити, що якість виконання поставлених перед АРМА державою завдань, які виражаються в реалізації, зокрема, інтересу держави у вигляді забезпечення економічного добробуту України – залежав, залежить та буде залежати від виконання працівниками АРМА зазначених

законом [9] вимог при реалізації своїх повноважень.

При цьому наслідком виконання АРМА своїх повноважень є «результативність», яка може виражатися в економічному ефекті від діяльності АРМА – відношення отриманого результату до касових видатків із Державного бюджету України на діяльність АРМА.

Результативність подальшого виконання АРМА своїх повноважень в інтересах держави також залежить від відповідального підходу до формування та забезпечення передумов для реалізації державної політики, що відноситься до сфери повноважень АРМА.

Тому, таким підходом (як одним із основних) є формування у майбутнього покоління, зокрема, здобувачів відповідного рівня та ступеня освіти:

навичок конструктивної міжособистісної та суспільної взаємодії, яка ґрунтується на взаємоповазі, обміну досвідом і співпраці;

впровадження принципів солідарності та турботи про спільне благополуччя, яке у тому числі забезпечується прищепленням набутих (при реалізації державної політики у сфері виявлення, розшуку та управління активами одержаними від корупційних та інших злочинів) результативних для суспільства та держави знань і навичок для забезпечення ідеї безперервного правонаступництва держави з реалізації політики в зазначеній сфері.

Таким чином, з метою забезпечення передумов для подальшої реалізації державної політики, що відноситься до сфери повноважень АРМА, та забезпечення збереження набутих знань та практичних навичок з реалізації зазначеної державної політики, та на їх основі забезпечити примноження і збільшення результатів майбутніми поколіннями (в ідеях реалізації справи всього Українського народу) – нагально необхідним є передача та поширення таких знань і навичок серед здобувачів вищої освіти у галузях знань дотичних до державної політики, що реалізується АРМА. Як приклад, під час участі в наукових заходах, що проводяться на базі закладів вищої освіти; налагодженням взаємодії із закладами вищої освіти, із відповідним укладенням угод про співробітництво та партнерство на досягнення зазначеної ідеї, і т.п. При цьому, на сьогоднішній день АРМА здійснюються означені заходи [10], але реалізація таких заходів потребує застосування аналогії до інших сфер суспільного життя по принципу «не як випадок, а як правило» – тобто вимагає системного підходу, як приклад було застосовано системний підхід до прищеплення знань та навичок із цивільного захисту, на усіх рівнях суспільного життя [11].

Тому, задля забезпечення функціонування механізмів держави відповідно до реального стану справ, у тому числі з метою забезпечення передумов для підготовки аналітиків, задля забезпечення виконання завдань з виявлення та розшуку активів, із урахуванням можливостей та набутого досвіду України, у тому числі й АРМА, реалії сучасності та перспективи майбутнього нагально вимагають впровадження професії «цифровий детектив» - у зв'язку з чим означена ідея заслуговує на свою увагу та вимагає подальшого впровадження в практичну реалізацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Белл Деніел. Китайська модель. Політична меритократія та межі демократії /пер. з англ. Олександр Дем'янчук. – 2 ге вид., випр. – К.: Наш Формат, 2023. – 336 с.
2. Сингапурська історія. Мемуари Лі Куан Ю. Том 1/Пер. з англ. К. Сисосва, Л.Савицька. – К.: Видавництво Олексія Капусти: підрозділ «Агенції «Стандарт» - 2012. 514 с.
3. Віртуальні активи злочинців та корупціонерів стануть ресурсом для державного бюджету – Олена Дума. URL: <https://arma.gov.ua/news/typical/virtualni-aktivi-zlochintiv-ta-koruptsioneriv-stanut-resursom-dlya-derjavnogo-byudjetu-olena-duma> (дата звернення: 12.05.2025).
4. Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів : Закон України від 10.11.2015 р. № 772-VIII : станом на 17 трав. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/772-19#Text> (дата звернення: 17.05.2025).
5. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ Президента України від 11.05.2023 р. № 273/2023 : станом на 17 трав. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/273/2023#Text> (дата звернення: 17.05.2025).
6. АРМА сприяє реалізації проекту «Цифровий детектив». URL: <https://arma.gov.ua/news/typical/arma-spriyae-realizatsii-proektu-tsifrovii-detektiv> (дата звернення: 17.05.2025).
7. АРМА розробило Рекомендації з розшуку та арешту криптовалютних активів. URL: <https://arma.gov.ua/news/typical/arma-rozrobilo-rekomendatsii-z-rozshuku-ta-areshtu-kriptovalyutnih-aktiviv> (дата звернення: 17.05.2025).
8. Фахівці АРМА переймали досвід британських та американських експертів у сфері розшуку віртуальних активів. URL: <https://arma.gov.ua/news/typical/fahivtsi-arma-pereymali-dosvid-britanskih-ta-amerikanskih-ekspertiv-u-sferi-rozshuku-virtualnih-aktiviv> (дата звернення: 17.05.2025).
9. Про запобігання корупції : Закон України від 14.10.2014 р. № 1700-VII : станом на 17 трав. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1700-18#Text> (дата звернення: 17.05.2025).
10. Агентство з розшуку та менеджменту активів. URL: <https://arma.gov.ua> (дата звернення: 17.05.2025).
11. Закон України «Про внесення змін до деяких законодавчих актів України щодо розмежування повноважень між центральним органом виконавчої влади, що забезпечує формування державної політики у сфері цивільного захисту, та центральним органом виконавчої влади, що реалізує державну політику у сфері цивільного захисту» від 21.04.2022 № 2228-IX. Урядовий кур'єр. 2022. 17 черв. (№ 133).

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT

Парушев Данило Михайлович

курсант 2-го курсу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС

Поляков Євген Валентинович

доцент кафедри оперативного-розшукової діяльності

навчально-наукового інституту підготовки фахівців для підрозділів

кримінальної поліції

Національної поліції України ОДУВС

к.ю.н., доцент, полковник поліції

Розвідка на основі відкритих джерел (OSINT) являє собою систематизований процес збору, обробки та аналізу загальнодоступної інформації з метою отримання цінних розвідувальних даних. У сучасному світі, де обсяги відкритої інформації постійно зростають, OSINT набуває критичного значення для широкого кола користувачів – від державних установ та правоохоронних органів до журналістів, бізнесу та громадських активістів. Особливо актуальним є застосування практичних інструментів та алгоритмів OSINT в Україні, яка зіткнулася з гібридною війною, інформаційною агресією та необхідністю зміцнення національної безпеки.

Для України, яка перебуває в стані збройного конфлікту та протистоїть інформаційній агресії, знання та вміння у сфері OSINT є надзвичайно важливими. Триваючий конфлікт в Україні став каталізатором для широкого впровадження та розвитку практик OSINT у країні, перетворивши його на ключовий інструмент для забезпечення національної стійкості. Необхідність протистояти дезінформації, виявляти загрози та збирати інформацію про дії противника зумовила підвищений інтерес до методів та інструментів OSINT на різних рівнях суспільства.

Стандартизовані фреймворки для аналізу тактики, технік та процедур (TTPs). Стандартизовані фреймворки з відкритим кодом направляють аналітиків у виявленні та описі маніпулятивних дій, які використовуються на кожному етапі операцій FIMI (Foreign Information Manipulation and Interference), від планування до виконання. Ці моделі дозволяють ефективно розпізнавати ранні ознаки інциденту FIMI, ділитися та порівнювати аналітичні дані між командами, а також швидше зривати зловмисні операції. Прикладами цих моделей є модель «Ланцюг знищення онлайн-операції» чиї ланки включають (серед інших) придбання активів, координацію та планування, забезпечення залучення та довговічності), та фреймворк DISARM Red (організований у планування, підготовку, виконання та оцінку).

У межах стандартизованих фреймворків для аналізу тактики, технік та процедур (TTPs) у контексті протидії іноземному інформаційному

маніпулюванню та втручанню (FIMI) спрямовують увагу аналітиків на детальну класифікацію маніпулятивних дій, їх контекстуалізацію в межах етапів операції, виявлення індикаторів компрометації та поведінки, розуміння мотивації зловмисників, розробку ефективних контрзаходів, сприяння спільному розумінню та комунікації, відстеження еволюції TTPs та побудову бази знань, що є критично важливим для ефективної протидії загрозам FIMI.

Баланс і відповідальність: розслідування повинні поєднувати технічні можливості з етичною доцільністю, мінімізуючи шкоду окремим особам і групам. Це передбачає збалансування права на доступ до інформації з правом на приватність, забезпечуючи, щоб слідчі практики ненавмисно не увічнювали IBD (інформаційно-дезінформаційну діяльність). Обізнаність щодо правових обмежень. Ознайомлення з місцевими, національними та міжнародними законами, що регулюють цифрові розслідування, є важливим. Це включає забезпечення дотримання Загального регламенту про захист даних (GDPR) та інших відповідних правових рамок. Оцінка ризиків: проведення комплексної оцінки ризиків необхідне для виявлення потенційних правових та етичних питань, які можуть виникнути під час розслідування. Ця оцінка повинна враховувати ризики для слідчої групи, об'єктів розслідування та будь-яких третіх сторін, яких це може торкнутися. Розробка стратегій для пом'якшення цих вразливостей має вирішальне значення для підтримки цілісності та законності розслідування. Політики платформ: ознайомлення з політиками платформ, які досліджуються, забезпечує дотримання Умов надання послуг і розуміння того, як їх можна використовувати в зловмисних цілях. У світлі чинного національного законодавства та законодавства ЄС, такого як Закон про цифрові послуги (DSA), ця обізнаність сприяє підзвітності платформ, дозволяючи слідчим виявляти та пом'якшувати системні ризики.

Розслідування інформаційно-дезінформаційної діяльності (IBD) повинні поєднувати технічні можливості з етичною відповідальністю, мінімізуючи шкоду окремим особам та групам через збалансування доступу до інформації та права на приватність, а також уникаючи ненавмисного увічнення IBD; при цьому є важливим ознайомлення з місцевими, національними та міжнародними законами, такими як GDPR, що регулюють цифрові розслідування, проведення комплексної оцінки ризиків для виявлення та пом'якшення потенційних правових та етичних питань для всіх залучених сторін, та детальне ознайомлення з політиками досліджуваних платформ, зокрема у контексті чинного національного законодавства та законодавства ЄС, такого як DSA, для забезпечення їх дотримання та виявлення зловмисного використання. Згідно до законодавства України та практик спецслужб України, розслідування інформаційно-дезінформаційної діяльності (ІДД) здійснюються з урахуванням конституційних прав і свобод громадян, зокрема права на приватність та невтручання в особисте життя, що

вимагає отримання відповідних судових рішень для проведення певних слідчих дій. Законодавство України, включаючи Кримінальний процесуальний кодекс та закони про оперативно-розшукову діяльність, визначає чіткі процедури та підстави для збору та використання інформації, отриманої в ході розслідувань. Спецслужби України, такі як Служба безпеки України (СБУ) та інші уповноважені органи, керуються цими законодавчими нормами, а також відомчими інструкціями та етичними стандартами, що наголошують на необхідності мінімізації шкоди третім особам та запобіганні зловживанню отриманою інформацією. Особлива увага приділяється захисту персональних даних відповідно до Закону України «Про захист персональних даних». Крім того, у контексті протидії ІДД, враховується законодавство про інформацію, інформаційну безпеку та захист критичної інфраструктури, а також міжнародні договори та стандарти у цій сфері.

Повномасштабна війна з Росією породила величезний потік інформації, включно з дезінформацією, пропагандою та фейками. OSINT є критично важливим для верифікації даних, виявлення ворожої діяльності та документування воєнних злочинів. Однак, складність полягає у фільтрації достовірної інформації серед інформаційного шуму та протидії ворожим ІПСО (інформаційно-психологічним операціям). Зростає кількість кібератак на державні та приватні структури. OSINT може допомогти у виявленні потенційних загроз, аналізі шкідливого програмного забезпечення, відстеженні кіберзлочинців та розумінні їхніх тактик. Проблема полягає у швидкому реагуванні на нові загрози та необхідності постійного оновлення знань про кіберландшафт. OSINT може бути ефективним інструментом для виявлення корупційних схем, відстеження незаконних фінансових потоків, ідентифікації злочинних угруповань та збору доказів. Складність полягає у роботі з великими обсягами розрізнених даних та необхідності їхньої якісної обробки та аналізу. Зі збільшенням обсягу публічно доступної інформації зростає ризик порушення приватності. Важливо використовувати OSINT етично та в межах законодавства, уникаючи незаконного збору та розголошення персональних даних. Не всі державні органи, правоохоронні структури та аналітичні центри мають достатньо кваліфікованих фахівців з OSINT та необхідні інструменти. Існує потреба у навчанні, обміні досвідом та розвитку відповідних компетенцій.

Підсумовуючи, використання OSINT в Україні є життєво важливим та перспективним напрямком, особливо в умовах триваючої війни та складного інформаційного ландшафту. Попри значну проблематику, пов'язану з інформаційною агресією, кіберзагрозами, питаннями приватності та необхідністю підвищення кваліфікації фахівців, OSINT надає потужні інструменти для аналізу, верифікації та виявлення важливої інформації. Для повноцінного використання потенціалу OSINT в Україні необхідно активно працювати над вирішенням існуючих проблем, включаючи підвищення рівня обізнаності, навчання фахівців, покращення доступу до відкритих даних та

дотримання етичних норм. Успішне інтегрування OSINT у роботу державних органів, правоохоронних структур, аналітичних центрів та громадських організацій зробить Україну більш стійкою до зовнішніх та внутрішніх загроз, сприятиме її безпеці та розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. How to Detect and Analyse Identity-Based Disinformation/FIMI A Practical Guide to Conduct Open Source Investigations (November 2024) European Union External Action. с.5-8
2. Заяць, І. М. *OSINT як інструмент розслідувальної журналістики: прикладна перспектива*. Вісник Національного університету «Острозька академія». Серія: Право, № 1, с. 72–78. 2023 р.
3. Козлов, В. О. *Методи та засоби OSINT у сфері інформаційної безпеки*. Захист інформації, № 4, с. 32–39. 2020 р.
4. Савчук, Т. Г. *Інформаційна безпека та відкриті джерела: ризики та можливості*. Державне управління: удосконалення та розвиток, № 12. 2020 р.

«SSL STRIPPING» ТА «ARP POISONING» ЯК МЕТОДИ ОТРИМАННЯ ДОКАЗОВОЇ ІНФОРМАЦІЇ: ПРОБЛЕМНІ АСПЕКТИ

Пастух Дмитро Сергійович

студент 3 курсу 6 групи
відділення підготовки студентів денної
форми навчання інституту права та безпеки
спеціальності 081 «Право» ОДУВС
Науковий керівник:

Албул С. В.

кандидат юридичних наук, професор, професор
кафедри оперативно-розшукової діяльності навчально-наукового
інституту підготовки фахівців для підрозділів
кримінальної поліції НПУ ОДУВС

Право кожної особи на приватне та особисте життя є фундаментальним та невід’ємним, незалежно від її громадянства, місця перебування чи правового статусу. Ці права гарантуються як національним законодавством, так і міжнародно-правовими актами. Разом з тим, у сучасних умовах воєнного стану, соціальної напруги, економічної нестабільності, інформаційної перенасиченості та психологічного тиску особа може свідомо або несвідомо, у тому числі під впливом соціальної інженерії, вчиняти діяння, що підпадають під ознаки кримінального правопорушення.

Із розвитком національної системи забезпечення правопорядку,

оперативна діяльність отримала нормативно визначені рамки. У правовій системі України закріплені поняття оперативно-розшукових заходів, гласних та негласних слідчих (розшукових) дій, які регулюються, зокрема, Законом України «Про оперативно-розшукову діяльність» [1, с. 23], Кримінальним процесуальним кодексом України [5], а також низкою підзаконних нормативних актів та наказів. Однак практика свідчить про те, що за певних умов можливе здійснення негласних заходів і без попереднього погодження з уповноваженими особами. У подальшому постає питання про те, як зібрану таким чином інформацію трансформувати у належний та допустимий доказ у кримінальному провадженні. Отже сьогодні розглянемо особливості використання оперативних методів поза межами формальних процедур, а також визначено умови, за яких здобута інформація може набути статусу доказу відповідно до вимог кримінального процесуального законодавства.

Безумовно, з початком повномасштабного вторгнення на територію України, абревіатура OSINT (Open Source Intelligence), тобто розвідка на основі відкритих джерел, стала значно поширенішою у публічному дискурсі [3, с. 244]. У загальному розумінні, це методологія збору та аналізу інформації, яка є вільно доступною для громадськості. Ключовою характеристикою OSINT є те, що не передбачає порушення норм Розділу XVI Кримінального кодексу України, який стосується правопорушень у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку [4]. Однак, якщо заглибитися у питання походження величезних масивів інформації, що циркулюють не лише на загальнодоступних інтернет-ресурсах, але й у таких специфічних сегментах як DarkNet, виникає закономірне питання. Особливо, коли певні дані, що з'являються, зокрема, і в контексті діяльності деяких правоохоронних структур, презентуються як отримані з відкритих джерел.

Розглянемо кілька методів, за допомогою яких конфіденційна інформація може бути скомпрометована та перетворена на загальнодоступну. Йдеться про складні з технічної точки зору кіберзагрози, які, однак, набули широкого поширення через свою ефективність. Одним із таких методів є SSL Stripping — різновид атаки типу «людина посередині» (Man-in-the-Middle). Суть цього методу полягає у навмисному зниженні рівня безпеки з'єднання: зловмисник змінює захищене HTTPS-з'єднання на незашифроване HTTP, що відкриває можливість для перехоплення чутливих даних користувача. У зоні ризику можуть опинитися особисті дані, електронні цифрові підписи, а також нотаріальні документи.

Ще однією поширеною атакою є ARP Poisoning, яка базується на маніпуляції протоколом ARP (Address Resolution Protocol). У цьому випадку в локальну мережу надсилається підроблене ARP-повідомлення, що дозволяє зловмиснику перенаправити мережевий трафік через свій пристрій. Подібна атака дає змогу здійснювати перехоплення даних у реальному часі, підмінювати інформацію або отримати несанкціонований доступ до внутрішніх електронних

систем. Особливо небезпечно це для осіб, що мають справу з державними або корпоративними реєстрами, базами даних чи іншими електронними ресурсами, які містять конфіденційні відомості [2, с. 358].

На прикладі розглянутих кіберзагроз чітко простежується механізм, за допомогою якого конфіденційна інформація поступово втрачає свій захищений статус і перетворюється на загальнодоступну. Сучасні атаки, зокрема ті, що реалізуються через Wi-Fi-мережі, дозволяють зловмисникам обійти логічний захист інфраструктури без необхідності фізичного втручання. Отримавши доступ до маршрутизації трафіку, нападник фактично «вбудовується» у комунікаційний процес між користувачем і зовнішнім середовищем. У таких умовах користувач самостійно, без усвідомлення загрози, передає чутливі дані – логіни, паролі, платіжну інформацію, повідомлення з месенджерів, доступ до електронної пошти, акаунтів у банківських застосунках та соціальних мережах. Тобто, усе, що використовується в інтернет-просторі, стає доступним третім особам. На відміну від швидких атак, ці кібероперації можуть тривати тривалий час – тижнями або навіть місяцями – до моменту накопичення максимально повного масиву інформації, придатного для подальшого використання. У разі, якщо такий витік відбувається в контексті правоохоронної діяльності, зібрані дані можуть бути оприлюднені на платформах, подібних до WikiLeaks, що забезпечує їхнє стрімке поширення через журналістські розслідування та суспільний резонанс. Відтак, конфіденційна інформація набуває відкритого статусу, а її зміст починає використовуватись у межах кримінального провадження, формально задовольняючи вимоги доказової бази для НСРД, хоча її джерело – анонімне.

Якщо ж атака ініційована не правоохоронними органами, а приватними особами зі зловмисними намірами, наслідки можуть бути вкрай небезпечними: від шантажу й вимагання до спонукання жертви до вчинення протиправних дій. При цьому правове регулювання таких ситуацій в Україні залишається недосконалим – чинне законодавство не дає чітких відповідей щодо допустимості використання подібної інформації та юридичної відповідальності за її розповсюдження.

Отже, узагальнюючи викладене, варто наголосити на необхідності формування більш відповідального підходу до питань кібербезпеки як з боку держави, так і з боку громадян. Ігнорування її критичної ролі в сучасному інформаційному суспільстві є недопустимим. На особливу увагу заслуговує проблема застарілих державних стандартів комплексної системи захисту інформації (КСЗІ), які вже не відповідають викликам цифрової епохи. Доцільним кроком могло б стати їх перегляд або повна відмова на користь міжнародно визнаних стандартів, таких як ISO/IEC 27001, що забезпечують системний підхід до управління інформаційною безпекою. Важливо також забезпечити базову цифрову гігієну на рівні та рівні особистого користування. Громадяни мають бути проінформовані щодо актуальних загроз і методів протидії їм через офіційні джерела – зокрема, ресурси

Кіберполіції України, а також провідні українські та європейські платформи з кіберзахисту. Як мінімум, варто дотримуватись базових рекомендацій: використовувати приховані мережі Wi-Fi, уникати підключення до відкритих громадських точок доступу, ретельно перевіряти підозрілі посилання за допомогою антивірусного ПЗ таких розробників, як ESET або Symantec. Крім того, важливо впровадити у користування менеджери паролів, зокрема KeePass або Bitwarden, а також регулярно відключати функцію мобільної точки доступу, щоб зменшити ризики несанкціонованого підключення до пристроїв. Лише поєднання системного регулювання та підвищення цифрової обізнаності здатне забезпечити надійний рівень інформаційної безпеки як на рівні держави, так і кожного окремого користувача.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Албул С.В. Оперативно-розшукова діяльність: навчальний посібник / С. В. Албул, С. О. Єгоров, Є. В. Поляков, Т. Г. Щурат; за заг. ред. проф. С.В. Албула. Одеса : ОДУВС, 2023. 375 с.
2. Боксгорн А.В., Машенко В.С., Клейман М.Ю., Пастух Д.С. Блокчейн-технології як інструмент забезпечення кібербезпеки у сфері нотаріальної діяльності України. Право та державне управління. 2024. № 3. С. 357–364.
3. Ісмайлов К.Ю., Савенко Д.О. OSINT та соціальні мережі: загрози та можливості для молодіжних комунікацій. Sociological and psychologacal models of youth communication: VII International-scientific and practical conference (February 18-21, 2025). Copenhagen, Denmark, 2025. С 242–246.
4. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III із змін. [Електронний ресурс]. URL: <http://zakon1.rada.gov.ua> (дата звернення 11.05.2025 р.).
5. Кримінальний процесуальний кодекс України : закон України від 13.04.2012 № 4651-VI [Електронний ресурс]. URL: <http://zakon1.rada.gov.ua> (дата звернення 11.05.2025 р.).

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT

Перовський Микита Михайлович

курсант 2-го курсу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС

Науковий керівник:

Поляков Є. В.

доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту
підготовки фахівців для підрозділів
кримінальної поліції Національної поліції України ОДУВС
к.ю.н., доцент, полковник поліції

У сучасному цифровому середовищі збір та аналіз відкритої інформації набуває виняткового значення для державних органів, журналістських розслідувань, приватних компаній і спеціалізованих структур безпеки. Open Source Intelligence (OSINT) — це розвідувальна діяльність, що здійснюється шляхом збору даних з відкритих джерел, їх систематизації, фільтрації та аналітичного опрацювання. Попри широке використання цього підходу за кордоном, в Україні лише нещодавно відзначається формування сталої практики використання OSINT як окремого елемента інформаційної безпеки та дослідницьких методик.

Під практичними інструментами OSINT варто розуміти сукупність технічних і програмних засобів, які дозволяють отримати доступ до релевантної інформації з відкритих джерел, таких як соціальні мережі, онлайн-форуми, сайти державних установ, засоби масової інформації та реєстри. Серед поширених засобів, що застосовуються в OSINT-діяльності, варто відзначити сервіси аналізу метаданих (ExifTool, Metadata2Go), агрегатори інформації (Maltego, Spiderfoot), пошукові системи спеціального призначення (Shodan, Censys) та програми для роботи з API відкритих реєстрів.

Збір інформації за методикою OSINT відбувається поетапно. Алгоритм дослідження починається з чіткої постановки цілей збору інформації. Далі — визначення ключових запитів, формулювання гіпотез і побудова структури пошуку. На третьому етапі відбувається безпосередній збір інформації з релевантних джерел, при цьому обов'язково застосовується перевірка достовірності та верифікація інформації, отриманої з відкритих джерел.

Особливу увагу слід звернути на юридичні аспекти використання OSINT. Закон України «Про інформацію» та Закон України «Про доступ до публічної інформації» визначають рамки правомірного доступу до відкритих джерел. У цьому контексті важливо дотримуватися вимог щодо захисту персональних даних, передбачених Законом України «Про захист персональних даних», особливо коли мова йде про ідентифікацію фізичних

осіб або використання зібраної інформації у правоохоронних цілях.

Практичне використання OSINT має широке застосування у сфері безпеки. Так, в умовах збройної агресії проти України розвідувальні спільноти, волонтери та журналісти активно застосовують OSINT для встановлення місць дислокації ворожих військ, ідентифікації осіб, причетних до воєнних злочинів, документування пошкоджень об'єктів інфраструктури. Алгоритм дій у цьому випадку включає моніторинг соціальних мереж противника, геолокаційний аналіз, перевірку зображень і відео на предмет маніпуляцій.

Варто також зауважити, що систематизація знань у сфері OSINT набуває особливого значення у підготовці фахівців правоохоронних органів, аналітиків кібербезпеки та дослідників. Освітні платформи, тематичні онлайн-курси, а також публікації профільних науковців сприяють формуванню базових і практичних навичок у цій сфері. Окремо заслуговує на увагу досвід співпраці з міжнародними партнерами, зокрема участь у проєктах з цифрової безпеки та аналізу відкритих даних.

Таким чином, OSINT не лише демонструє ефективність у практичній площині, але й вимагає високого рівня відповідальності щодо зібраної інформації. Подальший розвиток цієї сфери в Україні повинен супроводжуватися оновленням нормативної бази, розвитком аналітичної інфраструктури та підготовкою фахівців відповідного профілю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бондаренко, О. І. *Використання OSINT в аналітичній діяльності правоохоронних органів*. Науковий вісник Дніпропетровського державного університету внутрішніх справ, № 2, с. 45–51. 2022 р.
2. Мельничук, С. А. *Правові аспекти використання відкритих джерел інформації в Україні*. Юридичний науковий електронний журнал, № 6, с. 88–91. 2021 р.
3. Заяць, І. М. *OSINT як інструмент розслідувальної журналістики: прикладна перспектива*. Вісник Національного університету «Острозька академія». Серія: Право, № 1, с. 72–78. 2023 р.
4. Козлов, В. О. *Методи та засоби OSINT у сфері інформаційної безпеки*. Захист інформації, № 4, с. 32–39. 2020 р.
5. Савчук, Т. Г. *Інформаційна безпека та відкриті джерела: ризики та можливості*. Державне управління: удосконалення та розвиток, № 12. 2020 р.

СУЧАСНІ ПОТУЖНІ ІНСТРУМЕНТИ OSINT

Пядишев В. Г.

професор кафедри кримінального аналізу та інформаційних технологій, д.ю.н., професор ОДУВС

Інструменти OSINT є ключовою частиною будь-якого процесу збору інформації, особливо коли йдеться про розуміння та зменшення поверхні

атаки в кіберрозвідці. OSINT – це потужний ресурс для збору даних у різних форматах, таких як текст, відео, зображення та аудіо. Використання передових технологій, таких як машинне навчання та нейронні мережі, дозволяє розпізнавати тенденції та закономірності, а також ідентифікувати ключові елементи, такі як окремі особи чи теми, шляхом аналізу різних джерел даних.

OSINT Framework. Це ключовий веб-інструмент для дослідників, який організовує ресурси розвідки з відкритим кодом за джерелом, типом та контекстом. Він широко використовується в різних секторах, включаючи уряд, правоохоронні органи та корпоративну безпеку, для задоволення різноманітних потреб у зборі даних. Внесок спільноти постійно вдосконалює фреймворк, тоді як його робота відповідає правовим стандартам, таким як GDPR, для забезпечення етичного збору даних [1, с. 1].

Google Dorks використовується з 2002 року, пропонує спеціалізовані запити, які використовують величезну індексацію Google для допомоги в розслідуваннях безпеки. Ці запити можуть знаходити певні типи файлів, розширення, текст на сторінках, заголовки та URL-адреси – інструменти, безцінні для дослідження деталей про осіб та компанії. Незважаючи на те, що пошукові системи зазвичай не індексують конфіденційні дані, такі як файли журналів, *Google Dorks* все ще може виявляти таку інформацію, забезпечуючи критичний ресурс для IT-безпеки.

theHarvester включений до дистрибутиву Kali Linux, – це комплексний інструмент, який використовується для збору інформації про субдомени, віртуальні хости, відкриті порти та адреси електронної пошти, пов'язані з будь-якою компанією чи веб-сайтом. *theHarvester* використовує такі джерела, як сервери ключів PGP, пошукові системи, такі як Google та Bing, і соціальні мережі, такі як LinkedIn, для збору даних, підтримуючи як пасивну розвідку, так і активні тести на проникнення. Цей інструмент особливо корисний для початкових етапів тестування на проникнення як у локальних, так і в авторизованих мережах третіх сторін [2, с. 2].

API SecurityTrails надає миттєвий доступ до поточних записів DNS-сервера та історичних записів (відомих як історія DNS), деталей домену та пов'язаних доменів, інформації про IP-адреси, а також даних WHOIS, щоб ви могли інтегрувати їх у власні програми для виявлення активів, розвідки загроз, оцінки ризиків тощо. Найкраще те, що вам потрібен лише HTTP-запит для отримання даних [3, с. 1].

BGPView дозволяє без зусиль відстежувати інформацію про маршрутизацію BGP та дані IP-адрес за допомогою *BGPView*, що спрощує завдання моніторингу мережі. Аналізувати конфігурації мережі, виявляйте загрози безпеці та безперешкодно контролюйте зміни маршрутизації. Цей інтуїтивно зрозумілий мережевий інструмент пропонує комплексну аналітику, доступну безпосередньо з вашого браузера, що дозволяє приймати обґрунтовані рішення для оптимізації продуктивності мережі, визначення

походження зловмисників тощо.

Recorded Future – база даних вразливостей. Надає доступ до детальної інформації про вразливості з цієї безкоштовної бази даних CVE. Цей інструмент надає безцінну інформацію командам безпеки, щоб випереджати нові CVE. Він містить корисну інформацію, таку як оцінка CVSS, рівень складності атаки, доступність, зведення кожного CVE, а також уражені продукти та ресурси для пом'якшення наслідків [4, с. 2].

Triage – «пісочниця шкідливого програмного забезпечення». Дозволяє безкоштовно досліджувати зразки шкідливого програмного забезпечення за допомогою однієї з найсучасніших та найпопулярніших пісочниць для аналізу шкідливого програмного забезпечення. Ця платформа пропонує налаштоване середовище, де ви можете надсилати великі обсяги зразків шкідливого програмного забезпечення, що дозволяє виявляти та витягувати конфігурації для широкого спектру сімейств шкідливих програм [5, с. 7].

Mitaka – це розширення для браузера OSINT, яке може допомогти покращити щоденні операції, пропонуючи інтуїтивно зрозумілий доступ до різноманітних функцій збору розвідувальних даних для ефективного виконання розвідувальних та слідчих завдань. Розроблене з орієнтованим на користувача підходом, *Mitaka* бездоганно інтегрує кілька модулів OSINT, що дозволяє проводити комплексний аналіз цільових об'єктів.

Recorded Future's Browser Extension дозволяє легко отримувати доступ до даних розвідки з будь-якого веб-ресурсу за допомогою цього розширення для браузера для аналізу загроз, що оптимізує операції безпеки. Це розширення OSINT допоможе вам розслідувати фішингові електронні листи, виявляти IOC, визначити пріоритети виправлення вразливостей та пришивидшувати обробку сповіщень у вашій SIEM.

HavelbeenPwned (Чи мене підловили?) може допомогти вам перевірити, чи був ваш обліковий запис скомпрометований у минулому. Цей сайт був розроблений Тросем Хантом, одним із найшанованіших фахівців з IT-безпеки на цьому ринку, і він роками надає точні звіти. Якщо ви підозрюєте, що ваш обліковий запис був скомпрометований, або хочете перевірити наявність сторонніх порушень зовнішніх облікових записів, це ідеальний інструмент. Він може відстежувати веб-компрометації з багатьох джерел, таких як Gmail, Hotmail, облікові записи Yahoo, а також LastFM, Kickstarter, Wordpress .com, LinkedIn та багато інших популярних веб-сайтів.

BuiltWith: служить комплексним профайлером для визначення різних технологій, розгорнутих на веб-сайтах, від серверних фреймворків до аналітики та систем управління контентом. Він надає поглиблений аналіз веб-налаштувань, що є вирішальним для конкурентної розвідки та розробки технологічної стратегії. Цей інструмент життєво важливий для тих, хто шукає розуміння технологічної інфраструктури цифрових платформ.

Shodan: розроблений Джоном Матерлі у 2009 році, служить монітором мережевої безпеки та спеціалізованою пошуковою системою для глибокого

Інтернету та Інтернету речей. Він дозволяє користувачам досліджувати безліч підключених до мережі пристроїв, організовуючи результати за країною, операційною системою та типом мережі, надаючи безцінну інформацію для дослідників IT-безпеки.

SpiderFoot: розроблений Стівом Мікаллефом, виділяється як провідний інструмент розвідки для автоматизації OSINT зі швидкими результатами в розвідці, розвідці загроз та моніторингу периметра. Він використовує понад 100 публічних джерел даних для збору розвідувальних даних про різні цілі, включаючи загальні імена, доменні імена, адреси електронної пошти та IP-адреси, спрощуючи процес завдяки простому у використанні вибору модулів та специфікації цілей.

Maltego, розроблений Paterva та представлений у дистрибутиві Kali Linux, є потужним інструментом, призначеним для детальної цифрової розвідки цілей. Він використовує «перетворення» для інтеграції та аналізу даних із зовнішніх програм, доступний як у безкоштовній, так і в комерційній версіях. Користувачі можуть запускати розслідування для отримання комплексних результатів, таких як IP-адреси, домени та номери AS, через платформу Maltego.

Nmap. Цей мережевий та портовий сканер є чудовим інструментом для збору розвідувальних даних, пропонуючи буквально десятки команд Nmap для виконання процесів розвідки як з терміналу, так і з графічного інтерфейсу.

Отже, існує безліч безкоштовних інструментів OSINT, які окремі особи та організації можуть використовувати вже сьогодні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. OSINT Framework. *OSINT Framework Com.* Site. URL : <https://osintframework.com/> (дата звернення: 02.05.2025).

2. TheHarvester. The information gathering suite. . *Edge-Security.Com* Site. URL : <https://www.edge-security.com/theharvester.php> (дата звернення: 02.05.2025).

3. SecurityTrails. Overview. *Securitytrails.Com.* URL : <https://docs.securitytrails.com/docs/overview> (дата звернення: 02.05.2025).

4. Recorded Future: Advanced Cyber Threat Intelligence. *Recordedfuture.Com.* URL : <https://www.recordedfuture.com/> (дата звернення: 02.05.2025).

5. Borges, E. Top 15 OSINT Tools for Expert Intelligence Gathering. *Recorded Futur* 29th April 2024. Site. URL : <https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools> (дата звернення: 02.05.2025).

**ВИКОНАННЯ ОБОВ'ЯЗКУ ЩОДО ЗАХИСТУ ВІТЧИЗНИ,
НЕЗАЛЕЖНОСТІ ТА ТЕРИТОРІАЛЬНОЇ ЦІЛІСНОСТІ УКРАЇНИ ЯК
ОБСТАВИНА, ЩО ВИКЛЮЧАЄ КРИМІНАЛЬНУ
ВІДПОВІДАЛЬНІСТЬ**

Флоренко Ганна Олександрівна,
студентка 2 курсу 3 групи
інституту права та безпеки
Науковий керівник:
Резніченко Г.С.

к.ю.н. ,доцент, доцент кафедри
кримінально-правових дисциплін ОДУВС

Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України як обставини, що виключає кримінальну відповідальність, зумовлена сучасними військово-політичними викликами, збройною агресією проти України та необхідністю правового врегулювання дій громадян, які беруть участь у захисті держави. В умовах війни важливо чітко визначити межі правомірного застосування сили, зокрема військовослужбовцями, добровольцями та іншими особами, які виконують конституційний обов'язок щодо оборони країни. Це сприяє зміцненню правопорядку, захисту прав захисників та формуванню справедливого правосуддя, що відповідає нормам міжнародного гуманітарного права.

В умовах триваючої збройної агресії російської федерації проти України, захист прав громадян, включаючи їхні основоположні права на життя, здоров'я, честь, гідність та власність, набуває особливої актуальності. Для забезпечення ефективного захисту цих прав, а також для регулювання порядку несення військової служби, 15 березня 2022 року Верховна Рада України прийняла Закон України «Про внесення змін до Кримінального кодексу України та інших законодавчих актів України щодо визначення обставин, що виключають кримінальну протиправність діяння та забезпечують бойовий імунітет в умовах дії воєнного стану». Цей закон вніс зміни до Кримінального кодексу України, зокрема, доповнивши його статтею 43-1, яка визначає обставини, що виключають кримінальну протиправність діяння в умовах воєнного стану. [3]

Згідно з частиною першою статті 43-1 Кримінального кодексу України, дії, вчинені в умовах воєнного стану або збройного конфлікту з метою відсічі агресії російської федерації чи іншої країни, не вважаються кримінальними правопорушеннями, якщо вони завдали шкоди життю чи здоров'ю агресора або правоохоронюваним інтересам. Проте, це правило не діє у випадках катувань, застосування заборонених міжнародним правом засобів ведення війни або інших порушень законів і звичаїв війни, визначених міжнародними договорами, ратифікованими Верховною Радою

України. [1]

Прейс С.В., зазначає, що аналіз статті 43-1 Кримінального кодексу України виявляє, що вона охоплює два типи ситуацій, які не є взаємовиключними, а можуть поєднуватися в одному діянні. Обидва типи мають спільні характеристики: діяння має відбуватися в умовах воєнного стану або збройного конфлікту, спричиненого агресією іншої держави; воно повинно бути спрямоване на відсіч або стримування цієї агресії; та воно не повинно містити ознак катувань, використання заборонених міжнародним правом засобів війни або інших порушень законів і звичаїв війни, визначених міжнародними договорами, ратифікованими Верховною Радою України.[4, с. 531]

Шармар О.М., аналізуючи статтю 43-1 Кримінального кодексу України закріплює, що захист Вітчизни як право та обов'язок особи. Поняття «бойового імунітету», що включає формулювання «неможливо було передбачити», вказує на відсутність необережної вини. Відсутність вини, своєю чергою, виключає склад кримінального правопорушення та підстави для кримінальної відповідальності.[6, с. 32]

Закон України «Про оборону України» доповнено визначенням «бойового імунітету», що звільняє військове командування, військовослужбовців, добровольців територіальної оборони, правоохоронців та інших осіб, які беруть участь в обороні України, від відповідальності за втрати особового складу, техніки та наслідки застосування зброї, якщо ці наслідки неможливо було передбачити або вони охоплюються виправданим ризиком. Виняток становлять випадки порушення законів війни та міжнародних договорів.[2]

Особа не несе відповідальності за застосування зброї, бойових припасів або вибухових речовин проти агресора, а також за пошкодження або знищення майна, пов'язані з цими діями, якщо вони були вчинені в умовах воєнного стану і спрямовані на відсіч агресії. Важливо розуміти, що надання таких прав, тісно пов'язане з дотриманням міжнародних норм. Навіть заподіяння шкоди правоохоронюваним інтересам не вважається кримінальним правопорушенням, якщо це сталося в процесі відсічі агресії в умовах воєнного стану. Таким чином, законодавець намагається створити правові умови для ефективного захисту України від збройної агресії, забезпечуючи захисникам певний ступінь правового захисту, але при цьому наголошуючи на необхідності дотримання міжнародних норм і правил.[5, с. 3]

В умовах триваючої збройної агресії проти України питання правового врегулювання дій військовослужбовців, добровольців та інших осіб, які виконують свій конституційний обов'язок щодо захисту держави, набуває особливої актуальності. Законодавчі зміни, зокрема прийняття статті 43-1 Кримінального кодексу України, спрямовані на врегулювання обставин, що виключають кримінальну відповідальність за дії, вчинені в умовах воєнного стану, якщо вони були спрямовані на відсіч агресії. Це дозволяє забезпечити ефективний захист України та її громадян, а також надає

військовослужбовцям необхідний бойовий імунітет.

Однак, бойовий імунітет не є абсолютним і не звільняє від відповідальності за порушення законів і звичаїв війни, катування або застосування заборонених міжнародним правом методів ведення війни. Це свідчить про прагнення законодавця забезпечити баланс між захистом військовослужбовців та дотриманням міжнародних норм. Важливо, що законодавство визнає дії, спрямовані на захист країни, такими, що не містять складу кримінального правопорушення, якщо вони здійснені в межах виправданого ризику і без умислу на вчинення воєнних злочинів.

Запровадження правових механізмів бойового імунітету є важливим кроком для зміцнення обороноздатності України. Це сприяє захисту військовослужбовців від необґрунтованого переслідування, що дозволяє їм виконувати бойові завдання без остраху за можливі юридичні наслідки, якщо їхні дії відповідали встановленим нормам. Водночас, законодавство залишає простір для правового контролю, запобігаючи безкарності у випадках порушень міжнародного гуманітарного права.

Таким чином, українське законодавство намагається забезпечити правовий захист осіб, які беруть участь у захисті країни, водночас встановлюючи чіткі межі застосування сили та наголошуючи на необхідності дотримання міжнародних норм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний кодекс України : Закон України від 05 квітня 2001 р. № 2341-III. URL : <https://zakon.rada.gov.ua/laws/show/2341-14> find=1&text=колабор#wl_1 (дата звернення: 12.
2. Про оборону України : Закон України від 6 грудня 1991 року № 1932-XII. URL : <https://zakon.rada.gov.ua/laws/show/1932-12#n138>
3. Про внесення змін до Кримінального кодексу України та інших законодавчих актів України щодо визначення обставин, що виключають кримінальну протиправність діяння та забезпечують бойовий імунітет в умовах дії воєнного стану : Закон України від 15.03.2022 року № 2124-IX. URL: <https://zakon.rada.gov.ua/laws/show/2124-20>
4. Преїс Є.В. Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, як новелла українського законодавства. *Юридичний науковий електронний журнал*. 2023. №4. С. 520-532.
5. Ковальчук О.Ю., Острогляд О.В. Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, як обставина, що виключає кримінальну протиправність діяння. 2023. №2. С. 4
6. Шрамар О.М. Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України як обставина, що виключає кримінальну протиправність діяння. *Вісник Асоціації кримінального права України*. 2022. № 1(17). С. 24-35.

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT У ПРОТИДІІ ОРГАНІЗОВАНИЙ ЗЛОЧИННОСТІ В УКРАЇНІ

Санакоев Дмитро Борисович

кандидат юридичних наук, доцент,
інспектор відділу оперативного моніторингу
Управління кримінального аналізу
ГУНП в Харківській області,
підполковник поліції

В умовах динамічного розвитку інформаційного простору ХХІ століття протидія організованій злочинності набуває якісно нових характеристик. З огляду на застосування сучасними злочинними угрупованнями передових цифрових технологій, від правоохоронних органів України вимагається забезпечення найвищого рівня оперативності та точності у здійсненні відповідних заходів [1]. Останній звіт SOCTA-2025 підтверджує, що організована злочинність являє собою значну та деструктивну силу, яка демонструє безпрецедентні темпи розвитку. Її еволюція зумовлена активним використанням новітніх технологій, цифрових платформ та нестабільної геополітичної ситуації, що сприяє розширенню її діяльності та посиленню впливу [2]. У цьому контексті, OSINT постає не як тимчасове явище, а як стратегічно важливий інструмент. Його застосування дозволяє систематизувати великі обсяги розрізнених даних, формуючи цілісне розуміння структури та діяльності злочинного світу.

OSINT базується на ідеї, що кожен публічно доступний фрагмент інформації може стати джерелом до викриття складних злочинних схем. В основі цієї парадигми – інтеграція кібернетичних підходів, машинного навчання та аналізу великих даних (Big Data). Завдяки цьому правоохоронні органи мають можливість не просто збирати інформацію, а створювати прогностичні моделі, що дозволяють оперативно реагувати на будь-які загрози. Теоретико-пізнавальний підхід OSINT трансформує розосереджені дані в єдину стратегічну картину, що дає змогу використовувати їх як основу для прийняття управлінських рішень на найвищому рівні.

Цей підхід підтверджується численними дослідженнями, які демонструють, що прив'язка до наукової методології забезпечує не лише оперативність, а й високий рівень достовірності аналізу даних. В умовах глобалізації та інтеграції цифрового простору, теоретична база OSINT стає незамінною платформою для протидії транснаціональній організованій злочинності [3-6].

Сучасні методи OSINT включають вагомий набір технологічних рішень, що суттєво вдосконалюють процес збору та аналізу даних, перетворюючи його на потужний інструмент аналітичного дослідження: *1) пошукові системи з розширеним функціоналом.* Сучасні алгоритми Google

Dorking та Yandex Dorking дозволяють здійснювати глибокі пошукові операції, вилучаючи релевантну інформацію з мільйонів доступних джерел; 2) *аналітичні платформи*. Інструменти на кшталт Maltego, SpiderFoot та Recon-ng створюють деталізовані мережеві карти зв'язків, що допомагають розкрити закриті схеми і структури злочинних груп; 3) *системи візуалізації даних*. Ключовим елементом є програмні засоби, здатні перетворити численні дані у зрозумілі графічні моделі – аналітичні діаграми, «мапи» зв'язків та часові лінії, які відкривають нові виміри розуміння ситуації. Позитивним прикладом таких систем є, зокрема, IBM i2 Analyst's Notebook, Palantir Gotham, Neo4j та ін. Ці системи використовуються правоохоронними і розвідувальними структурами у багатьох країнах для інтеграції великих обсягів даних і їх оперативної візуалізації; 4) *алгоритми машинного навчання*. Сучасні аналітичні платформи не лише відображають поточний стан злочинних мереж, але й дають змогу прогнозувати їх еволюцію завдяки використанню алгоритмів машинного навчання та штучного інтелекту. Такий інтегрований підхід допомагає оперативно реагувати на загрози та вдосконалювати методи протидії.

Реальний потенціал OSINT виявляється в інтеграції цих інструментів у злагоджену систему роботи правоохоронних органів. Спільна робота фахівців з кібербезпеки, аналітиків та поліцейських створює синергійний ефект, що перевищує суму окремих дій. Прикладами ефективного використання правоохоронними органами аналітичних інструментів у протидії організованій злочинності є, зокрема, досвід Європолу [7] та багатьох інших.

На базі сучасних аналітичних платформ сформувались алгоритми, що забезпечують максимальну ефективність роботи з OSINT [8, с. 6], водночас, як показує аналіз практики підрозділів кримінального аналізу Національної поліції України, побудувати типовий алгоритм такої роботи за аналогією з алгоритмами розслідування окремих видів кримінальних правопорушень не завжди є ефективним із кількох причин.

По-перше, такі алгоритми занадто лінійні та статичні, адже зазвичай представлені як послідовність чітко визначених кроків. У реальності OSINT-розслідування часто є ітеративним процесом, де результати одного етапу можуть вимагати повернення до попередніх або паралельного виконання кількох завдань. А це потребує гнучкості та можливості адаптації до непередбачуваних змін у доступних даних. *По-друге*, на кожному етапі алгоритму має приділятися увага дотриманню етичних норм та національного законодавства, питанням законності збору даних, захисту приватності та відповідальності за використання OSINT-інформації, що є критично важливим для використання такої інформації у доказуванні. *По-третє*, алгоритмізація цього процесу має враховувати динамічний процес змін доступності та характеру відкритих джерел, появи нових, та закриття старих платформ, змін API та політики конфіденційності, що вимагає

постійного моніторингу та адаптації до цих змін. *По-четверте*, такі алгоритми мають враховувати необхідність використання високоефективних інструментів та методів для роботи з великими даними в реальному часі, а не у статистиці. *По-п'яте*, ефективна протидія організованій злочинності вимагає співпраці між OSINT-аналітиками, слідчими, криміналістами та іншими експертами, що також має бути враховано при побудові алгоритмів з інтеграцією OSINT-розвідок у загальний процес розслідування.

На цих підставах пропонуємо алгоритм OSINT-розслідувань з питань протидії організованій злочинності з урахуванням принципів гнучкості, етичності, динамічного підходу до джерел, ефективної обробки даних та міждисциплінарної співпраці та в умовах дії правового режиму воєнного стану:

Формулювання розвідувального питання та визначення меж розслідування: чітке визначення інформаційної потреби, яка має бути задоволена за допомогою OSINT. Врахування юридичних та етичних обмежень. (Див., наприклад: [9]).

Стратегічне планування збору даних: визначення пріоритетних категорій джерел (наприклад, соціальні мережі, публічні реєстри, Darknet-форуми). Розробка стратегії використання інструментів автоматизованого збору даних (скриптів, API) та ручних методів (глибокий аналіз контенту, встановлення контактів під прикриттям, моніторинг закритих форумів). Врахування потенційних ризиків та методів їхнього мінімізації (наприклад, використання VPN, віртуальних машин) (Див., наприклад: [10]).

Динамічний збір та фільтрація даних: постійний моніторинг визначених джерел на предмет нової інформації. Застосування фільтрів та критеріїв для відбору релевантних даних на ранніх етапах. Використання технік машинного навчання для автоматичної класифікації та пріоритизації інформації.

Етична та юридична оцінка зібраних даних: На кожному етапі перевірка законності отримання та використання даних. Оцінка потенційного впливу на приватність осіб. Дотримання принципів мінімізації даних та пропорційності (Див., наприклад, [11; 12]).

Інтегрований аналіз та кореляція: об'єднання даних з різних джерел для отримання цілісної картини. Використання різних аналітичних методів (мережевий аналіз, геопросторовий аналіз, часовий аналіз, кримінальний аналіз). Застосування платформ для візуалізації даних та виявлення прихованих зв'язків.

Контекстуалізація та верифікація: порівняння OSINT-результатів з іншими джерелами інформації (наприклад, даними правоохоронних органів, свідченнями). Оцінка надійності джерел та достовірності отриманої інформації. Застосування методів критичного мислення та аналізу підтверджень.

Спільне використання розвідувальної інформації та співпраця: обмін OSINT-результатами з іншими членами слідчої групи та відповідними органами; забезпечення належного рівня захисту чутливої інформації; сприяння міждисциплінарній співпраці для інтеграції OSINT у загальний

процес розслідування, зокрема, на підставі Меморандуму про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку [13].

Зворотний зв'язок та адаптація: оцінка ефективності застосованих OSINT-методів та інструментів. В умовах дії правового режиму воєнного стану вважаємо за доцільне перейняти досвід військових підрозділів та включити принципи навчання на основі досвіду (AAR – After Action Review) як обов'язковий елемент OSINT-розслідувань, що передбачає збір відгуків від користувачів розвідувальної інформації, постійне вдосконалення алгоритму на основі отриманого досвіду та змін у інформаційному просторі (Див., наприклад, [14]).

Отже, боротьба з організованою злочинністю вимагає від правоохоронних органів України не тільки впровадження новітніх технологій, але й системного осмислення процесу збору і аналізу даних. У цій доповіді ми демонструємо, що OSINT – це потужний аналітичний інструмент, який, поєднуючи наукову методологію, сучасні алгоритмічні рішення та інтеграцію цифрових технологій, може забезпечити не лише реактивну, а й проактивну роботу у сфері протидії організованій злочинності. Поєднання технологічних інновацій і правового забезпечення створює унікальну платформу для ефективної та законодавчо обґрунтованої протидії злочинним об'єднанням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Санакоєв Д., Вашко А. та Єфімов В. (2022). Впровадження європейської методології SOCTA у боротьбі з організованою злочинністю в Україні. *Науковий вісник Дніпровського державного університету внутрішніх справ, 1 (116)*, 213-220.
2. The changing DNA of serious and organised crime (EU-SOCTA 2025). URL: <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
3. Краснов О. Транснаціональна організована злочинність: риси та напрями протидії. *Вісник Національної академії Державної прикордонної служби України: Юридичні науки, 2019. Випуск 3*. URL: <https://periodica.nadpsu.edu.ua/index.php/legal/article/view/22/24>
4. Жаровська Г.П. Теорія та практика протидії транснаціональній організованій злочинності в Україні. Дис. на здоб. наук. ст. д.ю.н. за спец. 12.00.08 – кримінальне право та криминологія; кримінально-виконавче право. Національна академія внутрішніх справ, Київ, 2019. 593 с.
5. Жаровська Г.П. Наукові підходи до визначення організованої транснаціональної злочинності. *Науковий вісник Національної академії внутрішніх справ, 2018. № 3 (108)*. URL: <https://elar.navs.edu.ua/items/88430554-d23c-4b26-8032-0bd5e6670971>
6. Думчиков М.О. Використання OSINT технологій для виявлення

- корупційних правопорушень: сучасні підходи та виклики. Академічні візії. Вип. 26/2024. URL: <https://academy-vision.org/index.php/av/article/download/1391/1269/1288>)
7. Encrypted app intelligence exposes sprawling criminal networks across Europe: Europol (15.04.2025). URL: <https://www.europol.europa.eu/media-press/newsroom/news/encrypted-app-intelligence-exposes-sprawling-criminal-networks-across-europe>
 8. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний poradnik / Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Харків: ПІЮК для СБУ, 2023. URL: https://dspace.nlu.edu.ua/jspui/bitstream/123456789/19712/1/P_OSINT.pdf
 9. NATO Open Source Intelligence Handbook, 2002. URL: (https://athens.indymedia.org/media/old/nato_osint_reader.pdf)
 10. The OSINT Foundation Body of Knowledge, 2022. URL: <https://www.osintfoundation.com/Document.asp?DocID=11775>
 11. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)». URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
 12. Протокол Берклі з ведення розслідувань з 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 (Попередня версія), Нью-Йорк і Женева, 2020. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>
 13. Меморандум про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку (ратифіковано Законом України від 04.06.2015 № 507-VIII). URL: https://zakon.rada.gov.ua/laws/show/984_a12#Text
 14. After Action Review: покрокова інструкція проведення для інструкторів і командирів в Збройних Силах України: «Аналіз Проведених Дій». (2024). URL: <https://drive.google.com/file/d/1gNlveGjb7Vy4ctkyA-imD2cnuLMV3yak/view>

OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТОВАННІ ВОЄННИХ ЗЛОЧИНІВ

Сінчук Михайло Сергійович

курсант 201 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України Одеського
державного університету внутрішніх справ
Науковий керівник:

Свинаренко Ю. П.

доктор філософії, завідувач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України Одеського
державного університету внутрішніх справ

Документування воєнних злочинів є важливою складовою правосуддя під час збройного конфлікту, а сучасні технології відіграють важливу роль у забезпеченні об'єктивності та надійності доказової бази. Одним з таких інструментів є використання відкритих джерел інформації OSINT, що включає супутникові знімки, відео з соціальних мереж, документи з інтернет-ресурсів та інші доступні джерела. В Україні, після початку збройної агресії росії в 2022 році, застосування OSINT-технологій набуло особливої актуальності для підтвердження фактів порушень міжнародного гуманітарного права, зокрема воєнних злочинів [1].

В Україні використання даних з відкритих джерел регулюється кількома важливими законодавчими актами. Згідно зі статтею 84 Кримінального процесуального кодексу України КПК, докази є фактичними даними, що мають значення для встановлення обставин кримінального провадження. Це включає інформацію з відкритих джерел, яка повинна бути належним чином зафіксована, збережена і перевірена на достовірність. Стаття 85 КПК визначає вимоги до перевірки доказів, що надають можливість органам правопорядку використовувати дані з відкритих джерел, у тому числі через верифікацію та аналіз інформації для забезпечення правосуддя [3].

На міжнародному рівні використання OSINT у розслідуваннях воєнних злочинів регулюється низкою стандартів та практик, затверджених міжнародними організаціями, такими як Рада Європи, Європейський Союз та Міжнародний кримінальний суд (МКС). Програма підтримки, започаткована ЄС та Радою Європи, спрямована на навчання слідчих і прокурорів, які займаються документуванням порушень прав людини і воєнних злочинів. Під час спеціальних тренінгів, проведених в Україні та за її межами, учасники ознайомлюються з методами збору та аналізу даних з відкритих джерел, а також з правовими аспектами їх використання в кримінальних справах.

Важливою є також співпраця з Міжнародним кримінальним судом, який активно використовує OSINT для розслідування злочинів в Україні [4, с.168].

Практичне застосування OSINT у розслідуваннях воєнних злочинів включає широкий спектр технологій, таких як супутникові знімки, геолокаційні дані, аналіз відео та фото з соціальних мереж, а також перехоплені електронні комунікації. Наприклад, супутникові знімки можуть фіксувати зміни на місцевості, що є доказом атаки на цивільні об'єкти або інфраструктуру. Геолокаційні дані дозволяють відстежити переміщення військових підрозділів або техніки в зоні бойових дій. Відео та фото, зняті місцевими мешканцями або міжнародними журналістами, можуть стати важливими доказами для ідентифікації порушників та підтвердження фактів насильства або злочинних дій [5, с.42].

Незважаючи на очевидні переваги, використання OSINT у документуванні воєнних злочинів стикається з певними викликами. Одним із головних є питання достовірності та автентичності отриманих даних. Оскільки відкриті джерела можуть бути маніпульованими або сфальсифікованими, для їх перевірки необхідно застосовувати спеціалізовані інструменти, такі як програмне забезпечення для верифікації відео та фотографій, а також геолокаційні інструменти для точного визначення місця події.

Приватний сектор і громадські організації також відіграють важливу роль у зборі та аналізі даних з відкритих джерел. Спеціалізовані компанії з кібербезпеки, а також неурядові організації, що займаються правами людини, активно співпрацюють з державними органами для збору доказів і документування злочинів. Наприклад, низка організацій використовує власні платформи для збору та зберігання електронних доказів, надаючи їх правоохоронним органам для подальшого розслідування. У жовтні 2024 року Національний координаційний центр кібербезпеки при РНБО України, разом з міжнародними партнерами, провели форум, присвячений електронним доказам і застосуванню OSINT у контексті воєнних злочинів [2].

Міжнародна співпраця є важливою складовою ефективного використання OSINT у розслідуваннях воєнних злочинів. Європол і Євроюст створили спеціальні робочі групи, що об'єднують фахівців з різних країн і забезпечують обмін інформацією. Міжнародні організації, такі як Міжнародний кримінальний суд МКС, активно працюють над збором доказів із відкритих джерел, що дозволяє створювати надійну доказову базу для подальшого притягнення до відповідальності осіб, що скоїли воєнні злочини. Європол, зокрема, створив спеціальну групу, яка допомагає українським правоохоронним органам здійснювати комплексний аналіз даних, отриманих через відкриті джерела [5, с.43].

Важливою складовою майбутнього розвитку OSINT в Україні є удосконалення нормативно-правової бази та впровадження новітніх технологій для збору та обробки відкритих джерел. Зокрема, необхідно розвивати законодавство в напрямку забезпечення належної правової

підготовки слідчих органів для використання даних з відкритих джерел, створювати інструменти для безпечного збору та збереження таких доказів. В Україні також необхідно вдосконалювати співпрацю з міжнародними партнерами, зокрема для створення інтегрованих платформ для обміну інформацією та підтримки в розслідуваннях воєнних злочинів [4, с.171].

Отже, OSINT-технології є потужним інструментом у документуванні воєнних злочинів, оскільки вони дозволяють швидко отримувати достовірні докази, що можуть бути використані в міжнародних судах. Водночас, для ефективного використання таких технологій необхідно забезпечити належну правову регуляцію, застосовувати сучасні методи верифікації та активно співпрацювати з міжнародними партнерами. Розвиток інфраструктури для збору та обробки відкритих джерел є ключовим елементом для досягнення справедливості та притягнення до відповідальності осіб, що порушують міжнародне гуманітарне право.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України про оперативно-розшукову діяльність Відомості Верховної Ради України (ВВР), 1992, № 22, ст.303 URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>
2. Закон України Про Національну поліцію Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379 URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>
3. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88 URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
4. Івкова В., Опірський, І. OSINT-технології як загроза кібербезпеці держави. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2025р. №3(27), 165–179с.
5. Габорець О. А. Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі : робота на здобуття кваліфікаційного ступеня магістра: спец. 125 - Кібербезпека та захист інформації / наук. кер. В. В. Муж. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. 80 с.

ІНСТИТУЦІЙНЕ СТАНОВЛЕННЯ ТА ФОРМУВАННЯ СТАНДАРТІВ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Стратулат Аріяна Русланівна
курсант 308 взводу факультету підготовки
фахівців для органів досудового розслідування
Національної поліції України Одеського
державного університету внутрішніх справ

Тригуб С. М.
доктор філософії, викладач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України Одеського
державного університету внутрішніх справ

Розвиток системи кримінального аналізу та кібербезпеки в Україні тісно пов'язаний із загальним процесом реформування національного сектору безпеки та правоохоронної діяльності, що активізувався у зв'язку з гібридними загрозами, зростанням транснаціональної організованої злочинності та кіберзлочинності.

Інституційне становлення цього напрямку розпочалося із впровадження в оперативну діяльність окремих інструментів інформаційного аналізу наприкінці 2000-х років. Зокрема, використання програмного забезпечення IBM i2 Analyst's Notebook у підрозділах Міністерства внутрішніх справ України стало першим прикладом запозичення аналітичних методів, властивих західним моделям поліції, керованої даними (intelligence-led policing). Поступово ці підходи поширилися серед інших підрозділів кримінальної міліції, а їхня ефективність актуалізувала питання про необхідність інституціоналізації аналітичної функції. У своєму дослідженні В. А. Литвинов вказує, що «у 2016 році наказом Національної поліції створено відділ кримінального аналізу, який запрацював у структурі Департаменту інформаційної підтримки та координації поліції «102»» [1, с. 131; 2]. Формування окремого підрозділу кримінального аналізу, засвідчило про початок формалізації даного напрямку у межах правоохоронної системи. Згодом розвиток цієї функції продовжився через зміцнення кадрового потенціалу, внутрішнє навчання, запровадження методичних рекомендацій та адаптацію організаційних структур.

Паралельно з цим, кібербезпека як складова національної безпеки набула особливого значення у зв'язку з агресією російської федерації, що супроводжується масованими кібератаками на державні інформаційні ресурси. У 2015 році було створено Департамент кіберполіції, а у 2016–2017 роках - посилено нормативне регулювання у цій сфері, зокрема

ухвалено ЗУ «Про основні засади забезпечення кібербезпеки України» [3].

Окрему роль у формуванні інституційного поля відіграють:

- Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку), відповідальна за технічну та криптографічну безпеку;

- CERT-UA — урядова команда реагування на комп'ютерні надзвичайні події, яка виконує функції моніторингу, аналізу інцидентів та координації між суб'єктами забезпечення кібербезпеки;

- Служба безпеки України, яка у межах контррозвідального захисту відповідає за безпеку критичної інфраструктури, виявлення кібершпигунства та протидію диверсіям у цифровому просторі.

Важливим елементом національної кіберстратегії є координація дій між основними суб'єктами кібербезпеки. Співпраця між НПУ, СБУ, Держспецзв'язку та CERT-UA яка здебільшого відбувається через міжвідомчі робочі групи, спільні навчання та обмін інформацією про кіберінциденти.

Наприклад, у 2022 році успішне блокування атаки на енергетичну інфраструктуру України було забезпечене завдяки оперативному обміну даними між кіберполіцією, CERT-UA та фахівцями СБУ [4].

Формування стандартів у сфері кримінального аналізу та кібербезпеки в Україні відбувається як на основі національного законодавства, так і шляхом адаптації міжнародних моделей. Так, імплементація принципів ISO/IEC 27001, NIST Cybersecurity Framework, а також Директиви 2016/1148 свідчить про європейський вектор правового розвитку [5; 6].

Як зазначає М. В. Корнієнко правоохоронні органи постійно використовують «оперативний аналіз (аналіз телефонних дзвінків, злочинних угруповань, справ, порівняльний аналіз); тактичний аналіз (кримінальний аналіз, дослідження кримінальних тенденцій, геопросторовий аналіз, аналіз місць концентрації злочинності, часовий аналіз, МО-аналіз, створення кримінальних моделей, профілі підозрюваних/жертв); стратегічний аналіз (SWOT-аналіз, PEST-аналіз, аналіз моделей/форм злочинності та профілювання, аналіз тенденцій, аналіз з використанням географічного профілювання); аналіз даних з відкритих джерел (OSINT); аналіз даних з багатьох джерел (Multi-Source Analysis)» [7, с. 400 - 401].

На думку автора (М. В. Корнієнко), аналітичні схеми є ключовим інструментом у виявленні структури злочинних угруповань та їхніх лідерів. Застосування методів аналізу соціальних мереж дозволяє ідентифікувати основні канали комунікації між учасниками, а також визначити ключові фігури, що координують злочинну діяльність. Такий підхід істотно підвищує ефективність планування оперативних дій [7, с. 401].

Однак, національне законодавство постійно зіштовхується з викликами, оскільки у більшості випадків виявлено проблеми з дублюванням повноважень, браком єдиних протоколів реагування та відсутністю централізованої системи розподілу відповідальності. Така ситуація вимагає створення нормативно визначених механізмів координації, які передбачали б

чіткий розподіл функцій, загальні стандарти інформування та інтеграцію національних центрів аналізу кіберзагроз. Наприклад, у сфері кримінального аналізу національні стандарти мають передбачати визначення основних понять (наприклад, «аналітична розвідка», «оперативно-аналітична інформація», «аналітичне досьє»), етапів аналітичної обробки інформації, вимог до формування звітності та правил взаємодії між суб'єктами аналізу.

Таким чином, розвиток кримінального аналізу в Україні демонструє поступову інституціалізацію цієї функції в межах правоохоронної системи, а також зростання значущості аналітичних методів у забезпеченні національної безпеки. Використання сучасних інструментів аналізу, зокрема соціальних мережових структур, сприяє ефективному виявленню злочинних зв'язків та підвищенню якості оперативного планування. Водночас відсутність єдиних стандартів та чітких регламентів вимагає подальшої роботи над створенням нормативної основи, що забезпечить системність, узгодженість і правову визначеність у сфері кримінального аналізу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Литвинов В. А. Козловська Т. А., Жерновий М. М., Овсянюк Д. І. Історія становлення підрозділів кримінального аналізу Національної поліції України. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.) / редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук. Київ : Національна академія внутрішніх справ, 2022. С. 113–116.
2. Наказ Національної поліції від 08 квітня 2016 року № 296 дск.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 Редакція від 20.04.2025 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 05.04.2025)
4. Інформація щодо кібератак 15 лютого 2022 року. URL: <https://cert.gov.ua/article/37139> (дата звернення 05.04.2025)
5. Міжнародний стандарт ISO/IEC 27001 [Електронний ресурс]. – Режим доступу: <http://www.iso.org> (дата звернення 05.04.2025)
6. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережових та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (дата звернення 05.04.2025)
7. Корнієнко М. В. Кримінальний аналіз у діяльності Національної поліції України. *Право і суспільство*. 2024. № 1. Т. 2. С. 397-402.

АЛГОРИТМ OSINT-АНАЛІЗУ ПУБЛІЧНОГО КОНТЕНТУ З МЕТОЮ ВИЯВЛЕННЯ ЗЛОЧИНІВ У СФЕРІ НЕЗАКОННОГО ОБІГУ НАРКОТИКІВ (СТ. 307 КК УКРАЇНИ)

Токолов Олександр

курсант 3 курсу факультету підготовки фахівців
для органів досудового розслідування НПУ ОДУВС

Науковий керівник:

Афонін Дмитро

кандидат юридичних наук, доцент,
завідувач науково-дослідної лабораторії
з проблемних питань кримінального аналізу ОДУВС

У сучасних умовах цифровізації та гібридної агресії, незаконний обіг наркотичних засобів дедалі активніше переміщується в онлайн-простір. Соціальні мережі, месенджери, форуми та інші цифрові платформи стали середовищем, у якому здійснюється реклама, збут і комунікація між наркодилерами та споживачами. Особливої актуальності набуває застосування OSINT (розвідки з відкритих джерел) для виявлення та документування злочинів, передбачених статтею 307 Кримінального кодексу України.

У фокусі дослідження — практичне використання OSINT як інструмента для збору доказів, виявлення структур збуту наркотиків, аналізу онлайн-активності правопорушників, а також алгоритмізація самого процесу виявлення таких злочинів у відкритому цифровому середовищі. Одним із ключових джерел інформації виступають соціальні платформи, такі як Telegram, Instagram, Facebook, YouTube, де розміщується контент, пов'язаний із продажем заборонених речовин. Для виявлення відповідної інформації дослідник або співробітник правоохоронного органу може застосовувати пошукові запити із використанням кримінального жаргону, поширених хештегів, географічних назв і слів-маркерів, які характерні для таких каналів комунікації.

Збір інформації з відкритих джерел здійснюється як вручну, так і за допомогою спеціалізованих інструментів. Наприклад, Google Dorking дозволяє через пошукові оператори знайти прихований або непомітний контент, пов'язаний із незаконним обігом наркотиків. Використання ключових слів у комбінації з іменами міст, назвами речовин або типами фасування дозволяє виявити акаунти, пости або файли, які містять ознаки злочинної діяльності. У Telegram можна застосовувати парсери або боти для автоматичного вилучення повідомлень з тематичних каналів, а також для аналізу структури зв'язків між учасниками таких груп. Зображення, які публікуються у месенджерах або соцмережах, можуть містити приховану метадані — координати GPS, дату зйомки, ідентифікатори пристроїв. Така інформація дає змогу встановити місце розміщення «закладки» або особу, яка зробила фото.

За допомогою програмного забезпечення, такого як Maltego, можна

візуалізувати зв'язки між цифровими об'єктами — наприклад, Telegram-каналами, Instagram-акаунтами, електронними адресами, IP-адресами чи доменами. Це дозволяє створити картину діяльності конкретного наркоторговця або групи осіб [3]. Додатково використовуються сервіси типу Wayback Machine, які дають доступ до архівних версій сторінок, навіть якщо контент був видалений. Інструменти аналізу відео та зображень, наприклад, YouTube Data Viewer або ExifTool дозволяють підтвердити автентичність матеріалів та встановити їхнє першоджерело [2, с. 139].

Також, популярності на даний момент набуває GitHub - нова Open Source бібліотека для OSINT, сервіс Hunter.io як інструмент пошуку адрес корпоративної пошти, за допомогою якого можна отримати контактну інформацію відповідно до домену. Такі відомості необхідні, щоб далі перевірити знайдені email на компрометацію. Hunter.io здатний обробити і витягти необхідні дані з 67 мільйонів відкритих джерел за допомогою 5 ключових методів: Domain Search - пошук email по домену або назвою організації; Email Finder - пошук окремого співробітника на ім'я і компанії; Email Verifier - підтвердження працездатності та актуальності пошти; Email Count - дозволяє дізнатися кількість email для одного домену або для однієї компанії; Account Information - управління особистим обліковим записом [1, с. 136-137]

Зібрана інформація повинна фіксуватися відповідно до кримінального процесуального законодавства — із збереженням цифрових слідів, оформленням протоколу огляду, зазначенням дати і часу доступу до ресурсу, а також підтвердженням автентичності джерел. Важливо враховувати, що не вся інформація, зібрана за допомогою OSINT, може бути визнана допустимим доказом у кримінальному провадженні. Зокрема, якщо було порушено порядок збирання або не дотримано прав людини у сфері захисту персональних даних. Тому особливу увагу слід приділяти не лише технічним аспектам аналізу, а й правовим умовам використання здобутих даних.

Узагальнюючи викладене, варто зазначити, що застосування технологій OSINT у діяльності правоохоронних органів створює нові можливості для попередження та розслідування злочинів, пов'язаних із незаконним обігом наркотиків. Ефективне поєднання алгоритмічного мислення, цифрових інструментів і правових знань дозволяє фіксувати кримінальні прояви ще на етапі їх підготовки та створювати інформаційно-аналітичну основу для проведення подальших слідчих дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації С. 135-137 URL: https://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/39.pdf
2. Дрижакова Д.Ю., Волинєць Р.А. Використання відкритих джерел інформації (OSINT) у сфері безпеки держави: технології та перспективи С. 138-141 URL: <https://www.researchgate.net/publication/390316593>
3. Охотнік Т.В., Алексик Н.В. Maltego як інструмент розвідки на основі відкритих джерел URL: <http://www.konferenciaonline.org.ua/ua/article/id-69/>

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

Толмачевська Єлизавета Сергіївна

студентка 3 курсу відділення підготовки студентів
денної форми навчання інституту права та безпеки
спеціальності 081 «Право» ОДУВС

Науковий керівник:

Албул С. В.

кандидат юридичних наук, професор, професор кафедри
оперативно-розшукової діяльності навчально-наукового
інституту підготовки фахівців для підрозділів
кримінальної поліції НПУ ОДУВС

Актуальність теми зумовлена необхідністю визначення, яким чином кримінальний аналіз сприяє підвищенню ефективності оперативно-розшукових заходів у протидії кримінальним правопорушенням. Зокрема, мова йде про обґрунтування значення застосування аналітичних методів у процесі виявлення та розслідування злочинів, встановлення підозрюваних осіб, а також про вивчення перешкод, що виникають під час збору та аналізу оперативної інформації. Особливу увагу слід приділити викликам, пов'язаним із захистом персональних даних та забезпеченням приватності, що ускладнює застосування аналітичних інструментів і може вплинути на кінцеві результати кримінального аналізу. Окрім цього, відсутність уніфікованих стандартів і методологічних підходів до здійснення аналізу в різних правоохоронних органах може призвести до варіативності в ефективності його застосування. Ще одним суттєвим аспектом є необхідність підвищення професійної підготовки співробітників правоохоронних органів, що передбачає додаткові інвестиції з боку держави у навчання та розвиток фахових компетентностей аналітиків.

Кримінальне провадження є багатокомпонентним та міждисциплінарним процесом, який потребує системного підходу до збору, опрацювання та застосування інформації. Одним із ключових засобів забезпечення ефективності розслідування є кримінальний аналіз — метод, що дає змогу об'єктивно досліджувати фактичні дані, докази та інші суттєві елементи, пов'язані з кримінальним правопорушенням. В межах своєї компетенції підрозділи кримінального аналізу Національної поліції України здійснюють збір, обробку, зберігання та захист відповідної інформації [2, с. 6–7].

Кримінальний аналіз виступає окремим видом інформаційно-аналітичної діяльності, основна мета якого — виявлення та точне встановлення зв'язків між відомостями про злочин та іншими релевантними даними з різноманітних джерел, що використовуються для оперативно-

розшукової та слідчої роботи. Під час аналітичної діяльності здійснюється цілеспрямований пошук, фіксація, аналіз, візуалізація та передача кримінальної інформації, що сприяє її ефективному використанню [2, с. 6–7]. Загальна мета кримінального аналізу полягає у формуванні нових підходів до оперативно-розшукових заходів і досудового розслідування, створенні комплексного аналітичного продукту, ефективному плануванні слідчих дій (як гласних, так і негласних), а також у підтримці діяльності органів правопорядку шляхом оцінки стану протидії злочинності, ідентифікації ризиків та тенденцій її розвитку. Кримінальний аналіз дозволяє обробляти великі обсяги інформації, і без залучення спеціалізованих методик це було б неможливо. Його застосування дає змогу відстежувати складні структури зв'язків між фігурантами справ, прогнозувати розвиток злочинності, виявляти впливових осіб і груп, а також визначати пріоритети роботи правоохоронних органів [2, с. 6–7].

Усі форми аналітичної діяльності тісно пов'язані з оперативною та слідчою роботою: аналіз не лише супроводжує ці процеси, а й формує підґрунтя для ухвалення рішень щодо подальших дій. Під час аналізу розглядають інформацію про злочинця, знаряддя і спосіб вчинення злочину, час, місце та обставини події. Інформаційний обмін між слідчими та оперативними працівниками включає не лише передачу вже наявних даних, але й активний їх пошук. Значні інформаційні потоки опрацьовуються за допомогою інтелектуальних технологій, які полегшують роботу правоохоронців і підвищують ефективність процесуального прийняття рішень [2, с. 6–7].

Слід зауважити, що відповідно до положень глави 15 розділу II Кримінального процесуального кодексу України, доступ до інформації щодо абонентів, їхніх з'єднань, маршрутів передачі, обсягів і тривалості телекомунікаційних послуг, а також іншої пов'язаної інформації, здійснюється у межах тимчасового доступу до речей і документів. Такий доступ надається лише на підставі ухвали слідчого судді або суду, виданої за клопотанням слідчого, погодженого з прокурором (ч. 1 ст. 159 КПК України) [1]. У межах кримінального аналізу така інформація, як правило, надається операторами чи провайдерами телекомунікацій, що володіють відповідними даними, з метою ознайомлення або отримання копій у порядку, визначеному законом [1].

Застосування кримінального аналізу базується на всебічному опрацюванні різнопланової інформації, серед якої особливо цінними є результати оперативно-розшукової діяльності. Завдяки цьому вдається визначити як індивідуальну, так і групову належність об'єктів оперативного інтересу, дослідити їхні характеристики, встановити фактори впливу, передбачити ймовірний розвиток подій та виявити приховані взаємозв'язки між ними. Хоча традиційно кримінальний аналіз спирався переважно на закриті джерела інформації, зокрема оперативні матеріали, звіти про слідчі

дії та судові документи, останніми роками все більшого значення набуває використання відкритих джерел (OSINT), які дають змогу доповнювати і верифікувати дані, зібрані оперативним шляхом [3, с. 208].

Залежно від характеру завдань оперативних підрозділів, інформаційні потреби можуть суттєво відрізнятись. Для ефективної діяльності важливими є як достовірні й перевірені дані, так і їхня доступність. Інформацію класифікують за ступенем відкритості (відкриті, загальнодоступні, конфіденційні джерела) та за її характеристиками (первинна, вичерпна, часткова) [3, с. 208]. Важливу роль грає і джерело походження інформації. Так, для друкованих видань часто простіше ідентифікувати авторство та оцінити достовірність даних, тоді як телебачення чи радіо можуть містити елементи інтерпретації або суб'єктивної оцінки подій. Тому аналітик має вміти критично оцінювати надійність кожного інформаційного каналу.

З огляду на сучасні виклики, зокрема повномасштабне вторгнення росії на територію України, актуалізується роль OSINT у зборі доказової бази під час розслідування воєнних злочинів. Відкриті джерела дедалі частіше стають основою для документування порушень міжнародного гуманітарного права та ідентифікації винних осіб [3, с. 49–53]. Сучасний кримінальний аналіз також включає методи аналізу телефонного трафіку, профілювання злочинців, а також використання новітніх технологій, таких як аналітика великих масивів даних і комп'ютерне моделювання, що дозволяють виявляти складні логічні зв'язки між різними елементами злочинної діяльності.

Ретельне проведення кримінального аналізу істотно підвищує ефективність розслідування кримінальних правопорушень. Завдяки аналітичному опрацюванню даних можливо оперативніше ідентифікувати правопорушників, з'ясувати мотиви їхніх дій та встановити ймовірні способи вчинення злочину. До того ж, такий аналіз сприяє оптимальному використанню ресурсів, що виділяються на проведення розслідування. З огляду на це, кримінальний аналіз включає такі ключові елементи: впорядковані аналітичні процедури; дослідження окремих рис і закономірностей; виявлення та інтерпретація зв'язків між кримінальними відомостями й іншими джерелами; цілеспрямована інформаційно-аналітична діяльність; обробка даних, необхідних для управлінських або слідчих рішень; орієнтація на попередження, припинення, викриття та розслідування злочинів або прийняття відповідних управлінських дій [4, с. 9].

Сучасні дослідники розрізняють два види кримінального аналізу: аналітичний пошук і аналітичне дослідження. Перший зосереджується на структуризації інформації задля полегшення її подальшого інтерпретування, другий — на встановленні взаємозв'язків між особами, подіями та об'єктами [5, с. 133]. Таким чином, кримінальний аналіз відіграє ключову роль у процесі здобуття інформації в межах оперативно-розшукової діяльності та кримінального провадження [6, с. 79]. Його значення важко переоцінити, оскільки він дозволяє ефективно використовувати наявні ресурси та

прискорює процес викриття злочинців. Подальше вивчення цього напрямку має важливе значення для вдосконалення методів розслідування.

Отже, слід наголосити, що кримінальний аналіз має суттєве значення в процесі отримання та обробки інформації у межах кримінального провадження, він є невід'ємним елементом ефективного розслідування злочинів. Завдяки кримінальному аналізу можливо систематизувати та інтерпретувати великі масиви даних з різних джерел, що сприяє виявленню взаємозв'язків між різними аспектами злочинної діяльності. Окрім того, кримінальний аналіз дозволяє виявляти кримінальні тенденції, створювати психологічні та поведінкові профілі правопорушників і прогнозувати їхні подальші дії, що значно підвищує ефективність діяльності правоохоронних органів. Цей метод відіграє важливу роль у зміцненні безпеки суспільства та стабільному функціонуванні правоохоронної системи. Його застосування збільшує ймовірність успішного розкриття правопорушень та притягнення винних до відповідальності. У зв'язку з цим, подальше вдосконалення та розвиток підходів до кримінального аналізу є ключовими завданнями для сучасних органів правопорядку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний процесуальний кодекс України : закон України від 13 квіт. 2012 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9–10. Ст. 88.
2. Албул С. В. Основи кримінального аналізу: посібник з елементами тренінгу / Албул С.В., Користін О.Є., Заець О.М., Ісмайлов К.Ю., Тетерятник Г.К., Горбаньов І.М. Одеса : ОДУВС, 2016. 112 с.
3. Сучасні методи досудового розслідування кримінальних правопорушень: підручник / С. В. Албул, О. М. Цільмак, О. Є. Користін [та ін.] ; за заг. ред. О. М. Цільмак. Одеса : Фенікс, 2017. 352 с.
4. Швець Д. В. Оперативно-розшукове моделювання в розкритті злочинів. *Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. Міжнар. наук.-практ. конф. (Харків, 30 листоп. 2018 р.)* / МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2018. – С. 15.
5. Ханькевич А. М. Використання кримінального аналізу в діяльності підрозділів кримінальної поліції. *Сучасні проблеми правового, економічного та соціального розвитку держави : тези доп. Міжнар. наук.-практ. конф. (Харків, 30 листоп. 2018 р.)* / МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2018. – С. 193.
6. Албул С. В. Загрози терористичного характеру: до питання визначення поняття. *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення: матеріали III Міжнародної науково-практичної конференції (м. Дніпро, 16 червня 2023 р.)*. Дніпро: ВНПЗ «Дніпровський гуманітарний університет», 2023. С. 78–80.

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Толмаченко Єгор

курсант 211 взводу навчально - наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС

Свинаренко Юрій Павлович

доктор філософії, завідувач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Сучасні виклики у сфері безпеки вимагають від держав адаптивних стратегій боротьби зі злочинністю та загрозами в кіберпросторі. Україна, як держава, що перебуває в умовах активної гібридної війни, особливо гостро відчуває потребу в удосконаленні кримінального аналізу та системи кібербезпеки. Еволюція цих напрямів є критично важливою для забезпечення національної безпеки, захисту критичної інфраструктури та ефективної протидії транснаціональній злочинності. [1]

Кримінальний аналіз як спеціалізований напрям правоохоронної діяльності почав активно розвиватися в Україні з початку 2000-х років. Злочинність уже користувалась всіма перевагами сучасних технологій, саме тому перед поліцією постало завдання пошуку гідного системного рішення. Одним із таких рішень стала розбудова напряму кримінального аналізу. Проте істотного розвитку він набув після початку реформи правоохоронних органів у 2015 році. Визначальною подією стало впровадження інституцій кримінальної аналітики у Національній поліції України (НПУ).

На сьогодні підрозділи кримінального аналізу функціонують у кожному з 25 обласних управлінь поліції, а також створено 35 підрозділів на місцевому рівні (сектор кримінального аналізу відділу кримінальної поліції районного управління поліції). Кількість працівників підрозділів кримінального аналізу на всіх рівнях складає більше 400 осіб, майже 70 % з них це аналітики-практики. [3]

Пріоритети діяльності підрозділів кримінального аналізу визначені з урахуванням успішних зарубіжних моделей та вимогами сьогодення. Крім інформаційно-аналітичного супроводження розкриття злочинів загальнокримінальної спрямованості, аналітики зосереджені на проведенні аналітичних досліджень у сфері ліквідації економічного підґрунтя для злочинної діяльності, зборі доказової бази воєнних злочинів країни-агресора, а також проведенні відеоаналітичних досліджень.

Розвитку кримінального аналізу в Україні сприяла міжнародна технічна допомога, зокрема програми ЄС (EUAM Ukraine) та підтримка

INTERPOL. Було впроваджено сучасні програмні засоби, такі як Palantir, i2 Analyst's Notebook, а також національні системи аналізу великих масивів даних. [2]

Пріоритетним є також раціональний розподіл аналітичних ресурсів. Служба кримінального аналізу налагодила взаємодію з міжнародними партнерами та разом з ними організувала постійний навчальний процес. Організовано навчальні заходи, стажування та курси. Аналітиками взято участь у значній кількості зустрічей на міжнародному рівні з представниками провідних правоохоронних організацій Європейського союзу.

Одним із останніх нововведень стала також розбудова відділу, відповідального за відео- та фотоаналіз.

Відеоаналіз в поєднанні з таким новими технологіями, як супутникові знімки, а також використання спеціалізованого програмного забезпечення розширюють можливості аналітичних підрозділів.

На сьогодні основними завданнями кримінального аналізу в Україні є: виявлення нових моделей злочинної діяльності; профілювання злочинців; створення карт злочинності; інформаційна підтримка оперативно-розшукових заходів; аналіз зв'язків між учасниками злочинних груп.

Із початком широкомасштабної російської агресії в 2014 році питання кібербезпеки набуло особливої актуальності. Атаки на державні органи, об'єкти енергетичної, транспортної та банківської інфраструктури продемонстрували високий рівень кіберзагроз.

У відповідь на нові виклики Україна почала формувати стратегію кібербезпеки, яка включає кілька ключових аспектів: а) створення національної системи кібербезпеки; б) посилення співпраці між державними органами, приватним сектором і міжнародними партнерами; в) розвиток кадрового потенціалу; г) удосконалення законодавчої бази.

У 2021 році прийнято нову редакцію Стратегію кібербезпеки України, яка врахувала зміни у світовому та національному кіберпросторі.

Одним із головних викликів залишається інтеграція розрізнених зусиль у єдину національну систему кіберзахисту, що здатна ефективно реагувати на як окремі інциденти, так і на системні кіберкампанії проти України.

У сучасних умовах ефективна протидія злочинності потребує інтеграції інструментів кримінального аналізу із заходами кібербезпеки. Такий підхід дозволяє не лише розслідувати кіберзлочини, а й прогнозувати нові загрози та виявляти закономірності в цифровій поведінці злочинців.

Пріоритетом розбудови служби кримінального аналізу є успішна інтеграція у світовий аналітичний простір. З цією метою в Департаменті створено відділ міжнародного співробітництва з обміну аналітичною інформацією. Вимоги до таких аналітиків високі – крім професійних знань і навичок від них вимагається вільне володіння іноземною мовою, а також основами міжнародного права та економіки [4].

В Україні вже здійснюються перші кроки до такої інтеграції.

Наприклад:

кримінальні аналітики працюють із даними з відкритих джерел (OSINT); аналізуються блокчейн-транзакції з метою виявлення незаконної діяльності; застосовуються технології штучного інтелекту для моніторингу кіберзагроз.

Особливе значення має взаємодія між кіберпідрозділами правоохоронних органів та аналітичними підрозділами, що дозволяє оперативніше реагувати на інциденти та будувати профілактичні стратегії.

Як висновок, розвиток кримінального аналізу та кібербезпеки в Україні є важливим елементом побудови стійкої системи національної безпеки. Незважаючи на досягнуті успіхи, країна потребує подальшого: а) інвестування в технології та навчання фахівців; б) вдосконалення міжвідомчої координації; в) інтеграції міжнародних стандартів і практик.

В умовах постійної ескалації кіберзагроз та гібридних атак кримінальний аналіз і кібербезпека повинні розвиватися синхронно, утворюючи єдиний адаптивний механізм захисту держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Користін О. Є., Пефтієв Д. О., Пеньков С. В., Некрасов В. А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою / ІЛР : навчальний посібник. К: «Видавництво Людмила», 2019. 120 с.

2. Указ Президента України № 64/2022 «Про введення воєнного стану в Україні».

3. Регламент (ЄС) 2016/679 Європейського парламенту та Ради [Архівовано 26 травня 2018 у Wayback Machine] від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

4. Бутко Р. Ю. Розвиток системи кримінального аналізу в діяльності Національної поліції України в сучасних умовах Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : матеріали міжвідом. наук.-практ. конф. (Київ, 17 лист. 2023 р.) / [редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук]. Київ : Нац. акад. внутр. справ, 2023. С. 19–25.

ЗНАЧЕННЯ OSINT-ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

Третяк Софія Вікторівна

курсантка 2-го курсу факультету № 1

Донецького державного університету внутрішніх справ

Квашук Олександр Дмитрович

кандидат юридичних наук,

старший викладач кафедри кримінального процесу та криміналістики
факультету № 1 Донецького державного університету внутрішніх справ

Інтенсивний розвиток технологій у сучасному інформаційному цифровому світі продукує виникнення новітніх методів збирання та обробки інформації про особу та події, одним із яких є OSINT (англ. «Open Source INTelligence»), що активно упродовжується в діяльності урядових та корпоративних інституцій, журналістських розслідуваннях тощо.

У науковій літературі розвідка з відкритих джерел визначається як діяльність, що здійснюється заінтересованим суб'єктом, спрямована на отримання інформації та включає в себе збір, аналіз інформації та формування висновків. Об'єктом OSINT є відкриті джерела або відкрита інформація: від класичних друкованих ЗМІ до електронних реєстрів [1, с. 332]. OSINT надає можливість агрегувати інформацію з різноманітних відкритих джерел, що сприяє виявленню нових деталей, отриманню підтверджень вже відомих фактів та встановленню більш повної картини подій [2, с. 210].

Отже, досліджувана діяльність охоплює дії щодо збору, опрацювання та використання даних з метою задоволення інформаційних потреб суб'єкта розвідувальної діяльності. Як один із базових елементів розвідувального циклу, вона є необхідною для забезпечення повноти та всебічної інформованості суб'єкта під час підготовки та прийняття ним управлінських, стратегічних, тактичних та інших рішень. У контексті розгляду питань використання OSINT, поняття «розвідка» вживається у широкому значенні, що виходить за рамки діяльності суто розвідувальних органів та їх взаємодії з іншими суб'єктами розвідувального співтовариства з метою забезпечення національної безпеки і оборони [3]. Методологія OSINT, адаптована до практичних потреб в інших сферах діяльності, стає цінним інструментом вирішення конкретних завдань, необхідною передумовою якого є збір, аналіз та інтерпретація інформації з відкритих джерел.

OSINT можна розглядати як концепцію, методологію та набір технологічних інструментів, що використовуються для законного отримання та застосування інформації військового, політичного, економічного та іншого характеру з відкритих джерел, необхідної для ухвалення доцільних рішень у сфері національної оборони та безпеки, а також для виконання завдань

різноманітних розслідувань та в інших галузях діяльності. OSINT включає в себе моніторинг, збір первинних даних, їхню реєстрацію (фіксування), аналітичну й синтетичну обробку, можливе подальше поширення на відповідних платформах. Важливими проблемними аспектами етапу обробки є структурування потоку інформації, її верифікація та контекстуалізація, фільтрування інформаційного шуму та дезінформації, забезпечення взаємодії між різними суб'єктами, збереження даних, архівування тощо. Якісно опрацьована первинна інформація, отримана з відкритих джерел, може трансформуватися у практично значуще знання. Залучення достовірної інформації з відкритих джерел сприяє вільному обміну даними, оскільки цей процес, загалом, не передбачає використання таємних методів отримання інформації. За певних умов, якщо ця інформація не належить до категорії відомостей, що не підлягають засекреченню, вона може набути статусу державної таємниці.

Методологія розвідки на основі відкритих джерел успішно використовується як інструмент протидії в умовах кінетичної та гібридної воєн, виявлення фактів протиправної діяльності та грубих порушень прав людини. Якщо раніше аналіз відкритих даних переважно застосовувався для проведення журналістських, маркетингових досліджень, забезпечення безпеки бізнесу тощо, то в умовах війни OSINT трансформувався у важливий елемент виконання завдань протидії військовій агресії та розслідування воєнних злочинів.

Ефективне використання OSINT є дієвим механізмом для відстеження переміщення військової техніки та особового складу противника, розкриття їхніх намірів щодо стратегії і тактики ведення бойових дій. Так, зовнішні сервіси для геолокації є важливим джерелом інформації про території, що зазнали ударів з боку російських окупаційних сил, а перехоплення радіосигналів надає можливість обробляти ворожу комунікацію [4].

Практика правоохоронної діяльності у сучасних умовах йде шляхом адаптування цієї методології для вирішення завдань кримінального провадження. Під час війни OSINT ефективно упроваджується в практику розслідування воєнних злочинів. Об'єкти дослідження мають широкий діапазон інформаційних джерел – від офіційних урядових документів та повідомлень до соціальної інженерії та метаданих. Важливу роль у фіксуванні інформації відіграє контент соціальних мереж. Публікації військовослужбовців держави – агресора та цивільних громадян дозволяють отримати безпосереднє уявлення про реалії війни «з перших вуст». Це, своєю чергою, забезпечує даними щодо місць розташування та характеру дій російських збройних формувань і є одним із інструментів ідентифікації воєнних злочинців.

Фотографії та відеоматеріали, що публікуються в соціальних мережах, можуть містити ключову інформацію, яка уможливило встановлення осіб, їхнє місцезнаходження у певний момент часу, а також з'ясування окремих обставин вчинених ними діянь. Використання геопросторових даних, інтернет – ресурсів, як джерел інформації, дозволяє виявляти осіб, які брали участь у військових діях або були свідками злочинних подій, що

інтенсифікує процес пошуку та ідентифікації винних осіб та притягнення їх до кримінальної відповідальності.

Аналіз інтернет-ресурсів, супутникових знімків, відкритих баз даних та інших джерел, використання штучного інтелекту як інструменту обробки великого обсягу інформації, дозволяє оперативно фіксувати докази злочинів, верифікувати та перехресно підтверджувати інформацію з різних незалежних джерел, підвищуючи її достовірність. Аналіз та огляд фото - та відеоматеріалів, інших цифрових слідів, геопросторових даних, проведені із дотриманням належної процесуальної форми, часто є незамінними у процесі збирання, перевірки та оцінки доказів, які можуть бути використані в національних та міжнародних судових процесах.

Важливе значення під час розслідування воєнних злочинів має інформаційна взаємодія з національними та міжнародними OSINT-спільнотами. З 2019 року українська агенція Molfar, що діє у понад 39 країнах, спеціалізується на приватній розвідці, зокрема ідентифікує російських воєнних злочинців, проводить воєнні розслідування та аналізує воєнну ситуацію. Molfar намагається доносити результати своїх розслідувань до західних медіа та збирає реєстри іноземних пропагандистів, а також українських зрадників і ворогів, документуючи відповідні докази. Крім того, фахівці агенції навчають військовій OSINT-аналітиці представників СБУ, Держприкордонслужби, Міноборони та громадських організацій. Незалежна міжнародна команда Bellingcat, що складається з дослідників, слідчих та громадянських журналістів, з 2014 року використовує відкриті джерела та соціальні мережі для розслідування різноманітних подій, включаючи злочини проти людяності, використання хімічної зброї та конфлікти по всьому світу. У контексті війни в Україні Bellingcat на основі відкритих даних (фото, відео, переговорів) встановила ймовірних винних у збитті літака МН-17 у 2014 році. З початку повномасштабного вторгнення у 2022 році Bellingcat також фіксує випадки руйнувань цивільної інфраструктури та загибелі мирного населення, відображаючи цю інформацію на інтерактивній карті, доступній для дослідження за датою та місцем. Волонтерський проєкт InformNapalm виник у березні 2014 року у відповідь на російську агресію. Організація проводить глибокі дослідження російської збройної агресії проти України, ідентифікує російських військовослужбовців, причетних до гібридних війн в інших країнах, розкриває факти незаконного експорту російської зброї та військової техніки, збирає докази участі російських посадовців у плануванні підривних операцій та воєн на території інших держав, а також спростовує російську пропаганду [5, с. 40-41].

Таким чином, завдяки можливості збору, обробки та аналізу великих обсягів публічно доступної інформації та цифрових слідів, OSINT-технології та існуючі практики їх використання у різних сферах діяльності створюють додаткові можливості документування кримінально протиправних дій. Ефективне впровадження таких практик у правоохоронну діяльність є важливим завданням, виконання якого суттєво підвищує потенціал

розслідування задля достовірного встановлення обставин воєнних злочинів та реального притягнення до кримінальної відповідальності винних осіб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії the concept of OSINT and related categories. Юридичний науковий електронний журнал. 2024. № 9, С. 332-335. URL: http://lsej.org.ua/9_2024/80.pdf.
2. Калугін В., Сіфоров О. Використання OSINT у встановленні фактів воєнних злочинів та особи воєнних злочинців. Воєнний стан: теоретико-праксеологічні проблеми юриспруденції. 2024. С. 202-225. URL: <http://catalog.liha-pres.eu/index.php/liha-pres/catalog/view/329/9688/21916-1>
3. Про розвідку: Закон України від 17 вересня 2020 року № 912-IX. // Урядовий кур'єр. – 2020. – № 214. – URL: <https://zakon.rada.gov.ua/laws/show/912-20#n442> (дата звернення: 15.05.2025).
4. Ярошенко О. Коли журналістика знаходить союзника в OSINT. European Journalism Observatory. URL: https://ua.ejo-online.eu/8842/uncategorized/zhurnalistyka-znakhodyt-soiuznyka_osint (дата звернення: 16.05.2025).
5. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. №1(25), С. 19–50. URL: <https://doi.org/10.28925/2663-4023.2024.25.1950>.

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Трошев Андрій Дмитрович

курсант 202 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС

Свинаренко Юрій Павлович

доктор філософії, завідувач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Досить довгий час Україна перебуває в умовах тривалої гібридної війни, у якій кіберпростір став одним з головних театрів бойових дій. Атаки на енергетичну інфраструктуру, банківські системи, державні реєстри та військові бази стали не поодинокими інцидентами, а регулярним інструментом тиску та

дестабілізації. З огляду на це, посилення кібербезпеки й удосконалення методів кримінального аналізу стали не лише стратегічною потребою, а й елементом щоденної боротьби за безпеку громадян і стійкість державних інституцій.

Паралельно із зовнішніми загрозами зростає і внутрішня кіберзлочинність, що проявляється у формі фішингових атак, фінансових махінацій, розповсюдження шкідливого програмного забезпечення, атак із використанням штучного інтелекту. Технологічний розвиток, зокрема розширення мереж 5G, використання IoT та біометричних систем, лише ускладнює завдання правоохоронних органів. Саме тому питання розвитку кримінального аналізу як інструменту оперативного реагування, виявлення патернів злочинної поведінки та превенції кіберзагроз є вкрай актуальним.

Упродовж останніх п'яти років Україна зробила суттєвий прогрес у сфері кіберзахисту. У 2021 році було ухвалено Стратегію кібербезпеки України, яка передбачала створення єдиної національної системи кіберзахисту, розвиток спроможностей СБУ, Держспецз'язку, Кіберполіції та Збройних Сил у цьому напрямі. Проте виклики, з якими країна стикається у 2025 році, вимагають глибшої трансформації інструментів кримінального аналізу та інтеграції їх у кіберпростір [4, с. 81].

Одним із прикладів ефективного реагування на загрози стало створення в 2023 році Об'єднаного центру оперативного реагування на кіберінциденти при РНБО України. Центр функціонує у форматі міжвідомчої платформи, куди входять аналітики з СБУ, Держспецз'язку, Кіберполіції, ЗСУ та представники приватного ІТ-сектору. В основі його роботи лежить постійний моніторинг, швидкий обмін інформацією, а також застосування технологій кримінального аналізу, таких як big data analytics, машинне навчання та автоматизовані системи розпізнавання ризиків.

Кримінальний аналіз у сучасному розумінні перестав бути виключно методологією для традиційного розслідування. Нині це міждисциплінарна система, що поєднує кримінологію, інформатику, соціальну психологію, кібернетику та інформаційну безпеку. У 2024 році в рамках спільного проєкту МВС та міжнародної організації EUAM Ukraine було запроваджено програму підготовки кримінальних аналітиків нового покоління, які вміють працювати не лише з класичними доказами, а й із цифровими слідами злочинців: метаданими, IP-трафіком, логами серверів, записами з камер відеоспостереження, поведінковими моделями у соціальних мережах [1, с. 59].

У 2025 році важливим досягненням стало впровадження національної платформи «КіберЩит», яка функціонує як база обміну даними між державними органами та бізнесом. Ця система дозволяє інтегрувати результати кримінального аналізу з реальним станом кібербезпеки у режимі реального часу. «КіберЩит» не лише виявляє атаки, а й самостійно корелює їх із попередніми інцидентами, виявляє закономірності, прогнозує подальшу активність зловмисників, що дозволяє оперативно вживати контрзаходів.

Суттєвий вплив на якість кримінального аналізу має використання

штучного інтелекту (ШІ). З 2023 року Кіберполіція активно використовує систему «Аналітик+», створену в партнерстві з українськими ІТ-компаніями. Вона дозволяє на основі алгоритмів глибинного навчання автоматично визначати можливі цілі кібератак, профілі потенційних злочинців, а також будувати карту ризиків для окремих секторів – енергетики, банківської системи, телекомунікацій [3, с. 10].

Проте незважаючи на успіхи, існує низка проблем. Передусім - нестача кваліфікованих кадрів, особливо в регіонах. Більшість висококласних спеціалістів зосереджені в Києві та великих містах. Навчальні програми університетів часто відстають від темпів технологічного прогресу. Необхідною є модернізація вищої юридичної та технічної освіти з урахуванням тенденцій кримінального аналізу та кібербезпеки.

Крім того, потребує вдосконалення законодавча база. Деякі норми Кримінального кодексу України та процесуального законодавства не враховують новітні види цифрових доказів, що ускладнює їхню фіксацію, зберігання та використання в суді. Наприклад, немає чіткого визначення правового статусу даних, зібраних системами ШІ, що створює загрози для прав людини й утруднює судову практику [6, с. 9].

Також викликає занепокоєння недостатня координація між державними структурами. Попри формальну взаємодію, часто спостерігається дублювання функцій, конфлікти інтересів та недостатній рівень обміну інформацією. В умовах високої динаміки загроз така роз'єднаність знижує ефективність реагування.

Певну роль у покращенні ситуації може відіграти активніше залучення громадянського суспільства та бізнесу. Зокрема, компанії з фінансового сектору (банки, фінтех-стартапи) дедалі частіше створюють власні центри моніторингу загроз, які можуть стати частиною національної системи кіберзахисту. Такі приклади вже демонструють Monobank, NovaPay та інші технологічні гравці.

Цікавим трендом 2025 року стало також використання OSINT (open-source intelligence) у кримінальному аналізі. Аналітики активно використовують відкриті джерела -форуми даркнету, Telegram-канали, ресурси для обміну шкідливими скриптами, платформу GitHub. Такі методи дозволяють на ранніх стадіях виявляти координацію дій злочинців, зокрема в межах організованих груп, що працюють проти інфраструктури України [5, с. 327].

Перспективним напрямом також є розвиток міжнародного співробітництва. Україна у 2025 році активно інтегрується до європейської системи кіберзахисту, зокрема через участь у платформі Cyber Rapid Response Teams (CRRTs) та спільних ініціативах з INTERPOL, EUROPOL і NATO CCDCOE. Це дозволяє швидко реагувати на інциденти, що мають транскордонний характер, а також використовувати напрацювання інших країн для вдосконалення власної моделі безпеки [2, с. 60].

Розвиток кримінального аналізу та кібербезпеки в Україні у 2025 році є процесом, що перебуває у стані активного становлення та глибокої

трансформації. Попри значні виклики -зовнішні та внутрішні -держава демонструє прогрес у створенні інституційної, технологічної та освітньої бази для ефективної протидії кіберзлочинності. Кримінальний аналіз поступово еволюціонує від традиційної роботи зі статистикою до комплексного цифрового інструмента, здатного прогнозувати та упереджувати кіберінциденти.

Для забезпечення стійкості кіберпростору України у майбутньому необхідно зосередити зусилля на кількох напрямках: посилення міжвідомчої взаємодії, оновлення освітніх програм, удосконалення законодавства з урахуванням цифрової специфіки доказів, активне впровадження ШІ та big data в аналітичну діяльність, залучення бізнесу та громадян до спільної боротьби з кіберзагрозами. Також важливо забезпечити прозорість і дотримання прав людини під час роботи із цифровими даними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України [Текст] : матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.) / [редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук]. Київ : Нац. акад. внутр. справ, 2022. 333 с.
2. Баранов О. А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. 2014. № 2 (42). С. 54–62
3. Бортник С. М. Перспективи розвитку аналітичних систем предикативної аналітики. Застосування інформаційних технологій у діяльності правоохоронних органів : матеріали круглого столу (м. Харків, 14 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. С. 9–11.
4. Основи кримінального аналізу : підручник / А. М. Бабенко, О. М. Заєць, В. А. Некрасов та ін. ; за заг. ред. О. Є. Користіна. Одеса, 2019. 296 с.
5. Узлов Д. Ю., Струков В. М., Власов О. В. Використання інтелектуального аналізу даних у протидії інформаційній злочинності // Актуальні питання протидії кіберзлочинності та торгівлі людьми : матеріали Всеукр. наук.-практ. конф. (м. Харків, 23 листопада 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. С. 325–328.
6. Швець Д. В. Стратегічні напрямки використання новітніх технологій цифрового світу у попередженні злочинів. Застосування інформаційних технологій у діяльності правоохоронних органів : матеріали круглого столу (м. Харків, 14 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. С. 7–9.

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ УКРАЇНИ

Федорошевська Анна Валеріївна

курсантка 201 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС

Науковий керівник:

Свинаренко Ю. П.

доктор філософії, завідувач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Актуальність дослідження розвитку кримінального аналізу та кібербезпеки в Україні зумовлена динамічними змінами у сфері національної безпеки, стрімким технологічним прогресом та еволюцією державної політики у відповідь на нові виклики. В умовах сучасного інформаційного суспільства, що характеризується екстенсивним використанням мережі інтернет, соціальних медіа та зростаючою залежністю суспільства від інформаційних систем, питання протидії злочинності як у традиційному, так і в кібернетичному просторі набуває особливої гостроти. Розвиток та ефективне функціонування кримінального аналізу та кібербезпеки стають не просто важливими, а й невід'ємними складовими діяльності правоохоронних органів, спрямованими на забезпечення стабільності, захисту прав і свобод громадян та національних інтересів держави.

Першими на теренах України визнали необхідність виділення кримінального аналізу в окремий напрямок представники Державної прикордонної служби України, котрі завдяки наказу ДПСУ № 28 від 15 січня 2008 р. отримали Інструкцію про організації [1].

З 2016 року, коли в Національній поліції започаткували кримінальний аналіз, злочинність вже активно використовувала сучасні технології, що зумовило необхідність для поліції у пошуку ефективного системного рішення. Одним із кроків у цьому напрямку стало створення відділу кримінального аналізу, який спочатку складався лише з п'яти аналітиків, без планів на повноцінний підрозділ. Однак вже у 2017 році було створено самостійний підрозділ кримінального аналізу у складі кримінальної поліції, що сприяло більш ефективному впровадженню новітніх підходів у роботі та розкритті злочинів. У 2019 році відбулася переоцінка накопиченого досвіду та було створено перші п'ять територіальних підрозділів кримінального аналізу [2].

З початку 2020-х років Україна вступила в епоху інтенсивної цифровізації, яка співпала з розгортанням збройного конфлікту. Ці складні

умови стали каталізатором для якісно нового етапу розвитку кримінального аналізу. На озброєння правоохоронних органів активно впроваджуються передові методи обробки великих обсягів даних (Big Data), що дозволяє виявляти закономірності та зв'язки, раніше непомітні при традиційному аналізі. Широке застосування знаходить відеоаналітика, яка допомагає в ідентифікації осіб та подій, а також технології штучного інтелекту, здатні автоматизувати рутинні аналітичні завдання та прогнозувати потенційні загрози. Соціальні мережі стають важливим джерелом інформації для аналізу суспільних настроїв та виявлення протиправної діяльності. У відповідь на нові виклики створюються сучасні аналітичні центри не лише в Національній поліції, але й у Національній гвардії та Державній прикордонній службі. Основною метою цих центрів є ефективна боротьба з організованою злочинністю, своєчасне виявлення та попередження терористичних загроз, а також протидія різноманітним формам нелегальної діяльності, особливо тим, що пов'язані з умовами воєнного стану.

Паралельно з розвитком кримінального аналізу, великі зміни переживає і кібербезпека України. До 2014 року увага до кіберзагроз була обмеженою, а захист цифрової інфраструктури був малоефективним та слабким. Початок російської агресії змінив підхід держави до кібербезпеки. Саме з 2014 року відбувається становлення системної політики кібербезпеки: створюються спеціальні структури, активізується співпраця з НАТО, ЄС, США, запускається робота національних центрів реагування на кіберінциденти.

У 2016 році Україна заклала основи системного підходу до захисту свого кіберпростору, ухваливши першу Стратегію кібербезпеки [3]. Цей стратегічний крок став своєчасною відповіддю на зростаючі загрози у цифровому середовищі. Згодом, у 2018 році, для практичної реалізації положень стратегії та оперативного реагування на інциденти, розпочав свою роботу Державний центр кіберзахисту при Державній службі спеціального зв'язку та захисту інформації України (Держспецзв'язку) [4]. На жаль, після цих важливих кроків, Україна неодноразово стикалася з масштабними кібератаками, які стали серйозним викликом для національної безпеки. Ці події стали потужним стимулом для держави до подальшого посилення заходів кіберзахисту, приділяючи особливу увагу захисту об'єктів критичної інфраструктури, стабільне функціонування яких є життєво важливим для країни.

З 2022 року, після початку повномасштабного вторгнення РФ, кібербезпека набула стратегічного значення. Масові атаки на державні портали, банківський сектор, енергетику стали щоденною реальністю. У відповідь створено кібервійська, мобілізовано IT-волонтерів (так звана IT-армія), налагоджено координацію з провідними світовими технологічними компаніями. Україна успішно захищає свої цифрові кордони завдяки новим підходам, зокрема хмарним технологіям, інструментам моніторингу та автоматизованим системам захисту [5].

Отже, як кримінальний аналіз, так і кібербезпека в Україні пройшли

шлях від фрагментарного, слаборозвиненого стану до потужних напрямів діяльності, які визначають ефективність системи безпеки держави.

У найближчі роки кримінальний аналіз та кібербезпека залишатимуться пріоритетними напрямками у сфері національної безпеки України. З огляду на сучасні виклики, ці галузі мають значний потенціал для подальшого розвитку, що визначається як внутрішніми потребами держави, так і міжнародними зобов'язаннями України у сфері безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Львівський державний університет внутрішніх справ. Основи Кримінального аналізу. Навчальний посібник. І. А. Федчак. Львів 2021. ст 15.

2. Матеріали міжвідомчої науково-практичної конференції. “ Розвиток системи кримінального аналізу в діяльності національної поліції України в сучасних умовах” Бутко Роман Юрійович. Київ, 17 листопада 2023 року. ст 19.

3. Верховна рада України. Про стратегію кібербезпеки України. Документ n0003525-16, чинний, поточна редакція — Введення в дію від 18.03.2016, підстава - [96/2016](https://zakon.rada.gov.ua/laws/show/n0003525-16#Text). від 27 січня 2016 року. <https://zakon.rada.gov.ua/laws/show/n0003525-16#Text> (Дата звернення 29 04 2025)

4. Верховна рада України. Про затвердження плану заходів на 2018 рік з реалізації стратегії кібербезпеки України. Документ 481-2018-р, чинний, поточна редакція — Прийняття від 11.07.2018. <https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80#Text> (Дата звернення 29 04 2025)

5. GOV.UA Урядовий портал. “ Кібербезпека під час війни: базові заходи з кіберзахисту для українських організацій” 2023р. <https://www.kmu.gov.ua/news/kiberbezpeka-pid-chas-viiny-bazovi-zakhody-z-kiberzakhystu-dlia-ukrainskykh-orhanizatsii> (Дата звернення 29 04 2025)

ВИКОРИСТАННЯ МЕТОДІВ OSINT З МЕТОЮ РЕАЛІЗАЦІЇ ЗАВДАНЬ СИСТЕМИ API/PNR

Фігура Віталій Олегович

ад'юнкт відділення ад'юнктури і докторантури
Національної академії Державної прикордонної
служби України
Науковий керівник

Філіппов Станіслав Олександрович

доктор юридичних наук, професор,
заступник начальника факультету правоохоронної діяльності
Національної академії Державної прикордонної служби України,
orcid 0000-0001-6700-4194

Перспективним і в той же час актуальним є питання використання розвідки на основі відкритих джерел інформації (Open source intelligence, далі

- OSINT), як одного з додаткових, дієвих елементів в ході функціонування системи API/PNR в Україні.

OSINT – являє собою метод збору, обробки та аналізу інформації з загальнодоступних, відкритих джерел таких, як: веб-сайти, соціальні мережі, наявні бази даних, форуми, медіа та багато інших. Окрім того, що ефективність використання OSINT доведена в ході фіксування воєнних злочинів, які скоєні країною агресором (рф) упродовж війни, області його застосування є надзвичайно різноманітними. Для прикладу основними з них можна назвати такі:

безпекова - використовується правоохоронними органами, спеціальними службами з метою збору інформації щодо потенційних загроз у різних сферах (до прикладу, терористичних дій злочинців, прогнозування потенційних конфліктів, а також аналізу загроз кібербезпеці);

корпоративна безпека - застосовується для відстеження конкурентів, аналізу ринку та виявлення потенційних загроз у сфері бізнесу;

аналіз соціальних мереж - надає можливість використовувати дані щодо активності у соціальних мережах, аналізувати громадську думку та виявляти ботів;

кібербезпека дозволяє виявляти кіберзагрози, моніторить та аналізує різні інтернет-джерела, виявляє слабкі місця у кіберзахисті;

розслідування кримінальних правопорушень – отримувати докази з відкритих джерел.

Загалом, OSINT це надзвичайно потужний інструмент, який може застосовуватися для різноманітних цілей і завдань його повноцінне використання під час функціонування системи API/PNR в Україні на нашу думку, лише питання часу.

OSINT, відповідно до світової практики є одним з інструментів забезпечення Integrated Border Management – IBM, а також застосовується для ухвалення рішень у сфері авіаційної безпеки. Його роль у цьому полягає у доповненні закритих джерел інформації (баз даних Інтерполу; Schengen Information System - SIS та національних баз) відкритими даними з метою поглибленої оцінки ризиків.

Нами пропонується розглянути застосування OSINT в контексті забезпечення прикордонної безпеки у тісному поєднанні з системою API/PNR, яка в майбутньому буде запроваджена в Україні.

Так, у ході отримання будь якої інформації відносно пасажирів авіарейсів виникає необхідність їх додаткової перевірки за допомогою OSINT. Для цього можуть бути використані наступні етапи:

підготовчий - визначає цілі та окреслює джерела і шляхи пошуку вагомої інформації;

накопичуваний - в ході даного етапу проводиться первинний збір різного роду даних, які отримуються з усіх джерел інформації;

опрацювання - отримані дані уточнюються, перевіряються та

готуються для подальшого проведення аналізу;

аналіз та обробка – здійснюється аналіз отриманої інформації з метою виявлення тенденцій і формування висновків, готується звіт та надаються пропозиції щодо подальших кроків.

Відповідно до результатів отриманих даних з OSINT, а також в контексті забезпечення прикордонної безпеки під час функціонування системи API/PNR, уповноваженими особами прийматимуться рішення щодо:

проведення додаткової перевірки пасажирів авіарейсів та здійснення попереднього аналізу;

затримання, за наявності визначених законом підстав, даних осіб;

прийняття рішень щодо відмов у перетині державного кордону України;

внесення даних щодо потенційно небезпечних осіб до баз даних.

Надзвичайно важливим також є питання збереження персональних даних у ході реалізації завдань системи API/PNR. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108 РЄ), 28 січня 1981 р., - перший міжнародний правовий документ, спрямований безпосередньо і винятково на врегулювання питань захисту персональних даних [1]. Зокрема, як зазначає О. Торбас, Конвенція 108 РЄ визначає основоположні, або так звані «рамкові», засади, щодо обов'язків осіб, які збирають, опрацьовують, використовують персональні дані, зокрема у зв'язку з передачею персональних даних на міждержавному рівні (транскордонного обміну) [2, с.27]. У цьому контексті доцільно звернути увагу на мінімальні етико-правові стандарти використання відкритих даних для проведення ефективних розслідувань, сформульовані у Протоколі Берклі [3].

Загальний регламент про захист даних (GDPR) встановлює конкретні гарантії збереження конфіденційності. Зокрема, відповідно до принципів опрацювання персональних даних, які передбачені ст. 5 Регламенту, персональні дані слід: – опрацьовувати у законний, правомірний і прозорий спосіб щодо суб'єкта даних («законність, правомірність і прозорість»); – збирати для визначених, чітких і законних цілей і в подальшому не опрацьовувати у спосіб, що є несумісним з такими цілями; подальше опрацювання для досягнення цілей архівування у суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей не можна вважати, згідно зі статтею 89 (1), несумісним з первинними цілями («цільове обмеження»); – вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання («мінімізація даних»); – зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього ідентифікування персональні дані можна зберігати протягом більш тривалих періодів, доки їх опрацьовують винятково для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей відповідно до статті 89 (1) за умов вжиття відповідних технічних і організаційних заходів, передбачених цим

Регламентом для гарантування прав і свобод суб'єкта даних («обмеження зберігання»); – опрацьовувати в спосіб, що забезпечує належну безпеку персональних даних, у тому числі захист проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів («цілісність і конфіденційність»).

Таким чином, правомірною, на наш погляд, є постановка питання про застосування інструментів OSINT з метою реалізації завдань системи API/PNR. Дані інструменти можуть використовуватися як додаткові елементи забезпечення ефективності системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція № 108 Ради Європи від 28 січня 1981 року. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 10.05.2025).
2. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса : Видавництво «Юридика». 2024. С. 180.
3. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf> (дата звернення: 10.05.2025).

ВИКОНАННЯ ОБОВ'ЯЗКУ ЩОДО ЗАХИСТУ ВІТЧИЗНИ, НЕЗАЛЕЖНОСТІ ТА ТЕРИТОРІАЛЬНОЇ ЦІЛІСНОСТІ УКРАЇНИ ЯК ОБСТАВИНА, ЩО ВИКЛЮЧАЄ КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ

Флоренко Ганна Олександрівна,
Студентка 2 курсу 3 групи
інституту права та безпеки
Науковий керівник:
Резніченко Г.С.
к.ю.н., доцент, доцент кафедри
кримінально-правових дисциплін
ОДУВС

Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України як обставини, що виключає кримінальну відповідальність, зумовлена сучасними військово-політичними викликами, збройною агресією проти України та необхідністю правового врегулювання дій громадян, які беруть участь у захисті держави. В умовах війни важливо чітко визначити межі правомірного застосування сили, зокрема

військовослужбовцями, добровольцями та іншими особами, які виконують конституційний обов'язок щодо оборони країни. Це сприяє зміцненню правопорядку, захисту прав захисників та формуванню справедливого правосуддя, що відповідає нормам міжнародного гуманітарного права.

В умовах триваючої збройної агресії російської федерації проти України, захист прав громадян, включаючи їхні основоположні права на життя, здоров'я, честь, гідність та власність, набуває особливої актуальності. Для забезпечення ефективного захисту цих прав, а також для регулювання порядку несення військової служби, 15 березня 2022 року Верховна Рада України прийняла Закон України «Про внесення змін до Кримінального кодексу України та інших законодавчих актів України щодо визначення обставин, що виключають кримінальну протиправність діяння та забезпечують бойовий імунітет в умовах дії воєнного стану». Цей закон вніс зміни до Кримінального кодексу України, зокрема, доповнивши його статтею 43-1, яка визначає обставини, що виключають кримінальну протиправність діяння в умовах воєнного стану. [3]

Згідно з частиною першою статті 43-1 Кримінального кодексу України, дії, вчинені в умовах воєнного стану або збройного конфлікту з метою відсічі агресії російської федерації чи іншої країни, не вважаються кримінальними правопорушеннями, якщо вони завдали шкоди життю чи здоров'ю агресора або правоохоронюваним інтересам. Проте, це правило не діє у випадках катувань, застосування заборонених міжнародним правом засобів ведення війни або інших порушень законів і звичаїв війни, визначених міжнародними договорами, ратифікованими Верховною Радою України. [1]

Прейс Є.В., зазначає, що аналіз статті 43-1 Кримінального кодексу України виявляє, що вона охоплює два типи ситуацій, які не є взаємовиключними, а можуть поєднуватися в одному діянні. Обидва типи мають спільні характеристики: діяння має відбуватися в умовах воєнного стану або збройного конфлікту, спричиненого агресією іншої держави; воно повинно бути спрямоване на відсіч або стримування цієї агресії; та воно не повинно містити ознак катувань, використання заборонених міжнародним правом засобів війни або інших порушень законів і звичаїв війни, визначених міжнародними договорами, ратифікованими Верховною Радою України. [4, с. 531]

Шармар О.М., аналізуючи статтю 43-1 Кримінального кодексу України закріплює, що захист Вітчизни як право та обов'язок особи. Поняття «бойового імунітету», що включає формулювання «неможливо було передбачити», вказує на відсутність необережної вини. Відсутність вини, своєю чергою, виключає склад кримінального правопорушення та підстави для кримінальної відповідальності. [6, с. 32]

Закон України «Про оборону України» доповнено визначенням «бойового імунітету», що звільняє військово командування, військовослужбовців, добровольців територіальної оборони, правоохоронців та інших осіб, які беруть участь в обороні України, від відповідальності за

втрати особового складу, техніки та наслідки застосування зброї, якщо ці наслідки неможливо було передбачити або вони охоплюються виправданим ризиком. Виняток становлять випадки порушення законів війни та міжнародних договорів.[2]

Особа не несе відповідальності за застосування зброї, бойових припасів або вибухових речовин проти агресора, а також за пошкодження або знищення майна, пов'язані з цими діями, якщо вони були вчинені в умовах воєнного стану і спрямовані на відсіч агресії. Важливо розуміти, що надання таких прав, тісно пов'язане з дотриманням міжнародних норм. Навіть заповдіання шкоди правоохоронюваним інтересам не вважається кримінальним правопорушенням, якщо це сталося в процесі відсічі агресії в умовах воєнного стану. Таким чином, законодавець намагається створити правові умови для ефективного захисту України від збройної агресії, забезпечуючи захисникам певний ступінь правового захисту, але при цьому наголошуючи на необхідності дотримання міжнародних норм і правил.[5, с. 3]

В умовах триваючої збройної агресії проти України питання правового врегулювання дій військовослужбовців, добровольців та інших осіб, які виконують свій конституційний обов'язок щодо захисту держави, набуває особливої актуальності. Законодавчі зміни, зокрема прийняття статті 43-1 Кримінального кодексу України, спрямовані на врегулювання обставин, що виключають кримінальну відповідальність за дії, вчинені в умовах воєнного стану, якщо вони були спрямовані на відсіч агресії. Це дозволяє забезпечити ефективний захист України та її громадян, а також надає військовослужбовцям необхідний бойовий імунітет.

Однак, бойовий імунітет не є абсолютним і не звільняє від відповідальності за порушення законів і звичаїв війни, катування або застосування заборонених міжнародним правом методів ведення війни. Це свідчить про прагнення законодавця забезпечити баланс між захистом військовослужбовців та дотриманням міжнародних норм. Важливо, що законодавство визнає дії, спрямовані на захист країни, такими, що не містять складу кримінального правопорушення, якщо вони здійснені в межах виправданого ризику і без умислу на вчинення воєнних злочинів.

Запровадження правових механізмів бойового імунітету є важливим кроком для зміцнення обороноздатності України. Це сприяє захисту військовослужбовців від необґрунтованого переслідування, що дозволяє їм виконувати бойові завдання без остраху за можливі юридичні наслідки, якщо їхні дії відповідали встановленим нормам. Водночас, законодавство залишає простір для правового контролю, запобігаючи безкарності у випадках порушень міжнародного гуманітарного права.

Таким чином, українське законодавство намагається забезпечити правовий захист осіб, які беруть участь у захисті країни, водночас встановлюючи чіткі межі застосування сили та наголошуючи на необхідності дотримання міжнародних норм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний кодекс України : Закон України від 05 квітня 2001 р. № 2341-III. URL : <https://zakon.rada.gov.ua/laws/show/2341-14> find=1&text=колабор#w1_1 (дата звернення: 12).
2. Про оборону України : Закон України від 6 грудня 1991 року № 1932-XII. URL : <https://zakon.rada.gov.ua/laws/show/1932-12#n138>
3. Про внесення змін до Кримінального кодексу України та інших законодавчих актів України щодо визначення обставин, що виключають кримінальну протиправність діяння та забезпечують бойовий імунітет в умовах дії воєнного стану : Закон України від 15.03.2022 року № 2124-IX. URL: <https://zakon.rada.gov.ua/laws/show/2124-20>
4. Прейс Є.В. Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, як новелла українського законодавства. *Юридичний науковий електронний журнал*. 2023. №4. С. 520-532.
5. Ковальчук О.Ю., Острогляд О.В. Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, як обставина, що виключає кримінальну протиправність діяння. 2023. №2. С. 4
6. Шрамар О.М. Виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, як обставина, що виключає кримінальну протиправність діяння. *Вісник Асоціації кримінального права України*. 2022. № 1(17). С. 24-35.

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗАГРОЗАМ: АНАЛІЗ ТА ПЕРСПЕКТИВИ

Форос Ганна Володимирівна

кандидат юридичних наук, доцент
завідувачка кафедри кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ

У сучасному цифровому світі кіберпростір став невід'ємною частиною життєдіяльності держав, бізнесу та окремих громадян. Водночас зростання залежності від інформаційних технологій призвело до появи нових і складних кіберзагроз, які мають транснаціональний характер і становлять серйозну небезпеку для національної безпеки, економічної стабільності та суспільного добробуту. У цьому контексті вивчення та адаптація міжнародного досвіду у сфері протидії кіберзагрозам є надзвичайно актуальним завданням.

Багато країн прийняли комплексні національні стратегії кібербезпеки, які визначають цілі, пріоритети та основні напрями діяльності у цій сфері. Наприклад, стратегії США, Великої Британії, Німеччини та Естонії передбачають посилення кіберзахисту критичної інфраструктури, розвиток національних кіберсил, підвищення рівня кібергігієни населення та активну міжнародну співпрацю.

Дослідження в сфері міжнародного нормативно-правового забезпечення кібербезпеки фокусуються на регуляторних підходах, ефективних механізмах співпраці та стандартизації для протидії кіберзагрозам.

Різні країни світу розробляють та впроваджують власні стратегії та механізми для боротьби з кіберзагрозами. Аналіз їхнього досвіду дозволяє виділити кілька ключових підходів:

створення спеціалізованих державних органів. Так, для координації зусиль у сфері кібербезпеки багато країн створили спеціалізовані державні органи, такі як національні центри кібербезпеки (наприклад, NCSC у Великій Британії, BSI у Німеччині) або агентства з кібербезпеки (наприклад, CISA у США). Ці органи відповідають за моніторинг кіберзагроз, реагування на інциденти, розробку стандартів та рекомендацій, а також за співпрацю з приватним сектором та міжнародними партнерами;

- удосконалення нормативно-правового регулювання. Нормативно-правове регулювання кібербезпеки є ключовим елементом захисту держав і суспільства від кіберзагроз. Воно включає систему правових актів, стандартів та інструкцій, спрямованих на попередження, виявлення та протидію кіберзлочинам і кіберінцидентам. Становлення законодавчого забезпечення у цій сфері має особливе значення, оскільки дозволяє формувати правові основи для діяльності суб'єктів, відповідальних за кібербезпеку, а також забезпечувати належний рівень захисту інформаційних ресурсів та персональних даних громадян [1, с. 151]. Багато країн активно працюють над удосконаленням свого законодавства у сфері кібербезпеки, криміналізуючи нові види кіберзлочинів, встановлюючи відповідальність за їх вчинення та визначаючи процедури розслідування та судового переслідування. Важливу роль у цьому контексті відіграє Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), яка є основним міжнародним інструментом у цій сфері. Інші міжнародні документи, такі як резолюції ООН, Рекомендації Міжнародного союзу електрозв'язку (ITU) та Політика кібербезпеки Європейського Союзу, формують додаткові рамки та стандарти для забезпечення кібербезпеки. Вони не мають такої юридичної сили, як конвенції, але встановлюють орієнтири для національних урядів у формуванні власної політики у сфері кібербезпеки [2, с. 490];

розвиток державно-приватного партнерства. Кібербезпека є спільним завданням держави та приватного сектору. У багатьох країнах налагоджено ефективні механізми державно-приватного партнерства, які передбачають

обмін інформацією про кіберзагрози, спільне проведення навчань та тренувань, а також розробку спільних стандартів та рекомендацій;

міжнародна співпраця. Враховуючи транснаціональний характер кіберзагроз, міжнародна співпраця є критично важливим елементом ефективної протидії. Країни активно співпрацюють на двосторонній та багатосторонній основі, обмінюючись інформацією, проводячи спільні операції, розробляючи міжнародні стандарти та беручи участь у діяльності міжнародних організацій.

Попри досягнення в галузі міжнародної співпраці, існує чимало викликів. Один із основних викликів полягає у різниці правових систем і підходів до кібербезпеки у різних країнах. Також важливим викликом є питання конфіденційності і дотримання прав людини, що може суперечити потребам держав у сфері національної безпеки.

Інший виклик полягає в розбіжностях у технологічному розвитку країн, які впливають на їхню здатність реагувати на кіберзагрози. Країни з обмеженими ресурсами можуть потребувати технічної допомоги, щоб забезпечити належний рівень кібербезпеки.

Міжнародне регулювання кібербезпеки стикається з численними викликами через швидкий розвиток кіберзагроз, різницю в правових системах, політичних інтересах та економічних можливостях держав. Відсутність універсальних стандартів і правових норм, що ускладнює співпрацю між країнами, а також прагнення деяких держав захищати цифрові кордони, як фізичні, посилює труднощі у сфері. Важливим викликом є протидія кіберзлочинності та захист критичної інфраструктури, що вимагають скоординованих зусиль і правової взаємодії між країнами. Наприклад, зусилля Ради Європи через Конвенцію про кіберзлочинність спрямовані на правову співпрацю в боротьбі з кіберзлочинністю.

Щодо перспектив міжнародної співпраці в сфері протидії кіберзагрозам вимагає поглиблення міжнародної співпраці за такими напрямками:

- гармонізація законодавства, яке полягає в зближенні національних законодавств у сфері кібербезпеки з метою полегшення розслідування та розкриття кіберзлочинів на міжнародному рівні;

- розширення обміну інформацією або створення ефективних механізмів обміну оперативною інформацією про кіберзагрози між країнами;

- координація зусиль у сфері розробки нових технологій та методів захисту від кіберзагроз;

- надання технічної допомоги та обміну досвідом з країнами, які мають обмежені ресурси у сфері кібербезпеки;

- посилення ролі ООН, Ради Європи, ОБСЄ та інших міжнародних організацій у координації міжнародних зусиль у сфері кібербезпеки.

Перспективи розвитку міжнародного співробітництва також включають створення глобальних стандартів, таких як Директива NIS2 Європейського Союзу, що охоплюють технічні, регуляторні та юридичні

аспекти кібербезпеки. Важливим напрямком є кібердипломатія, де міжнародні ініціативи ООН спрямовані на досягнення принципів поведінки держав у кіберпросторі для забезпечення стабільності.

Таким чином, можна стверджувати, що ця сфера є однією з ключових у сучасному глобалізованому світі, де кіберзагрози набувають дедалі складніших форм та масштабів. Міжнародна спільнота вже має значні досягнення у боротьбі з кіберзагрозами, але необхідність ефективнішої гармонізації законодавства, розробки універсальних стандартів та посилення співпраці між країнами й надалі залишається актуальною. Ключовими аспектами, що потребують подальшої уваги, є стандартизація правових норм, розвиток кібердипломатії, захист критичної інфраструктури та посилення ролі міжнародних організацій у протидії кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Горулько В. Значення правового регулювання у забезпеченні кібербезпеки в умовах війни: досвід для України. Вісник Харківського національного університету імені В. Н. Каразіна. Сер.: Право. 2024. №37. С. 150–155. DOI: <https://doi.org/10.26565/2075-1834-2024-37-17>.
2. Сливка М. М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. Юридичний науковий електронний журнал. 2022. Вип. 10. С. 489–491.
3. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. Науковий вісник Національної академії внутрішніх справ. 2020. № 4. С. 119–124.

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT

Хомік Софія Василівна

курсант 209 взводу факультету підготовки фахівців для органів досудового розслідування Національної поліції України ОДУВС

Науковий керівник:

Тригуб С. М.

доктор філософії, викладач кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців підрозділів кримінальної поліції Національної поліції України ОДУВС

У сучасному світі, де інформаційні технології прискорено розвиваються, з'являються нові методи збору та аналізу даних, які створюють багато можливостей для отримання знань. Одним з таких методів є OSINT (Open Source Intelligence), який використовує відкриті джерела для збору

інформації. Завдяки легкому доступу до величезної кількості інформації в інтернеті, індивіди та організації можуть використовувати OSINT для виявлення особистої інформації про людей без їхньої згоди і відому.

Це відкриває широкі можливості для зловмисників, які можуть використовувати цю інформацію для шахрайства, маніпуляцій або навіть прямого шантажу. Крім того, використання OSINT утруднює захист особистих даних, оскільки багато інформації публікуються самими користувачами в соціальних мережах, форумах та інших платформах. У зв'язку з цим, визначення меж між необмеженим доступом до інформації та захистом приватності стає ключовим викликом для суспільства, законодавців, і технологічних компаній.

Основна дилема полягає в тому, як забезпечити безпечний простір в Інтернеті, де права осіб на конфіденційність будуть поважатися та захищатися, не обмежуючи при цьому свободу слова та доступ до відкритої інформації, яка може сприяти розвитку знань та інновацій. В цьому контексті виникає необхідність розробки комплексних методологій та інструментарію, що дозволять ідентифікувати та мінімізувати ризики, пов'язані з використанням OSINT, а також розробки ефективних стратегій захисту даних. [1, с. 20] OSINT дозволяє збирати різноманітну інформацію про людей з загальнодоступних джерел, включаючи, але не обмежуючись, іменами, електронними адресами, домашніми адресами та геолокацією. Використання електронних пристроїв, таких як смартфони та фітнес-трекери, а також обмін особистою інформацією через соціальні мережі та інші онлайн-платформи роблять пошук особистої інформації в Інтернеті тривіальним завданням. Це може мати як позитивні, так і негативні наслідки в залежності від того, як така інформація використовується та в якому контексті вона ділиться. Більшість людей, ймовірно, будуть здивовані кількістю інформації про них, яку можна знайти в Інтернеті через загальнодоступні джерела. [1, с. 21]

Однією з переваг розвідки з відкритих джерел, про яку часто забувають, є її універсальність. Її різноманітні програми виходять за рамки традиційних застосувань, таких як правоохоронні органи чи кібербезпека, і включають інноваційні підходи до реагування на стихійні лиха, виявлення шахрайства та управління репутацією в Інтернеті.

Ось декілька цікавих прикладів використання OSINT, які багато людей не беруть до уваги, коли думають про розвідувальні операції: 1) реагування на стихійні лиха - картографування кризових зон; 2) відстеження шахрайства з криптовалютою; 3) протидія дезінформації та фейковим новинам.

Використовуючи інструменти, які аналізують метадані, показники залученості та час публікації, аналітики можуть простежити еволюцію дезінформації та її поширення на різних платформах. OSINT дозволяє аналітикам швидко дискредитувати неправдиві наративи, надаючи фактичну інформацію та контекст, допомагаючи пом'якшити вплив дезінформації та сприяючи більш поінформованому публічному дискурсу.

Управління корпоративною репутацією OSINT дозволяє компаніям виявляти потенційні кризи у сфері зв'язків з громадськістю на ранній стадії, будь то відкликання продукту негативне висвітлення в ЗМІ або вірусні скарги клієнтів. Використовуючи платформи соціальних мереж, сайти з оглядами та новинні агентства, компанії можуть постійно відстежувати настрої громадськості щодо своїх продуктів, послуг та керівництва.

OSINT також дозволяє компаніям аналізувати тенденції в настроях споживачів, що дозволяє їм проактивно адаптувати свої маркетингові стратегії та комунікаційні зусилля. Розуміючи, що клієнти говорять про їхній бренд в Інтернеті, компанії можуть вирішувати проблеми до їх ескалації, тим самим захищаючи свою репутацію. Крім того, OSINT дозволяє бізнесу відстежувати конкурентів, їхні кампанії та громадське сприйняття, що надає цінну інформацію для прийняття стратегічних рішень та допомагає підтримувати конкурентну перевагу на ринку [2].

Також хочу виділити певні пошукові системи, сервіси, веб-ресурси які використовуються в сучасності та зазначити переваги системі OSINT - Shodan. Використовуючи гугл для відповідей на найпростіші життєві питання нереально крута пошукова система Shodan дає можливість хакерам переглядати виставлені активи. Так, сервіс відразу продемонструє вам вибірку результатів, які найповніше в плані сенсу відповідають вашому запиту. Найчастіше користуються системою для пошуку активів, підключених до мережі. Інструмент має відкритий вихідний код, дозволяє провести якісну аналітику з питань безпеки, перевірити вразливі місця конкретної мети (відкритість особистих даних, доступної паролів та портів, IP-адреси тощо). Також Shodan забезпечує найбільш адаптивний пошук спільнот.

Google Doks – це сервіс запущений з 2002 року. Він демонструє чудову продуктивність і є справді інтелектуальним інструментом, що базується на запитах. Сервіс має відкритий вихідний код, допомагаючи користувачам швидко орієнтуватися на результати чи індекс пошуку. [3, с. 14]

Maltego – вудований в Kali Linux ефективний інтелектуальний інструмент від компанії Paterva має відкритий код і призначений для серйозних досліджень цілей за допомогою перетворень. Написаний він мовою програмування Java. Для використання буде потрібна безкоштовна реєстрація на сайті виробника, після чого можна переходити до створення цифрових відбитків вибраної мети в мережі.

Перейдемо до переваг роботи: незважаючи на те, що існують сотні веб-ресурсів для пошуку даних про конкретних людей або юридичних фірм, користувачі ще не знають, як отримувати ексклюзив.

А ще є спеціальні сайти, які призначені для пошуку людей за деякими наданими даними. Достатньо ввести адресу електронної пошти або завантажити фотографію, а може вказати IP – ваш об'єкт знайдено всього за один клік. В одному місці ви отримаєте структуровану та впорядковану

інформацію з численних ресурсів у мережі. Перевіряйте конкретну особу чи цілу корпорацію всього за годину серфінгу в інтернеті. Це дозволить мінімізувати ризики недобросовісного партнерства чи шахрайства у разі.

Ще однією перевагою є унікальність самої системи OSINT. Тут немає шаблонних алгоритмів щодо вашого розслідування, оскільки всі випадки унікальні, тому вимагають індивідуального підходу. OSINT представлений рядом платформ, які дозволяють проводити комплекси дій за пару кліків: пошук та збирання даних, аналітика, дослідження динаміки змін, порівняння результатів за тимчасовий період тощо. Завдяки технології будь-який користувач може зібрати ексклюзивні дані, які добровільно вам ніхто не надасть: це вивчення сторінок, на які підписана шукана особа, і всі його «лайки», коментарі під публікаціями, коло спілкування та соціальні зв'язки. Ви можете перевірити людину на зв'язок та взаємодію з різними людьми, у тому числі блогерами, політиками, чиновниками, медійними персонами, громадськими організаціями, фондами. Такі можливості дозволяють оцінити рівень ризику взаємодії з тією чи іншою фігурою при особистому спілкуванні чи здійсненні серйозної угоди. Також вони допомагають вибрати оптимальну переговорну стратегію з урахуванням переваг, про які дуже легко дізнатися після моніторингу активності майбутнього партнера на форумах та соціальних мережах. OSINT просто необхідний для великих фірм та організацій, які хочуть працювати найбільш продуктивно, прибутково та з мінімальними ризиками витоку цінної комерційної інформації. [3, с. 15]

У ході опрацювання теми «Практичні інструменти та алгоритми використання OSINT» ми дійшли висновку, що розвідка з відкритих джерел — це не просто допоміжний інструмент, а цілісна аналітична система, здатна забезпечити стратегічно важливу інформацію для прийняття рішень у різних сферах. OSINT — це приклад того, як систематизований підхід до аналізу відкритих даних може мати практичну цінність як у сфері безпеки, так і в інформаційній, гуманітарній чи комерційній діяльності. Особливу увагу звернуто на те, що ефективне використання OSINT залежить не лише від знання інструментів, а й від розуміння алгоритмів обробки інформації, критичного мислення та дотримання етичних норм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Главацька А.Л., Ангельська О.В., Опірський І.Р. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. С. 20-21 URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/647/500>

2. 5 Fascinating use cases of open-source intelligence (OSINT). <https://sip-international.com/blog/5-use-cases-osint/>

3. Домчак С. І. Матеріали науково-практичної конференції. Інформаційні технології в освіті та практиці. ЛДУВС. Методика використання OSINT в діяльності кіберполіції. 16 грудня 2022 Р. С. 14-15 URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5241/1/16_12_2022.pdf#page=13

ПРОБЛЕМИ ІМПЛЕМЕНТАЦІЇ БУДАПЕШТСЬКОЇ КОНВЕНЦІЇ В УКРАЇНСЬКЕ ЗАКОНОДАВСТВО

Чорна Марина Василівна

доктор філософії в галузі права,

доцент кафедри державно-правових дисциплін та публічного управління Донецького державного університету внутрішніх справ

Беліков Костянтин Аркадійович

кандидат юридичних наук,

доцент кафедри державно-правових дисциплін та публічного управління Донецького державного університету внутрішніх справ

У сучасному інформаційному суспільстві питання кібербезпеки набувають особливої актуальності. Кіберзлочинність стає транснаціональним явищем, що вимагає координації зусиль міжнародної спільноти. Ключовим міжнародним документом у цій сфері є Конвенція про кіберзлочинність, підписана у Будапешті 23 листопада 2001 року (далі – Будапештська конвенція або Конвенція) [1]. Україна ратифікувала цю Конвенцію 7 вересня 2005 року, і вона набула чинності для нашої держави 1 липня 2006 року [2].

Ратифікація Будапештської конвенції зобов'язала Україну привести національне законодавство у відповідність до міжнародних стандартів боротьби з кіберзлочинністю. Однак, незважаючи на тривалий період імплементації, у вітчизняному законодавстві залишаються проблемні аспекти, які потребують подальшого вдосконалення. Особливої актуальності ці питання набувають у контексті військової агресії проти України, коли кібератаки стають одним із елементів гібридної війни.

Будапештська конвенція є першим і найважливішим міжнародним договором щодо злочинів, вчинених через Інтернет та інші комп'ютерні мережі. Її основними цілями є: гармонізація національного кримінального законодавства у сфері боротьби з кіберзлочинністю; забезпечення ефективних процесуальних інструментів для розслідування кіберзлочинів; налагодження міжнародного співробітництва правоохоронних органів різних держав [3, с. 125].

Конвенція визначає такі категорії кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав [1]. До Будапештської конвенції було прийнято Додатковий протокол щодо криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, який Україна також ратифікувала у 2006 році [4].

Імплементація Будапештської конвенції в українське законодавство здійснювалась поступово. Основними законодавчими актами України у сфері протидії кіберзлочинності є: Кримінальний кодекс України (Розділ XVI «Кримінальні правопорушення у сфері використання електронно-

обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку») [5]; Кримінальний процесуальний кодекс України (зокрема, глава 21 «Негласні слідчі (розшукові) дії») [6]; Закон України «Про основні засади забезпечення кібербезпеки України» [7]; Закон України «Про електронні комунікації» [8]; Закон України «Про національну безпеку України» [9]; Стратегія кібербезпеки України [10].

Також Україна вжила заходів для імплементації положень Конвенції щодо відповідальності за злочини, пов'язані з порушенням авторських і суміжних прав, шахрайством із використанням комп'ютерних технологій та дитячою порнографією [11, с. 170].

Особливо важливим кроком стало прийняття у 2017 році Закону України «Про основні засади забезпечення кібербезпеки України», який встановив правові та організаційні основи забезпечення кібербезпеки України [7]. Проте, незважаючи на позитивні зрушення, залишається низка проблемних аспектів імплементації Будапештської конвенції, які потребують подальшого вирішення.

Незважаючи на те, що в українському кримінальному законодавстві криміналізовано більшість діянь, передбачених Будапештською конвенцією, існують певні розбіжності та прогалини.

По-перше, проблемою є термінологічна неузгодженість. У Кримінальному кодексі України використовується термінологія, що не повністю відповідає термінології Конвенції. Це створює певні труднощі для правозастосовної практики та міжнародного співробітництва [12].

По-друге, існують прогалини в криміналізації окремих діянь. Зокрема, не повністю імплементовано положення ст. 6 Конвенції щодо відповідальності за зловживання пристроями. Українське законодавство передбачає відповідальність за створення та розповсюдження шкідливих програмних і технічних засобів, але не містить чітких положень щодо відповідальності за виготовлення, придбання, імпорт та володіння пристроями, призначеними для вчинення кіберзлочинів, а також за незаконне використання паролів, кодів доступу та інших подібних даних.

По-третє, існують проблеми з імплементацією положень Додаткового протоколу щодо криміналізації дій расистського та ксенофобного характеру. Хоча в українському законодавстві передбачено відповідальність за розпалювання національної, расової чи релігійної ворожнечі (ст. 161 КК України), ці норми не повністю охоплюють випадки поширення таких матеріалів через комп'ютерні системи.

Імплементація положень Будапештської конвенції щодо міжнародного співробітництва також мають низку проблем.

По-перше, існують труднощі з визначенням юрисдикції у справах про кіберзлочини. Транскордонний характер кіберзлочинності призводить до того, що злочин може бути вчинено з території однієї держави, а наслідки настають на території іншої держави, або злочинець, жертва та інфраструктура, що використовувалася для вчинення злочину, можуть

перебувати в різних юрисдикціях. Чинне законодавство України не містить чітких механізмів вирішення конфліктів юрисдикцій у таких випадках.

По-друге, проблемним є питання транскордонного доступу до комп'ютерних даних. Згідно зі ст. 32 Конвенції, держава-учасниця може отримати доступ до комп'ютерних даних, що знаходяться на території іншої держави, без її дозволу у двох випадках: якщо ці дані є загальнодоступними або якщо отримано добровільну згоду особи, яка має право розкривати ці дані. Однак ця стаття не вирішує проблему доступу до даних у інших випадках, наприклад, коли дані зберігаються у «хмарних» сервісах, а їх точне місцезнаходження невідоме.

По-третє, існують проблеми з оперативністю міжнародного співробітництва. Будапештська конвенція передбачає можливість створення системи цілодобової мережі (24/7) для забезпечення оперативної допомоги при розслідуванні кіберзлочинів. Однак, на практиці, така мережа не завжди функціонує ефективно через організаційні та технічні проблеми.

Отже, імплементація Будапештської конвенції в українське законодавство є важливим кроком для забезпечення ефективної боротьби з кіберзлочинністю та інтеграції України в європейський та міжнародний правовий простір. Незважаючи на значний прогрес у цьому напрямку, залишаються проблемні аспекти, які потребують подальшого вирішення.

Основними проблемами є термінологічна неузгодженість, прогалини в криміналізації окремих діянь, недосконалість процедур збирання та дослідження електронних доказів, проблеми міжнародного співробітництва, зокрема, щодо визначення юрисдикції та транскордонного доступу до комп'ютерних даних.

Для вирішення цих проблем необхідно вдосконалити вітчизняне законодавство з урахуванням міжнародних стандартів боротьби з кіберзлочинністю, забезпечити належний баланс між ефективністю розслідування кіберзлочинів та захистом прав людини, розвивати міжнародне співробітництво в цій сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про кіберзлочинність: міжнар. док. від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 17.05.2025).
2. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. URL: <https://zakon.rada.gov.ua/laws/show/2824-15#Text> (дата звернення: 17.05.2025).
3. Бурячок В. Л., Толюпа С. В., Аносов А. О., Козачок В. А., Лукова-Чуйко Н. В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. Київ: ДУТ, 2020. 345 с.
4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: міжнар. док. від 28.01.2003. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 17.05.2025).
5. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III.

- URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 17.05.2025).
6. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 17.05.2025).
 7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 17.05.2025).
 8. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 17.05.2025).
 9. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 17.05.2025).
 10. Марисюк К. Б., Канцір В. С., Канцір І. А. Кримінально-правова охорона інформаційної безпеки в Україні: монографія. Львів: Растр-7, 2023. 220 с.
 11. Михайліченко Т. О. Щодо питання гармонізації термінології законодавства України із положеннями Конвенції про кіберзлочинність. Право і суспільство. 2023. № 3. С. 110–116.

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ УКРАЇНИ

Шавлай Максим Олександрович

курсант 201 взводу, навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України ОДУВС

Науковий керівник:

Свинаренко Ю.П.

доктор філософії, завідувач кафедри
оперативно-розшукової діяльності
навчально-наукового інституту підготовки
фахівців підрозділів кримінальної поліції
Національної поліції України ОДУВС

Україна, як країна, що активно адаптується до європейських стандартів у сфері безпеки, стикається з низкою нових викликів, пов'язаних з боротьбою з кримінальністю та кіберзлочинністю. Злочини стають дедалі складнішими, зокрема завдяки використанню новітніх технологій, що призводить до значних економічних та соціальних втрат. Актуальність проблеми кіберзагроз і кримінального аналізу зростає, адже новітні методи й підходи, що відповідають міжнародним стандартам, повинні бути інтегровані

в діяльність правоохоронних органів України. Законодавство країни у цих сферах зазнає суттєвих змін, що включають прийняття нових нормативно-правових актів, спрямованих на посилення національної безпеки.

Одним із важливих напрямків розвитку правоохоронної діяльності є використання кримінального аналізу для прогнозування злочинної діяльності, що дозволяє значно підвищити ефективність боротьби з різними видами правопорушень. В Україні розробляються та впроваджуються численні ініціативи для розвитку кримінального аналізу. Наприклад, згідно з Законом України «Про оперативно-розшукову діяльність» (№ 2135-III від 18.02.2004), оперативні підрозділи зобов'язані здійснювати аналіз криміногенної ситуації, але при цьому законодавство не містить конкретних норм, які регулюють застосування кримінального аналізу для керівництва оперативно-розшуковими заходами, що створює певні обмеження для його повноцінного використання. З 2017 року в Україні почали активно застосовувати методи кримінального аналізу для боротьби з організованою злочинністю, зокрема шляхом використання сучасного програмного забезпечення для аналізу великих обсягів даних [1].

Важливою складовою розвитку кримінального аналізу є законодавчі ініціативи, прийняті в Україні. Наприклад, Закон України «Про Національну поліцію» (№ 580-VIII від 02.07.2015) визначає функцію кримінального аналізу як одну з основних завдань правоохоронних органів, зокрема в контексті аналізу злочинності та розробки методів запобігання правопорушенням. Проте, на сьогодні не існує єдиної інтегрованої системи кримінального аналізу в діяльності поліції, що потребує вдосконалення законодавства для більш ефективного регулювання цього процесу [2].

Кібербезпека в Україні є однією з ключових складових національної безпеки. Законодавство, зокрема Закон України «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII від 05.10.2017), визначає основні принципи, структуру і відповідальність за забезпечення кібербезпеки в державі [3]. Значну увагу приділено захисту критичної інформаційної інфраструктури, що визначено статтею 8 цього закону, а стаття 9 визначає механізми реагування на кіберінциденти. З 2020 року Україна активно співпрацює з Європейським Союзом у рамках ініціативи «Цифрова економіка» та з НАТО через програму «Кібербезпека», що сприяє розвитку національної спроможності у сфері кібербезпеки.

В Україні функціонує декілька ключових державних органів, відповідальних за забезпечення кібербезпеки та кримінального аналізу. Наприклад, відповідно до Закону України «Про Службу безпеки України» (№ 2229-IV від 18.02.2004), внесених змін у 2020 році, СБУ займається протидією кіберзагрозам, зокрема запобіганням атакам на критичну інфраструктуру [4]. Національна поліція України, згідно з Законом «Про Національну поліцію» (№ 580-VIII від 02.07.2015), виконує оперативно-розшукові функції, а Державна служба спеціального зв'язку та захисту інформації (Закон № 2163-VIII) займається безпекою інформаційних

ресурсів у державному секторі [2].

Міжнародна співпраця України у галузі кібербезпеки та кримінального аналізу відіграє важливу роль у зміцненні національної безпеки. З 2017 року Україна активно співпрацює з міжнародними партнерами у рамках Спільної робочої групи з кібербезпеки в рамках співпраці з НАТО. Крім того, країна бере участь у міжнародних ініціативах, таких як «Стратегічна програма кібербезпеки Європи», що сприяє розвитку національної спроможності у кіберпросторі. У 2021 році Україна підписала угоду про співпрацю з Європейським Союзом щодо захисту критичної інформаційної інфраструктури та обміну інформацією про кіберзлочини.

Одним із важливих аспектів розвитку кримінального аналізу та кібербезпеки є підготовка фахівців. В Україні запроваджено низку спеціалізованих навчальних програм у державних та приватних навчальних закладах. Наприклад, програми підготовки кадрів для роботи в сфері кримінального аналізу включають курси, що базуються на методах кримінології, кримінального права та аналітичної роботи. Одним із прикладів є курси, організовані Українським інститутом кримінальної аналітики. Для фахівців з кібербезпеки існують центри підвищення кваліфікації, створені при Академії кібербезпеки та Державній службі спеціального зв'язку [5, с.273].

Основними викликами в розвитку кримінального аналізу та кібербезпеки залишаються недостатнє фінансування, відсутність єдиного підходу до інтеграції кримінального аналізу в оперативну діяльність поліції та дефіцит кваліфікованих кадрів у сфері кібербезпеки. Однак, зусилля уряду, міжнародних партнерів та організацій, що надають підтримку Україні, створюють умови для значного покращення ситуації в цих галузях у найближчі роки.

Отже, розвиток кримінального аналізу та кібербезпеки є важливою складовою національної безпеки України. Однак для того, щоб ефективно реагувати на сучасні загрози, необхідно продовжити вдосконалювати законодавство, інтегрувати різні елементи безпеки та розвивати відповідні навчальні програми. Лише за таких умов Україна зможе суттєво посилити свою здатність протидіяти злочинності та кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України про оперативно-розшукову діяльність Відомості Верховної Ради України (ВВР), 1992, № 22, ст.303 URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>
2. Закон України Про Національну поліцію Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379 URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>
3. Закон України Про основні засади забезпечення кібербезпеки України Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
4. Закон України Про Службу безпеки України. Відомості Верховної Ради України (ВВР), 1992, № 27, ст.382 URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>
5. Щурат, Т. Г., М. О. Шавлай. Документування та розслідування колабораціонізму в умовах воєнного стану. *Оргкомітет конференції 2024р. 272-275с.*

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ УДОСКОНАЛЕННЯ OSINT-АНАЛІТИКИ

Шипрінський Нікіта Олегович,
здобувач першого (бакалаврського) рівня вищої освіти
спеціальності 081 «Право»
Одеського державного університету внутрішніх справ
Моргунова Тетяна Іванівна,
к.т.н., доцент, доцент кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету внутрішніх справ

У сучасному світі інформація стала стратегічним ресурсом, а розвідка на основі відкритих джерел (OSINT) відіграє важливу роль у забезпеченні безпеки та правопорядку.

Отримання інформації у відкритих джерелах в інтересах розкриття і розслідування злочинів – одне з актуальних напрямків вдосконалення діяльності правоохоронних органів [1]. OSINT дозволяє відстежувати події в реальному часі й формувати цілісну картину суспільних процесів. Проте зростання обсягів даних і ускладнення інформаційного середовища поставили під сумнів ефективність традиційної аналітики.

У сферу інтересів OSINT входить добування та аналіз офіційних документів, проектів статутів, відстеження нових наукових розробок, баз даних, комерційних і державних сайтів, мережеских щоденників і багато іншого [2].

Застосування штучного інтелекту стало ключовим етапом розвитку OSINT. Автоматизований аналіз текстів, зображень і поведінкових патернів відкриває нові можливості для протидії дезінформації та загрозам. Інтеграція AI у системи безпеки є необхідною відповіддю на гібридні виклики.

Мета цієї роботи – вивчити потенціал AI у вдосконаленні OSINT-аналітики, окреслити напрями його застосування та проаналізувати супутні виклики.

У цифровому середовищі OSINT є дієвим інструментом для збору даних із відкритих джерел: медіа, соцмереж, баз даних, супутникових сервісів. Водночас ручний аналіз дедалі менш ефективний у великих інформаційних потоках через помилки, затримки та суб'єктивність. Багато даних є фрагментарними або маніпулятивними, що підсилює потребу в інтелектуальних технологіях.

Штучний інтелект дає змогу оперативно обробляти великі масиви інформації, виявляти приховані загрози й мінімізувати вплив людського фактора. Найбільш ефективними залишаються технології NLP, автоматичне сортування повідомлень і аналіз візуального контенту.

Обробка природної мови (NLP) – це підгалузь комп'ютерних наук і штучного інтелекту, що займається взаємодією між комп'ютерами і людськими (природними) мовами [3].

Сучасні інструменти вже працюють у практиці: Maltego візуалізує зв'язки, IBM i2 виявляє складні взаємозалежності, GPT-моделі аналізують тексти в реальному часі, а Palantir і Hunchly структурують інформацію та фіксують аномалії.

Серед ключових завдань – виявлення фейків, бот-мереж і скоординованих інформаційних атак. Алгоритми розпізнають повторювані повідомлення й поведінкові шаблони, що дає змогу аналітику зосередитися на глибшій інтерпретації даних та формуванні ефективних стратегій інформаційної безпеки.

Щоб краще зрозуміти, як саме AI трансформує процес аналізу відкритих джерел, варто розглянути основні функції та результати його застосування в структурованому вигляді (табл. 1).

Як видно з табл. 1, штучний інтелект виконує не лише допоміжну роль, а й забезпечує структурне підсилення всіх ключових етапів OSINT-аналітики – від збору до візуалізації даних. Його ефективність значною мірою визначається алгоритмами, які дають змогу перетворювати необроблені дані на аналітично значущу інформацію.

Таблиця 1.

Функціональні можливості штучного інтелекту в OSINT-аналітиці

Напрямок застосування AI	Основні функції	Очікувані результати
Обробка природної мови (NLP)	Виявлення ключових слів, смислів, емоцій, контексту	Швидка і точна інтерпретація великого обсягу текстових даних
Класифікація та кластеризація	Автоматичне групування повідомлень за темами або ризиками	Сегментація інформації для ухвалення рішень
Аналіз зображень та відео	Визначення об'єктів, розпізнавання облич, фіксація аномалій	Виявлення фальсифікацій, підвищення достовірності верифікації
Виявлення аномалій та патернів	Пошук синхронізованих дій, нетипових змін у поведінці	Виявлення бот-мереж і інформаційних атак
Генерація аналітичної візуалізації	Побудова графів зв'язків, теплових карт, інтерактивних панелей	Інтуїтивне представлення складної інформації в реальному часі

Алгоритми штучного інтелекту лежать в основі процесів, що забезпечують автоматичне виявлення тенденцій, загроз і аномалій у складному інформаційному середовищі. Найбільш поширеними серед них є кластеризація (групування подібної інформації), класифікація (розподіл за категоріями), виявлення аномалій (фіксація нетипових змін або сигналів) і семантичний аналіз, який дозволяє розрізнити значення текстів у залежності від контексту.

Практичне застосування цих алгоритмів демонструється на прикладі

аналізу Telegram-каналів, що стали важливим джерелом інформації у воєнний та кризовий час. За допомогою навченої AI-моделі можна автоматично класифікувати повідомлення за рівнем ризику – наприклад, відокремлювати фейки, повідомлення з ознаками паніки або такі, що потенційно містять дані про безпеку об’єктів. Такий підхід дозволяє оперативно реагувати на поширення дезінформації, не витрачаючи ресурси на ручний перегляд кожного повідомлення.

Реалізація подібних сценаріїв потребує побудови автоматизованих аналітичних пайплайнів – послідовностей дій, що охоплюють усі етапи обробки даних: від їх збору та фільтрації до фінального аналізу й візуалізації результатів. Зокрема, на першому етапі дані надходять із відкритих джерел, далі проходять очищення та попередню обробку, після чого застосовуються алгоритми класифікації чи кластеризації. Завершальним етапом є виведення результатів у зручній формі – таблиці, графі, карти або інтерактивні дашборди, які забезпечують аналітику в реальному часі.

Таким чином, штучний інтелект у складі OSINT-систем перетворюється з допоміжного інструмента на повноцінну аналітичну платформу, здатну не тільки виявляти, а й прогнозувати потенційні інформаційні загрози.

Щоб узагальнити ключові переваги впровадження AI в OSINT-аналітику, розгляньмо порівняльну характеристику традиційного та інтелектуального підходу до обробки відкритих даних (табл. 2).

Таблиця 2.

Порівняння OSINT-аналізу без і з використанням штучного інтелекту

Критерій	Традиційний OSINT	OSINT з AI
Обсяг опрацьованих даних	Обмежений, потребує багато часу	Масштабований, обробка у реальному часі
Швидкість аналізу	Низька, ручна	Висока, автоматизована
Ризик помилок	Високий (людський фактор)	Знижений, за рахунок навчання моделей
Виявлення фейків і ботів	Суб’єктивне, залежить від аналітика	Автоматичне виявлення патернів і бот-активності
Ефективність у кризових умовах	Обмежена через брак ресурсу	Висока, завдяки швидкому виявленню аномалій

Інтеграція штучного інтелекту в OSINT-аналітику докорінно змінила способи обробки відкритих джерел. Завдяки AI стало можливим обробляти величезні обсяги даних у реальному часі, виявляючи загрози ще до їх широкого поширення. Автоматизація зменшує навантаження на аналітиків, даючи змогу зосередитися на глибокому аналізі.

Попри переваги, застосування AI в OSINT супроводжується проблемами: хибні спрацьовування, неякісні дані, культурні бар’єри, deepfake-технології та юридичні обмеження доступу. У таких умовах роль

аналітика зростає – саме він забезпечує критичну оцінку й захист від маніпуляцій.

OSINT з AI має стратегічне значення, особливо для систем нацбезпеки. Оскільки інформаційна війна часто є першим етапом конфлікту, важливо своєчасно виявляти загрози. Це потребує не лише адаптації чужих рішень, а й створення власних платформ, враховуючи мовні, політичні та кіберспецифіку.

Успішна реалізація неможлива без фахівців, які поєднують знання AI з аналітикою. Потрібні оновлені освітні програми та спеціалізовані OSINT-центри. Також необхідне дотримання етичних стандартів – прозорість, повага до приватності й недопущення зловживань, аби технології служили безпеці, а не загрозі.

Отже, майбутнє OSINT-аналітики в Україні – це поєднання технологічної досконалості, національного інтересу й етичної відповідальності. Лише така інтегрована екосистема здатна гарантувати інформаційну безпеку та стійкість держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ісмаїлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.

2. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. *Протибія кіберзлочинності та торгівлі людьми* Збірник матеріалів Міжнародної науково-практичної конференції. Харків: ХНУВС, 2020. С. 135-137.

3. Що таке обробка природної мови (Natural Language Processing, NLP)? *The Transmitted*: інформаційна онлайн-платформа. 2024. URL: <https://thetransmitted.com/adlucem/shho-take-obrobka-pryrodnoyi-movy-natural-language-processing-nlp/> (дата звернення: 14.05.2025).

БЕЗПЕКА У КІБЕРСФЕРІ

Шоломіцький Артур Аркадійович
курсант Національної академії Державної прикордонної служби
України імені Богдана Хмельницького

Науковий керівник:
Гончаренко Ольга Анатоліївна,
доктор філософських наук, професор,
Національна академія Державної
прикордонної служби України імені Богдана Хмельницького

Кібербезпека, або ж cybersecurity — це сукупність заходів, спрямованих на захист інформації та пристроїв, підключених до мережі, від несанкціонованого доступу, зловживань чи кіберзлочинів [6, с.12]. Вона покликана забезпечити конфіденційність, цілісність і доступність даних на всіх етапах їхнього існування. Якщо фізична безпека захищає людей і майно від крадіжок чи пошкоджень, то кібербезпека охоплює захист цифрової інформації, комп'ютерів, серверів, додатків і даних, що в них зберігаються. Її роль — не лише в охороні особистих файлів, а й у безпеці стратегічно важливих державних та корпоративних систем [3, с.48].

Поняття кіберзахисту передбачає здатність вчасно розпізнавати загрози та протидіяти їм [5, с.112]. Це активна робота над попередженням кібератак, реагуванням на спроби вторгнення та нейтралізацією наслідків. Незалежно від підходу, основна мета кіберзахисту — мінімізувати ризики та захистити цифровий простір від потенційної шкоди [2, с.15].

Агресивні кіберзагрози стають дедалі більш складними та різноманітними у міру розвитку технологій [4, с.32]. Кіберзлочинність включає злочини, що здійснюються через комп'ютерні мережі, зокрема крадіжку особистих даних, фінансових ресурсів чи інтелектуальної власності. Атаки за допомогою шкідливого програмного забезпечення (мальваре) мають на меті пошкодження або несанкціонований доступ до систем і даних, серед яких віруси, трояни та програми-вимагачі (ransomware) [3, с.50]. Фішинг є ще однією загрозою, де зловмисники використовують методи обману для здобуття конфіденційної інформації, такої як паролі чи дані кредитних карток. Однією з найнебезпечніших форм є атаки на критично важливу інфраструктуру, що включає енергетичні системи, транспорт або фінансові мережі, що може мати серйозні наслідки для національної безпеки [8, с.165].

Важливою складовою соціально-економічної безпеки кожної держави є національна стратегія кібербезпеки (National Cybersecurity Strategy, NCS). В Україні така стратегія була затверджена 27 січня 2016 року і визначила кібербезпеку та інформаційну безпеку серед ключових напрямів у протидії загрозам національній безпеці [7]. Щоб забезпечити її ефективне впровадження, уряд щорічно розробляє плани з конкретними заходами,

спрямованими на запобігання кіберінцидентам та готовність до реагування на них. Ці заходи включають створення повноцінної системи національного кіберзахисту [5, с.101].

Координацією та наглядом за цим процесом займаються державні органи, кожен з яких має свої обов'язки у сфері кібербезпеки. Зокрема, функціонує Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Він виконує роль головного координатора міжвідомчої взаємодії у випадках кібератак чи інцидентів в інформаційно-телекомунікаційних системах, особливо в об'єктах критичної інфраструктури, з метою підвищення загальної ефективності захисту [5, с. 105].

Одним із важливих інституційних елементів у цій системі є Національний координаційний центр кібербезпеки при РНБО України. Він відповідає за координацію міжвідомчої взаємодії у випадках кіберінцидентів, зокрема, коли мова йде про об'єкти критичної інфраструктури — енергетику, транспорт, зв'язок, фінанси. Центр не лише забезпечує оперативну реакцію, але й координує запобіжні заходи, здійснює аналітику та прогнозування загроз [7].

Окрім внутрішніх реформ, Україна активно рухається в напрямку європейської та євроатлантичної інтеграції в галузі кібербезпеки. Основу нормативного регулювання складають такі документи як Будапештська конвенція, Директива NIS ЄС, а також український Закон «Про основні засади забезпечення кібербезпеки України» [7]. Важливу роль відіграє й міжнародне партнерство: Україна співпрацює з НАТО, ЄС та іншими організаціями, що посилює її позиції в кіберпросторі [4, с.33].

Разом із тим, система все ще потребує удосконалення. Проблемними залишаються: нечіткість термінології в законодавстві, дублювання функцій між установами, обмежене фінансування та недостатня цифрова грамотність населення [1, с.316]. Тому важливим кроком є не лише формальне ухвалення норм, а й їх ефективне впровадження, підкріплене сучасними технічними рішеннями, навчальними ініціативами та підтримкою з боку громадянського суспільства [3, с.53].

Упродовж останніх років Україна зробила помітні кроки у формуванні національної системи кіберзахисту. Від 2016 року, коли було затверджено Національну стратегію кібербезпеки, країна перебуває у стані постійної адаптації до нових викликів — як технологічних, так і геополітичних [7]. Розвиток цифрової безпеки відбувається на тлі гібридної війни, в межах якої кібератаки стали інструментом інформаційної агресії.

Україна активно імплементує положення міжнародного законодавства: основу нормативної бази складають Будапештська конвенція про кіберзлочинність, Директива NIS та український закон «Про основні засади забезпечення кібербезпеки» [7]. Ці документи забезпечують інтеграцію в європейську систему кіберзахисту та слугують орієнтиром для побудови власної ефективної моделі. Особливу увагу сьогодні приділяють розвитку кадрового потенціалу та кіберграмотності. Створення європейської мережі центрів

кіберкомпетенцій (в межах проєктів CONCORDIA, SPARTA, ECHO тощо) демонструє, що нестача фахівців є проблемою не лише для України, а й для всього регіону [6, с.147]. Для її подолання розробляються навчальні програми, курси для держслужбовців, шкільна освіта з основ цифрової безпеки.

Успішний досвід партнерських країн, таких як Естонія, яка першою створила повноцінну модель цифрової держави, також враховується при формуванні української системи. Естонія не лише створила Центр кіберзахисту НАТО в Таллінні, але й щорічно проводить аналізи тисяч кіберінцидентів, що дозволяє швидко реагувати на загрози [5, с.189].

У межах реформи в Україні також акцентують увагу на необхідності інтелектуального захисту. Йдеться не лише про технічні інструменти (системи моніторингу, аналізу трафіку, криптографічний захист), а й про аналітичні механізми прогнозування поведінки зловмисників [2, с.16]. Розробка індикаторів безпеки, моделювання сценаріїв атак, виявлення аномальної поведінки — усе це є частиною нової кіберполітики [6, с.188].

Отже, кібербезпека є критично важливою складовою сучасного суспільства, забезпечуючи захист інформації та інфраструктури від зростаючих кіберзагроз. Розвиток ефективних механізмів кіберзахисту, вдосконалення законодавства, а також інтеграція з міжнародними стандартами є важливими етапами для зміцнення національної безпеки. Україна, попри численні виклики, активно впроваджує стратегії кіберзахисту, орієнтуючись на міжнародний досвід та сприяючи розвитку кадрів і цифрової грамотності. Водночас, для досягнення максимального ефекту необхідно продовжувати роботу з удосконалення системи, підвищення ефективності співпраці та ресурсного забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Лісовська, Ю. Кібербезпека: ризики та заходи : навч. посіб. / Ю. Лісовська. Київ : Кондор, 2019. 272 с.
2. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій// *Товари і ринки*. 2022. № 3. С.47-59
3. Довгань О, Литвинова Л., Дорогих С. (упоряд.). Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. Київ : 2023. № 7. 270 с.
4. Безуглий Д. Інформаційна безпека України: огляд останніх тенденцій // *Фізико-математична освіта*. 2018. Вип. 2(16). С.13-17
5. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: науково-практична інтернет-конференція, Державний університет телекомунікацій Навчально-наукового інституту захисту інформації. Київ, 2022. С.31-33
6. Фурашев, В. М. Кіберпростір та інформаційний простір, кібербезпека

та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // *Інформація і право*. 2012. № 2. С.162-169

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/Laws/show/447/2021#Text> (дата звернення: 24.04.2025)

8. Биков В. Ю., Буров О. Ю., Дементівська Н. П. Кібербезпека в цифровому навчальному середовищі// *Інформаційні технології і засоби навчання*. 2019. Т. 70, № 2. С.313-331

СУЧАСНИЙ СТАН ВЗАЄМОДІЇ ДЕРЖАВНИХ ОРГАНІВ ТА ГРОМАДСЬКИХ ОРГАНІЗАЦІЙ У ПРОЦЕСІ НАДАННЯ СОЦІАЛЬНОЇ ДОПОМОГИ

Алфьоров Сергій Юрійович,

здобувач Харківського національного
університету внутрішніх справ

ORCID: <https://orcid.org/0009-0007-3965-2574>

З кожним роком роль громадськості у вирішенні «долі» держави стає все більш суттєвою, що виражається у можливості українців впливати на порядок здійснення тих чи інших державних функцій та операцій. В даному випадку мова йде не тільки про соціальний контроль з боку населення, як платників податків та ключового джерела влади, а й консолідацію ресурсів та зусиль приватного та публічного сектору із вирішення відповідних суспільно-важливих питань. Такий формат взаємодії простежується в багатьох галузях, у тому числі й у сфері соціального захисту. Все частіше з'являються випадки співпраці державних органів та громадських організацій з питань надання соціальних послуг, що має свою специфіку та порядок.

В першу чергу слід звернути увагу на сферу надання гуманітарної допомоги. Законом України «Про гуманітарну допомогу» визначено, надають гуманітарну допомогу донори – юридичні особи, створені та зареєстровані відповідно до законодавства України або іноземної держави, та фізичні особи, що перебувають в Україні або за її межами, які добровільно надають гуманітарну допомогу отримувачам гуманітарної допомоги в Україні або за її межами [1]. В даному механізмі, держава представлена спеціально уповноваженими державними органами з питань гуманітарної допомоги, до яких належать: центральний орган виконавчої влади, що реалізує державну політику у сфері соціального захисту населення; Рада міністрів Автономної Республіки Крим; обласні, Київська та Севастопольська міські державні адміністрації. Спеціально уповноважені державні органи з питань гуманітарної допомоги приймають рішення за погодженням із митними органами, податковими органами, центральними органами виконавчої влади, що забезпечують формування та реалізують державну політику у сфері

охорони здоров'я, у сфері економічного розвитку, державну фінансову політику, центральним органом виконавчої влади, що реалізує державну політику у сфері цивільного захисту, Міністерством внутрішніх справ України, органами Національної поліції, Національним банком України чи його філіями (територіальними управліннями). Відповідно до Закону України «Про гуманітарну допомогу», центральний орган виконавчої влади, що реалізує державну політику у сфері соціального захисту населення, здійснює: визнання вантажів, коштів, у тому числі в іноземній валюті, виконаних робіт, наданих послуг гуманітарною допомогою; контроль за отриманням, розподілом, використанням за цільовим призначенням, підготовкою статистичної звітності, обліком гуманітарної допомоги, визнаної такою рішенням спеціально уповноважених державних органів з питань гуманітарної допомоги; контроль за діяльністю Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, що діють у межах наданих їм законодавством повноважень; забезпечення ведення автоматизованої системи реєстрації гуманітарної допомоги в порядку, встановленому Кабінетом Міністрів України тощо [1].

Дещо інша, але не менш дієва модель взаємодії державних органів а громадських організацій з питань надання соціальної допомоги та соціальної підтримки регламентована Законом України «Про основи соціальної захищеності осіб з інвалідністю в Україні». Так, відповідно до Розділу III Закону можуть утворюватися спеціальні громадські об'єднання осіб з інвалідністю та їх спілки з метою забезпечення рівних прав і можливостей осіб з інвалідністю та їх соціального захисту, виявлення, усунення перепон і бар'єрів, що перешкоджають забезпеченню прав і задоволенню потреб таких осіб, у тому числі стосовно доступу їх нарівні з іншими громадянами до об'єктів фізичного оточення, транспорту, інформації та зв'язку, а також з урахуванням індивідуальних можливостей, здібностей та інтересів - до освіти, праці, культури, фізичної культури і спорту, надання соціальних послуг, залучення осіб з інвалідністю до суспільної діяльності, здійснення громадського контролю за дотриманням прав осіб з інвалідністю, представництва їхніх інтересів та усунення будь-яких проявів дискримінації стосовно осіб з інвалідністю та мають право користуватися пільгами і преференціями, передбаченими законодавством. Представники всеукраїнських громадських об'єднань осіб з інвалідністю, їх спілок залучаються (за їх зверненням) до складу колегій і консультативно-дорадчих органів центральних органів виконавчої влади, а представники місцевих – до складу колегій і консультативно-дорадчих органів місцевих органів виконавчої влади та органів місцевого самоврядування відповідно до свого статусу та території діяльності. Центральні і місцеві органи виконавчої влади та органи місцевого самоврядування повинні надавати допомогу і сприяти громадським об'єднанням осіб з інвалідністю в їх діяльності. Місцеві органи таких об'єднань, а також трудові колективи їх підприємств (об'єднань), установ і організацій вправі вносити в органи місцевого самоврядування

пропозиції з питань соціального захисту осіб з інвалідністю [2].

Громадські організації відіграють важливу роль у процесі надання соціальної допомоги під час правового режиму воєнного стану та інших подібних надзвичайних подій. Наприклад, в статті 16 Закону України «Про забезпечення прав і свобод внутрішньо переміщених осіб» визначено, що органи державної виконавчої влади та органи місцевого самоврядування можуть залучати громадські об'єднання до процесу формування і реалізації державної політики щодо вирішення питань внутрішньо переміщених осіб [3]. В свою чергу, у Законі України «Про правовий режим воєнного стану», а саме в статті 17 документу, вказано, що органи державної влади України, Верховна Рада Автономної Республіки Крим, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування, підприємства, установи, організації, громадські об'єднання, а також громадяни зобов'язані сприяти діяльності військового командування та військових адміністрацій у запровадженні та здійсненні заходів правового режиму воєнного стану на відповідній території [4].

Сприяння громадських організацій органам державної влади та місцевого самоврядування виражається, передусім, у формуванні умов ефективного виконання публічних функцій. Тобто, об'єднання громадян своїми діями полегшують процес реалізації тих чи інших завдань і напрямів діяльності, наприклад, шляхом: вирішення питання про надання місця розміщення внутрішньо-переміщених осіб, координації центрів допомоги таким особам; здійснення евакуації цивільних осіб із небезпечних зон, які виникли внаслідок воєнного стану; надання засобів першої необхідності особам, які постраждали внаслідок бойових дій чи надзвичайних ситуацій і таке інше. В даному випадку громадські організації не дають соціальну допомогу, як таку, а лише допомагають органам державної влади піклуватись про населення з метою подальшої реалізації відносно його окремих верст інститутів соціального захисту.

Таким чином, порядок взаємодії державних органів та громадських організацій у процесі надання соціальної допомоги, включає в себе три ключові моделі співпраці: 1) контрольно-організаційну – відносини між державою та громадськими об'єднаннями полягають у здійсненні координації та контролю останніх публічним сектором в сфері надання гуманітарної допомоги. В даному контексті громадські організації використовуються державою, як розподільники матеріальних благ наданих в порядку гуманітарної допомоги населенню держави та, зокрема, тим його верстам, які перебувають у важкому, скрутному становищі; 2) участь представників громадськості в органах управління та консультативно-дорадчих органах відомств виконавчої влади. В даному випадку прикладом є діяльність громадських об'єднань осіб з інвалідністю, представників яких залучають до колегій та інших подібних інституцій управління центральних та місцевих органів державної влади, що дає можливість лобювати відповідним верстам населення свої інтереси; 3) сприяння громадськими

організаціями діяльності органів державної влади, у тому числі в сфері соціального захисту населення – дана модель передбачає створення належних умов силами громадськості для ефективного здійснення соціальної допомоги та її надходження безпосереднім адресатам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про гуманітарну допомогу: закон від 22.10.1999 №1192-XIV. Відомості Верховної Ради України. 1999. №51. Ст.451.
2. Про основи соціальної захищеності осіб з інвалідністю в Україні: закон від 21.03.1991 №875-XII. Відомості Верховної Ради УРСР. 1991. №21. Ст.252.
3. Про забезпечення прав і свобод внутрішньо переміщених осіб: закон від 20.10.2014 №1706-VII. Відомості Верховної Ради України. 205. №1. Ст.1.
4. Про правовий режим воєнного стану: закон від 12.05.2015 №389-VIII. Відомості Верховної Ради України. 2015. №28. Ст.250.

ДО ХАРАКТЕРИСТИКИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ МЕДІАТОРІВ В УКРАЇНІ

Глушенко Євген Володимирович,
аспірант Харківського національного
університету внутрішніх справ

ORCID: <https://orcid.org/0009-0005-0896-3324>

Важливим елементом адміністративно-правового статусу медіаторів є їх юридична відповідальність. Остання, як вбачається, є важливим правовим важелем стримувань і противаг в діяльності будь-якого суб'єкта адміністративних правовідносин. На нашу думку, юридичною відповідальністю медіатора є встановлені державою, в залежності від характеру протиправного діяння (дії або бездіяльності) та його наслідків, заходи примусу, які тягнуть для нього несприятливі наслідки майнового, особистісного, організаційного та іншого характеру.

Що стосується видів юридичної відповідальності, зокрема медіатора, то вони відповідають загальноприйнятому поділу їх на дисциплінарну, цивільно-правову, адміністративну та кримінальну відповідальність, яку вони несуть на загальних підставах. Відповідно до Закону України «Про медіацію», у разі порушення зобов'язань за договором про проведення медіації медіатор несе цивільно-правову відповідальність відповідно до закону. У випадках, передбачених законом, медіатор несе адміністративну чи кримінальну відповідальність. У разі недотримання норм професійної етики медіатор несе відповідальність, визначену статутом або положенням об'єднання медіаторів, членом якого він є [1].

Тому переходимо більш детально до характеристики кожного з її видів. Отже, що є дисциплінарною відповідальністю для медіатора? Відповідно до ст. 147 Кодексу законів про працю України до працівника за порушення трудової дисципліни може бути застосовано тільки один з таких заходів стягнення: догана та звільнення. Але одразу уточнюється, що законодавством, статутами і положеннями про дисципліну можуть бути передбачені для окремих категорій працівників й інші дисциплінарні стягнення [2]. Так, наприклад, в нашому випадку це може бути видалення медіатора з реєстру медіаторів або виключення з організації (об'єднання) медіаторів тощо. Таким чином дисциплінарними проступками у сфері медіації варто вважати: порушення трудової дисципліни; порушення правил внутрішнього трудового розпорядку; порушення порядку трудової діяльності; порушення етичних вимог медіатора; розголошення конфіденційної інформації щодо медіації та інформації отриманої під час медіації; порушення принципів самовизначення сторін, добровільної, рівної та активної участі сторін у процедурі медіації; використання повноважень в особистих (приватних) інтересах або в неправомірних особистих інтересах інших осіб (конфлікт інтересів); втрата нейтральності тощо.

Окрім того, за порушення трудової дисципліни одна зі сторін (сторони) може подати скаргу до об'єднання медіаторів в якому він зареєстрований. Для належного розгляду скарги обов'язково необхідно зазначити прізвище, ім'я, по-батькові медіатора, коротко описати ситуацію (при цьому дуже важливо зберігати конфіденційну інформацію іншої сторони). Одночасно з цим надана інформація має бути достатньою для того, щоб була можливість розглянути скаргу по суті. Скаргу можна також залишити безпосередньо в особистому профілі медіатора в Реєстрі медіаторів конкретного об'єднання.

Таким чином, дисциплінарна відповідальність медіатора є найпоширенішим видом юридичної відповідальності, який застосовується до нього у зв'язку з вчиненням ним дисциплінарного проступку та має свої особливості. Ці особливості полягають у тому, що дисциплінарна відповідальність медіатора настає для нього не тільки за порушення норм трудової дисципліни чи правил внутрішнього трудового розпорядку, але й за порушення етичних принципів, норм та стандартів, які виробляються їх об'єднаннями.

Цивільно-правова відповідальність медіатора пов'язана із діями, що порушили майнові права громадян, підприємств, установ або організацій і завдали їм шкоди. При цьому вона повинна наставати тільки у випадках серйозного нехтування медіатором своїми обов'язками, явних зловживань, грубої недбалості або, навіть, злочину. Обов'язковою передумовою відшкодування шкоди, завданої ним, має бути його умисел на порушення чинного законодавства, в результаті якого спричинено шкоду правам і законним інтересам сторонам медіаційного процесу. Цивільно-правова

відповідальність за таких умов має компенсаційний, майновий характер і полягає в застосуванні до медіатора-винуватця в інтересах іншої особи (осіб) встановлених законом засобів впливу, які тягнуть за собою негативні для нього наслідки у вигляді відшкодування збитків, сплати штрафу і т. ін. Відповідна норма згаданий раніше статті 15 Закону України «Про медіацію» [3]. При визначенні розміру шкоди для відшкодування медіатором має враховуватися його майнове становище, співвідношення розміру заподіяної шкоди до його грошової винагороди, ризик виникнення шкоди, досвід роботи, а також інші обставини, у зв'язку з якими повне відшкодування медіатором шкоди буде обґрунтованим. Але не вирішеним залишається питання з приводу того у якій формі здійснюватиметься цивільно-правова відповідальність – відшкодовуватиметься моральна шкода чи матеріальні збитки. Відтак це питання необхідно вирішити в законодавчому порядку.

Адміністративна відповідальність є найбільш поширеною формою юридичної відповідальності. Остання настає для медіатора на загальних підставах, тобто якщо він вчинив протиправне діяння передбачене Кодексом України про адміністративні правопорушення та іншими актами державного управління (що є особливістю адміністративної відповідальності), то він буде нести відповідальність як загальний суб'єкт проступку. Сторони медіації у разі вчинення медіатором адміністративного правопорушення можуть оскаржити такі дії до органів суду та інших осіб, уповноважених на те державою.

Що стосується стягнень, які застосовується за вчинення адміністративних правопорушень у сфері медіації, то вони переважно мають майновий характер. Кодекс України про адміністративні правопорушення (далі – КУпАП) за такі види протиправної поведінки передбачає, у переважній своїй більшості, штраф (грошове стягнення, що накладається на медіатора за адміністративні правопорушення у випадках і розмірі, встановлених КУпАП та іншими законами України). Інколи у санкціях статей особливої частини КУпАП за правопорушення пов'язані із корупцією, або ті, які мають конфлікт інтересів чи пов'язані зі зловживанням своїх прав, можемо зустріти такий додатковий вид стягнення як конфіскація, тобто примусова безоплатна передача предмета, який став знаряддям вчинення або безпосереднім об'єктом адміністративного правопорушення, у власність держави за рішенням суду [4].

Кримінальна відповідальність є найвищою мірою відповідальності, тобто найбільш суворим видом державного примусу, який застосовується до медіатора на загальних підставах. На загальнотеоретичному рівні під кримінальною відповідальністю запропоновано розуміти такий вид юридичної відповідальності, який настає за вчинення суспільно-небезпечного діяння, що містить ознаки складу злочину, передбаченого Кримінальним кодексом України. При цьому варто зазначити, що в рамках кримінальної відповідальності медіаторів доцільно виокремити два види

проступків: 1) ті, які медіатор вчиняє поза межами своєї професійної діяльності (тобто ті, які мають наслідком застосування стягнення до медіатора як до загального суб'єкта кримінальної відповідальності); 2) ті, що пов'язані з його правовим статусом в процесі медіації (наприклад статті 365-2 «Зловживання повноваженнями особами, які надають публічні послуги» чи 368-4 «Підкуп особи, яка надає публічні послуги» та ряд інших). Але при цьому варто акцентувати увагу на тому, що статус медіатора не є кваліфікуючою обставиною та не впливає на характер та розмір стягнення, яке буде застосовуватися до медіатора у зв'язку зі вчиненням кримінального проступку.

Таким чином, підбиваючи підсумки щодо юридичної відповідальності медіаторів, зазначимо, що даний інститут є невід'ємним атрибутом адміністративно-правового статусу медіатора, а тому потребує якісного предметного нормативного врегулювання. Зокрема, має бути вироблений єдиний механізм притягнення медіатора до дисциплінарної відповідальності, яка є найбільш поширеним заходом примусу, що застосовується до нього у зв'язку з невиконанням або неналежним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про медіацію / Закон України від 16.11.2021 № 1875-IX
URL: <https://zakon.rada.gov.ua/laws/show/1875-20/conv#Text>
2. Кодекс законів про працю України: закон України від 10.12.71 р. № 322-VIII // База даних «Законодавство України» / Верховна Рада України. URL: <http://zakon.rada.gov.ua/laws/show/322-08>.
3. Про медіацію / Закон України від 16.11.2021 № 1875-IX
URL: <https://zakon.rada.gov.ua/laws/show/1875-20/conv#Text>
4. Кодекс України про адміністративні правопорушення: закон України від 7 грудня 1984 року № 8073-X // База даних «Законодавство України» / Верховна Рада України. URL: <http://zakon.rada.gov.ua/laws/show/80731-10>.

СОЦІАЛЬНА ІНКЛЮЗИВНІСТЬ, ЯК ВАЖЛИВИЙ ЧИННИК НЕОБХІДНОСТІ ДІДЖИТАЛІЗАЦІЇ СФЕРИ НАДАННЯ АДМІНІСТРАТИВНИХ ПОСЛУГ В УКРАЇНІ

Грачов Єгор Олегович,
аспірант Харківського національного
університету внутрішніх справ
ORCID: <https://orcid.org/0009-0000-5049-3921>

Вперше термін «інклюзія» було застосовано в 1970-х роках у США, коли дослідники визначали соціальну інклюзію, під якою розуміли збільшення ступеня участі всіх громадян у соціумі, коли кожна людина як індивідуальність сприймається суспільством і має можливість повноцінно

брати участь у соціальних процесах. Право участі у соціумі базується на соціальній етиці у всіх сферах життя. Сам термін «інклюзія» (від англійського «inclusion» – включення) означає процес збільшення ступеня участі всіх громадян у суспільстві (як цілісній соціальній системі), направлений на розвиток рівності. У ХХІ сторіччі попри всі глобалізаційні та технологічні процеси дискримінація за різними ознаками все ще має місце, інклюзивність стала першочерговою метою рухів за розширення прав та можливостей людини. Останніми роками дуже популярними стають дискусії щодо розширення поняття інклюзивності і застосування його в якості індикатора економічного розвитку національної економіки. Такий підхід чітко окреслився на Всесвітньому економічному форумі в Давосі у 2017 році, де був запропонований Індекс інклюзивного росту та розвитку, який використовується для загальної оцінки стану економічного розвитку країни. Створення цього показника обумовлено тим, що існуючі підходи до оцінки рівня розвитку країн (наприклад із застосуванням показника внутрішній валовий продукт на душу населення), не в повній мірі відповідає сучасним вимогам. Зокрема, в країнах з високими темпами економічного зростання можна спостерігати одночасне зростання нерівності за рівнем доходів населення [1;2, с.45].

Відгалуженням наведеної категорії є соціальна інклюзія, яка з'явилась як результат переходу суспільства до соціальної політики, яка базується на соціальній моделі інвалідності. Фактично це процес змін у політичній, економічній, соціальній сферах, спрямований на утвердження соціальної рівності. Це забезпечення таких умов, за яких усі діти й дорослі могли б брати участь у житті суспільства як рівноправні його члени, яких поважають і які роблять свій внесок у суспільний розвиток. Соціальна інклюзія відображає активний і спрямований на розвиток людини підхід до суспільного добробуту, що передбачає не просто ліквідацію бар'єрів чи ризиків, а дещо більше: зміну концепції соціальної політики. «Соціальна інклюзія» – це процес, спрямований на забезпечення людям, які зазнають ризику бідності та соціального вилучення, можливостей та ресурсів, необхідних для того, щоб повною мірою брати участь в економічному, соціальному та культурному житті та досягти рівня життя і добробуту відповідно до стандартів якості життя. Дії держав відповідно до принципів соціальної інклюзії мають забезпечувати людям ширші можливості для участі в підготовці та прийнятті рішень, що їх стосуються, та реалізації їхніх основних прав [3, с.12-13].

О.О. Стрельнікова та Н.О. Єсіна пишуть, що соціальна інклюзія в сучасному українському суспільстві стає певним соціальним механізмом, інструментом, спрямованим на подолання бар'єрів та обмежень на шляху до соціального благополуччя та добробуту, що докорінно змінює існуючу державну соціальну політику. Власне, соціальне включення можна визначити як бажану ситуацію, у межах котрої всі члени суспільства володіють

достатніми ресурсами та можливостями задля повноцінної та рівноправної участі в усіх сферах суспільної діяльності. Соціальна інклюзія торкається усіх соціальних процесів й фактично сприяє утвердженню у суспільстві соціальної рівності. На їх погляд соціальна інклюзія може відбуватися у два способи: по-перше, за умови підвищення соціального статусу, що дозволить особі або групі осіб більшою мірою впливати на усі аспекти життя громади чи суспільства в цілому; по-друге, через повернення особи або групи осіб до загальноновизнаної соціальної ієрархії [4, с.238].

Таким чином, соціальна інклюзивність передбачає панування в державі стану, який забезпечує справедливе розподілення ресурсів, а також надання можливості всім верстам населення вступати в рівні суспільно-правові відносини із іншими суб'єктами, реалізовувати свої права та інтереси, бути частиною суспільства. Дана концепція, передусім, відноситься до фізичних осіб із вадами здоров'я, які в силу об'єктивних причин обмежені в своїх фізичних можливостях. Однак, за умови існування інклюзивного соціального середовища подібні особи можуть цілком комфортно співіснувати з іншими людьми, а також вести наблизений до загального спосіб життя. Логічно, що таким суб'єктам необхідно забезпечити рівний та повний доступ до всіх існуючих адміністративних послуг. Саме діджиталізація надає широкі можливості у даному напрямку.

Використовуючи цифрові механіки та технології будь-яка особа, навіть із суттєвими фізичними обмеженнями, може звернутись до органів влади і місцевого самоврядування для вирішення своїх проблем і реалізації суб'єктивних прав, інтересів. Другим аспектом, який можна відмітити в даному контексті, є те, що в умовах оцифрованих адміністративних послуг набагато легше забезпечити інклюзивні умови виконання державних функцій. В цьому випадку основні зусилля повинні бути приділені електронним системам та сервісам, які надають доступ до адміністративних послуг. Вони повинні забезпечуватись спеціальним інтерфейсом та логікою за використання якої кожна людина, з будь-якими вадами зможе контактувати із державою. Організувати саме такі умови набагато простіше, чим, наприклад, будувати спеціальні архітектурно-технічні споруди для осіб з проблемами руху безпосередньо в органі влади чи місцевого самоврядування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gupta, J., Cornelissen, V. and Ros-Tonen, M. (2015), "Inclusive development", In: Encyclopedia of Global Environmental Governance and Politics, Cheltenham, Great Britain, pp. 35-44.
2. Мельник М.А. Інклюзивна політика держави під час війни. Вісник Східноукраїнського національного університету імені Володимира Даля. 2022. №6(276). С.44-49.
3. Стандарти громадсько-активної школи: соціальна інклюзія: навчально-методичний посібник. Найда Ю.М., Ткаченко Л.М. Під заг. ред.

Даниленко Л.І., К.: ТОВ «Видавничий дім «Плеяди», 2014. 68 с.

4. Стрельнікова О.О., Єсіна Н.О. Поняття та сутність соціальної інклюзії у соціальній роботі. Сучасне суспільство. 2019. Випуск 1(17). С.233-241.

ДО ХАРАКТЕРИСТИКИ КЛЮЧОВИХ ПРИНЦИПІВ ЗДІЙСНЕННЯ ДЕРЖАВНОГО КОНТРОЛЮ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Пичурин Артем Анатолійович,

аспірант Харківського національного
університету внутрішніх справ

ORCID: <https://orcid.org/0009-0009-4515-0663>

Здійснення державного контролю у сфері використання інформаційних технологій є складним за своєю сутністю та змістом процесом, в основі якого лежить система відправних начал, тобто принципів. Останні в розрізі представленої у роботі проблематики являють собою сукупність основоположних, керівних, загальнообов'язкових, закріплених в законодавстві спеціальних ідей-цінностей, з огляду на які регламентовано поведінку учасників суспільно-правових відносин, що виникають в сфері здійснення відповідного різновиду державного контролю за впровадженням та використанням інформаційних технологій в Україні.

В юридичній літературі до принципів державної контрольної діяльності, як правило відносять: принцип розмежування повноважень, принцип формальної рівності підконтрольних об'єктів, принцип оптимізованого використання контрольних ресурсів, принцип відкритості та прозорості, принцип об'єктивності, принципи пропорційності, незалежності, стабільності та інші [1;2;3;4]. На нашу думку, до принципів, з огляду на які має здійснюватися державний контроль в сфері використання інформаційних технологій, відносяться наступні:

- верховенство права. Даний принцип закріплено статтею 8 Конституції, але розкривається його зміст у Постанові Пленуму Верховного Суду України «Про застосування Конституції України при здійсненні правосуддя» від 01.11.1996 №9. В документі визначено, що принцип верховенства права полягає у тому, що конституційні права і свободи людини та громадянина є безпосередньо діючими, вони визначають зміст та спрямованість діяльності органів законодавчої та виконавчої влади, органів місцевого самоврядування і забезпечуються захистом правосуддя [5]. Також варто відзначити Рішення Конституційного Суду України у справі за конституційним поданням Верховного Суду України щодо відповідності

Конституції України (конституційності) положень статті 69 Кримінального кодексу України (справа про призначення судом більш м'якого покарання) від 02.11.2004 № 15-рп/2004, в якому зазначається: верховенство права – це панування права в суспільстві. Верховенство права вимагає від держави його втілення у правотворчу та правозастосовну діяльність, зокрема у закони, які за своїм змістом мають бути проникнуті передусім ідеями соціальної справедливості, свободи, рівності тощо. Справедливість – одна з основних засад права, є вирішальною у визначенні його як регулятора суспільних відносин, одним із загальнолюдських вимірів права. Зазвичай справедливість розглядають як властивість права, виражену, зокрема, в рівному юридичному масштабі поведінки й у пропорційності юридичної відповідальності вчиненому правопорушенню [6;7, с.154]. З огляду на викладене, принцип верховенства права, як керівна засада державного контролю в сфері використання інформаційних технологій, визначає панування права, правових методів та інструментів у контексті регулювання та упорядкування суспільних відносин, які виникають під час здійснення зазначеної діяльності. Тобто, поведінка суб'єктів цих відносин повністю та безальтернативно скеровується правом;

- гуманізм та забезпечення прав людини. Зміст наведеного принципу полягає у тому, що зазначений тип офіційної діяльності повинен спрямовуватись, передусім, на утвердження, забезпечення та захист прав, свобод і законних інтересів людини. Інструменти контролю в результаті свого застосування мають покращувати життєдіяльність людей, підвищувати ефективність та нормативну урегульованість ІТ в усіх сферах життя, сприяти безпеці їх використання та впровадження;

- законність державного контролю. Цей принцип вимагає, щоб державний контроль в сфері використання інформаційних технологій: по-перше, здійснювався тільки прямо уповноваженими на це законодавством органами та їх посадовими особами; по-друге, суб'єкти реалізації контролю мають суворо та неухильно дотримуватись законодавчих вимог, порядку здійснення контрольної діяльності та посадових інструкцій; по-третє, порушення законності відповідними суб'єктами владних повноважень гарантовано є підставою для притягнення їх до юридичної відповідальності;

- об'єктивність та рівність державного контролю. Основу принципу складають Конституційні положення в яких прописано, що усі люди є вільні і рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними. Громадяни мають рівні конституційні права і свободи та є рівними перед законом. Не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками. Рівність прав жінки і чоловіка забезпечується: наданням жінкам рівних з чоловіками можливостей у громадсько-політичній і культурній діяльності, у здобутті освіти і

професійній підготовці, у праці та винагороді за неї; спеціальними заходами щодо охорони праці і здоров'я жінок, встановленням пенсійних пільг; створенням умов, які дають жінкам можливість поєднувати працю з материнством; правовим захистом, матеріальною і моральною підтримкою материнства і дитинства, включаючи надання оплачуваних відпусток та інших пільг вагітним жінкам і матерям [8]. В свою чергу, об'єктивність – це дійсне, незалежне від волі та свідомості людини, існування світу, предметів, їх властивостей і відношення; належність до об'єктивної дійсності; відповідність об'єктивній дійсності, неупередженість. Об'єктивність як категорія, що показує правильне відображення у свідомості явищ реальної дійсності, визначає такий підхід до дослідження, який однаково враховує всі обставини, які свідчать як за, так і проти обвинуваченого, виражає ставлення до збирання, перевірки й оцінки доказів, сприяє формуванню достовірних висновків по справі [9, с.116]. Згідно до даного принципу державний контроль в сфері використання інформаційних технологій має відбуватись неупереджено, в рамках визначених цілей та меж, жодним чином не виділяючи об'єкти контролю з огляду на фактори, які не ставлять предмет контрольної діяльності. Наприклад, не можна використовувати більш лояльні контрольні інструменти до організацій з великим обсягом доходу та вагомих соціальним статусом та умисно, значно суворіше ставитись до малих підприємств, установ та організацій, які знаходяться на початку своєї діяльності або не мають широких матеріально-технічних ресурсів;

- плановість та системність. Державний контроль у сфері використання ІТ повинен відбуватись постійно за рахунок регулярних перевірок та застосування інших контрольних заходів, що забезпечуватиме високий рівень правильності, обґрунтованості упровадження інформаційних технологій та дозволить оперативно реагувати на будь-які порушення в даній сфері, захистити і забезпечити права і свободи фізичних та юридичних осіб;

- прозорість контрольної діяльності. Як і будь-які публічні дії суб'єктів владних повноважень, державний контроль в сфері використання інформаційних технологій – це не закрита, секретна діяльність. Засоби, способи та заходи його здійснення повинні бути зрозумілими для всіх суб'єктів, здійснюватися офіційними представниками державних органів, а також бути оскаржуваними, у разі незгоди окремих осіб із результатами контрольної діяльності.

Таким чином, принципи державного контролю в сфері використання інформаційних технологій є важливими основами конструкції правового регулювання даної публічно-владної діяльності, якими забезпечується перебування процесу її реалізації у правовому полі, а також високий рівень ефективності та суспільної орієнтованості. Завдяки принципам державний контроль є інструментом, який сприяє упровадженню, розвитку та використанню ІТ в різних сферах життєдіяльності нашої держави, а не важелем офіційного, деструктивного впливу. А відтак, важливим завданням законодавця є розширення кола та змісту відповідних принципів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гурковський М.П., Сидор М.Я. Принципи процесуального режиму державного нагляду (контролю) у сфері діяльності МВС України. Соціально-правові студії. 2020. Випуск 3(9). С.77-83.
2. Бондаренко В.А., Єсімов С.С. Принципи організації та здійснення державного нагляду і контролю у сфері освіти. Соціально-правові студії. 2018. Випуск 2. С.32-32.
3. Гришина Н.В. Система принципів державного контролю. Вісник Харківського національного університету імені В.Н.Каразіна Серія«ПРАВО». 2017. С.72-75.
4. Ярема О.Г. Принципи державного контролю (нагляду) в контексті процесуальної діяльності контрольних органів. Юридичний науковий електронний журнал. 2021. №11. С.548-551.
5. Про застосування Конституції України при здійсненні правосуддя: постанова від 01.11.1996 №9. URL: <https://zakon.rada.gov.ua/laws/card/v0009700-96>.
6. Рішення Конституційного Суду України у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень статті 69 Кримінального кодексу України (справа про призначення судом більш м'якого покарання): рішення від 02.11.2004 №15-рп/2004. Офіційний вісник України. 2004. №45. Ст.2975.
7. Подорожній Є.Ю. Особливості юридичної відповідальності у трудовому праві України: дис... д-ра. юрид. наук : Харків: Харківський національний університет внутрішніх справ. 2016. 426 с.
8. Конституція України: закон від 28.06.1996 №254к/96-ВР. Офіційний вісник України. 2010. №72/1. Ст.2598.
9. Чурикова І.В. Всебічність, повага й об'єктивність процесуальної діяльності слідчого: дис... канд. юрид. наук : Київ: Київський національний університет внутрішніх справ. 2009. 223 с.

ДО ХАРАКТЕРИСТИКИ ФУНКЦІЙ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

Федоренко Роман Олександрович

здобувач Харківського національного університету внутрішніх справ

ORCID: <https://orcid.org/0009-0001-9560-6659>

В загальнонауковому розумінні функція – це напрям, вектор діяльності якогось механізму; обов'язкове до виконання кола завдань, тощо. В свою чергу функції публічного адміністрування в умовах воєнного стану – відносно самостійні, похідні від мети та завдань публічного адміністрування в умовах дії правового режиму воєнного стану та спрямовані на їх реалізацію напрямки юридично-визначеної діяльності публічно-владних органів. Варто

відзначити, що перелік цих функцій не є модельним, оскільки мова йде про тип діяльності не загального, а спеціального змісту, який реалізується за наявності окремого кола обставин. Зважаючи на це, до переліку останніх найбільш доцільно віднести:

- правоохоронну функцію. Це комплексний напрям публічного адміністрування, який передбачає спеціальну діяльність органів публічної влади щодо: підтримки та забезпечення правопорядку на території держави та окремих місцевостях під час дії правового режиму воєнного стану; запобігання, припинення та профілактики правопорушень; організації та забезпечення активної взаємодії між уповноваженими правоохоронними органами та іншими органами влади, підприємствами, установами та організаціями всіх форм власності, які мають ресурси та можливості сприяти виконанню цілей правоохоронної діяльності; організації ефективного та якісного виконання заходів правового режиму воєнного стану; виявлення осіб та груп, які провадять деструктивну, розвідницько-підривно діяльність, що шкодить національним інтересам та створює загрозу населенню держави;

- функцію координації. Під час дії правового режиму воєнного стану важливого значення набуває централізована та послідовна діяльність всіх суб'єктів публічного адміністрування. Досягається це за рахунок координації, тобто, єдиноначального спрямування роботи підпорядкованих суб'єктів, яка полягає у поставленні загальних управлінських цілей обов'язкових до виконання. Координація відбувається на всіх рівнях публічного адміністрування, починаючи від центрального апарату держави, та закінчуючи місцевими органами публічної влади. За рахунок цього досягається послідовність публічного адміністрування та його відповідність поточним викликам і політиці держави в умовах збройної агресії;

- контрольну функцію. Це напрям діяльності зміст якого полягає у перевірці якогось підконтрольного об'єкта на предмет його відповідності встановленим нормативним правилам, вимогам, тощо. В контексті публічного адміністрування під час воєнного стану, контроль стосується перевірки роботи суб'єктів публічної влади на предмет якості, повноти та законності виконання своїх безпосередніх повноважень, а також реалізації додаткових, покладених на них безпосередньо в рамках дії правового режиму та зумовлених викликами особливого періоду. Контрольна функція вкрай важлива, адже дозволяє забезпечити ефективну роботу всієї системи публічного адміністрування у таких складних умовах;

- функцію планування і прогнозування. Планування та прогнозування надають можливість пристосувати публічне управління до умов та обмежень воєнного стану за рахунок визначення особливостей та специфіки майбутньої діяльності та встановлення перспективних показників її результативності. Наприклад, в останні роки внаслідок проблем із електропостачанням, що виникли після обстрілів з боку російської федерації, важливим питанням роботи багатьох органів влади і місцевого самоврядування стало планування виконання своїх повноважень в умовах «блекаутів», тобто, тотальної відсутності електроенергії, а також та опалення через це [1;2];

- гуманітарно-соціальну функцію. Негативні явища, наслідком яких є уведення воєнного стану, найчастіше мають кризове значення для багатьох груп населення України. Так, збройна агресія часто викликає втрату доступу людей до ключових благ повсякденного життя, зокрема, медикаментів, продуктів, одягу та речей побутового використання. Крім цього, актуальним також є питання проживання уразливих верст населення на територіях де є загроза їх життю та здоров'ю, наприклад, дітей, осіб похилого віку в зонах ведення активних бойових дій. Зазначені питання є однією з основних прерогатив діяльності суб'єктів публічного адміністрування, які в межах своєї компетенції та повноважень повинні забезпечувати гуманітарну допомогу населенню, проводити необхідні евакуаційні заходи і таке інше;

- мобілізаційну функцію. Зазначений напрям діяльності в цілому пов'язано із реалізацією вимог Закону України «Про мобілізаційну підготовку та мобілізацію», а також інших нормативно-правових актів в цій сфері. За положеннями Закону, мобілізація – це комплекс заходів, здійснюваних з метою планомірного переведення національної економіки, діяльності органів державної влади, інших державних органів, органів місцевого самоврядування, підприємств, установ і організацій на функціонування в умовах особливого періоду, а Збройних Сил України, інших військових формувань, сил цивільного захисту - на організацію і штати воєнного часу. Мобілізація може бути загальною або частковою та проводиться відкрито чи приховано. В свою чергу, особливий період – період функціонування національної економіки, органів державної влади, інших державних органів, органів місцевого самоврядування, сил оборони і сил безпеки, підприємств, установ і організацій, а також виконання громадянами України свого конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, що настає з моменту оголошення рішення про мобілізацію (крім цільової) або доведення його до виконавців стосовно прихованої мобілізації чи з моменту введення воєнного стану в Україні або в окремих її місцевостях та охоплює час мобілізації, воєнний час і час демобілізації після закінчення воєнних дій. Організація здійснення заходів з мобілізаційної підготовки та мобілізації і контроль за здійсненням цих заходів в органах державної влади, інших державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, які мають мобілізаційні завдання (замовлення), покладаються на їх мобілізаційні підрозділи або призначених працівників з питань мобілізаційної роботи [3].

Таким чином, саме наведені вище функції, як вбачається, найбільш змістовно та повно характеризують практичний бік здійснення публічного адміністрування в умовах воєнного стану. Як недолік теоретичного та практичного характеру слід відзначити той факт, що останні не віднайшли свого законодавчого закріплення, що є суттєвою прогалиною, яка потребує усунення.

Література:

1. План на випадок блекаутів: як українські лікарні можуть працювати в умовах відключень світла?: стаття від 30.01.2024. Офіційний веб-сайт Міністерства охорони здоров'я України. URL: <https://moz.gov.ua/uk/plan-na-vipadok-blekautiv-jak-ukrainski-likarni-mozhut-pracjuvati-v-umovah-vidkljuchen-svitla>.
2. Алгоритм дій на випадок блекаутів: у Володимирі провели навчання для комунальних служб та органів управління: стаття. Офіційний сайт Володимирівської міської ради. URL: <https://volodymyrada.gov.ua/algorytm-dij-na-vypadok-blekautiv-u-volodymyri-provely-navchannya-dlya-komunalnyh-sluzhb-ta-organiv-upravlinnya/>.
3. Про мобілізаційну підготовку та мобілізацію: закон від 21.10.1993 №3543-XII. Відомості Верховної Ради України. 1993. №44. Ст.416.

РОЛЬ ЗВО МВС УКРАЇНИ У НАУКОВОМУ ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Кікінчук Василь Юрійович,

професор кафедри адміністративної діяльності ННІ № 3
Харківського національного університету внутрішніх справ
<https://orcid.org/0000-0001-7457-4507>

З давніх часів епіцентрами розвитку наукового знання ставали заклади вищої освіти. У сфері правоохоронної діяльності та підготовки висококваліфікованих юридичних кадрів особливе місце займають заклади вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських, що належать до сфери управління Міністерства внутрішніх справ України (далі – ЗВО МВС України). Наявний кадровий та матеріально-технічний потенціал дозволяє розглядати такі заклади вищої освіти як платформи постійної взаємодії наукової спільноти та практичних підрозділів Національної поліції України.

Законодавство України про вищу освіту визначає, що наукова і науково-технічна діяльність у закладах вищої освіти є невід'ємною частиною освітнього процесу і здійснюється з метою інтеграції наукової, навчальної та виробничої діяльності в системі вищої освіти. Інтеграція науково-дослідницької діяльності здобувачів освіти у систему вищої освіти передбачає орієнтацію навчання на формування та розвиток дослідницьких умінь здобувачів освіти шляхом залучення їх до науково-дослідної роботи під керівництвом викладача, а також самостійно [1, с. 68]. Це включає розробку коротких наукових повідомлень, щоб навчитися організовувати дослідницькі завдання за встановлений проміжок часу. Крім того, вдосконалюються ораторські навички. Здобувачі освіти набувають інших

здібностей, таких як здатність протистояти сумнівам і підвищення впевненості у собі [1, с. 70].

Курсанти та студенти закладів вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських, мають змогу на безоплатній основі опублікувати власні тези доповідей на міжнародних і всеукраїнських наукових конференціях і круглих столах, отримати доступ до міжнародних програм, наукометричних баз даних, наукових гуртків, товариств, зустрічей, присвячених їх розвитку як юних науковців. Слід додати, що переважна більшість таких заходів і зустрічей проводяться у співпраці з практичними підрозділами Національної поліції України, у тому числі тими, що виконують службово-бойові завдання із захисту територіальної цілісності держави в умовах воєнного стану.

Як стверджують дослідники, наукова робота студентів-юристів є невід'ємною частиною освітнього процесу у закладах вищої освіти. Дослідницькі навички є важливими для студентів-юристів з огляду на те, що у своїй професійній діяльності вони стикаються зі складними завданнями та питаннями, коли йдеться про необхідність самостійно засвоювати нові знання, знаходити аргументи, у тому числі наукові, обґрунтовувати свою правову позицію та викладати її в усній та/або письмовій формі [2, с. 21].

Слід додати, що майбутнім поліцейським володіння методологією наукової діяльності дозволяє грамотно складати будь-який процесуальний документи, давати вичерпну письмову чи усну відповідь на запити адвокатів, критично аналізувати ситуацію у професійній діяльності, проявляти високий рівень комунікативної компетентності, що передбачає налагодження взаємодії з широким колом суб'єктів, підтримання з ними конструктивної співпраці та довірливих відносин.

Водночас в ході аналізу наукового забезпечення діяльності Національної поліції України в умовах воєнного стану неможливо оминати увагою руйнівний вплив на нього постійних ракетних і артилерійських обстрілів, що проявляється в колосальних руйнуваннях інфраструктури, приміщень кафедр і науково-дослідних лабораторій, вимушеному переміщенні окремих закладів вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських.

При цьому окремі науковці впевнені, що якість освіти залежить не стільки від форм навчання, скільки від науково-методичного забезпечення викладачами навчальних дисциплін, використання ними новітніх форм і методів навчання, відповідності змісту тем, що розглядаються, сучасним тенденціям і подіям, що відбуваються у світі; дистанційне навчання сприймається студентами як тимчасова незручність, до якої вони успішно адаптувалися завдяки можливості опанувати електронні курси та використовувати різні інтернет-платформи для спілкування з викладачами та колегами [3, с. 105]. Дійсно, як засвідчує досвід окремих закладів вищої освіти, що суттєво постраждали від бойових дій, за умови активного використання цифрових продуктів та максимальної самовіддачі науково-

педагогічного складу можливо продовжувати та навіть прискорювати темпи наукової діяльності.

Таким чином, наукове забезпечення діяльності Національної поліції України в умовах воєнного стану багато в чому пов'язане з діяльністю закладів вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських, їх кадровим, матеріально-технічним потенціалом, залученістю здобувачів освіти-майбутніх поліцейських до проведення наукових досліджень, постійною співпрацею з практичними підрозділами та постійним генеруванням новітніх ідей, зокрема у сфері адміністративно-правової доктрини.

Література:

1. Melnyk V., Melnyk R., Dekhtiarova O., Upatova I., Boiko-Buzyl Y. Scientific activity of students as a component of the educational process. *Ad alta-journal of interdisciplinary research*. 2021. № 11 (2). pp. 68-71,
2. Riabovol L., Harust Y., Dzhafarova O., Sobol Y. Students' scientific activity as a component of the lawyers' professional training. *Asia Life Sciences*. 2019. № 2. pp. 21-43.
3. Klishevych N., Pavliuk R., Sulitskyi V., Liakh T. Education in the conditions of pandemic and war: Ukrainian students' representative opinions. *E-Learning in the Transformation of Education in Digital Society*. 2022. № 14. pp. 105-119.

ОСОБЛИВОСТІ ПРОТИДІЇ КОРУПЦІЇ У СЛІДЧИХ ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Музичук Едуард Олександрович,

науковий співробітник

Науково-дослідної лабораторії з проблем
правового забезпечення діяльності поліції
та протидії злочинності

Навчально-наукового інституту № 2

Харківського національного
університету внутрішніх справ

e-mail: edmuzychuk@gmail.com;

ORCID: <https://orcid.org/0009-0000-8695-8807>

Протидія корупції в слідчих підрозділах Національної поліції України є надзвичайно важливою для забезпечення правопорядку та підвищення довіри до правоохоронної системи. Корупційна діяльність співробітників слідчих підрозділів Національної поліції України, може негативно впливати на результативність розслідувань, порушувати права громадян і перешкоджати ефективному виконанню службових обов'язків. Тому необхідність системної протидії цій корупції стає очевидною.

Однією з основних складових протидії корупції є наявність нормативно-правової бази. Протидія корупційним проявам у Національній поліції здійснюється відповідно до кількох важливих законодавчих актів. Закон України "Про запобігання корупції" визначає основні принципи антикорупційної політики, зокрема обов'язкове декларування майна, доходів та витрат державних службовців, що дозволяє відстежувати можливі невідповідності в доходах. Також Кримінальний кодекс України передбачає кримінальну відповідальність за корупційні злочини, такі як отримання неправомірної вигоди або зловживання службовим становищем. Закон України "Про Національну поліцію" регулює діяльність поліцейських і містить положення про запобігання корупційним проявам серед особового складу.

Інституційний контроль у цій сфері здійснюється через кілька ключових органів і структур. Управління внутрішньої безпеки НПУ займається виявленням та розслідуванням випадків корупції серед поліцейських. Важливу роль відіграють Спеціалізована антикорупційна прокуратура (САП) та Національне антикорупційне бюро України (НАБУ), які мають повноваження проводити розслідування стосовно корупційних дій серед працівників поліції, особливо вищих чинів. Крім того, дисциплінарні комісії в межах НПУ здійснюють внутрішні розслідування і можуть накладати санкції на порушників.

Запобігання корупції також включає декілька важливих механізмів. Зокрема, обов'язкове декларування доходів є інструментом контролю за майновим станом слідчих. Перевірки доброчесності, що включають тестування на знання законодавства та оцінку моральних якостей, сприяють відбору професійно підготовлених і етично надійних працівників. Атестаційні комісії регулярно проводять переатестації поліцейських, щоб відстежувати відповідність їхніх професійних і етичних якостей.

Окремо варто зазначити важливість навчання та підвищення обізнаності поліцейських. Регулярні антикорупційні тренінги та семінари для слідчих підрозділів покликані підвищити їхню обізнаність щодо корупційних ризиків і способів запобігання їм. Також психологічні тренінги допомагають слідчим протистояти спокусам і зберігати етичні стандарти під час виконання службових обов'язків.

Цифровізація процесів є ще одним важливим інструментом протидії корупції. Впровадження систем електронного документообігу та автоматизованих баз даних значно знижує можливість корупційних проявів, адже мінімізує людський фактор у роботі з інформацією. Крім того, система електронного декларування доходів та майна підвищує прозорість діяльності слідчих, що ускладнює здійснення корупційних дій.

Громадський контроль та взаємодія з суспільством також відіграють важливу роль у боротьбі з корупцією. Громадські організації та медіа активно займаються розслідуванням і виявленням фактів корупції, що сприяє прозорості правоохоронної системи. Важливим інструментом є інформаційна відкритість та доступність результатів розслідувань корупційних правопорушень, які публікуються на офіційних ресурсах НПУ. Громадяни

мають можливість повідомляти про випадки корупції через гарячу лінію або онлайн-платформи, що дає змогу оперативно реагувати на корупційні прояви.

Незважаючи на наявність усіх зазначених механізмів, існують і певні виклики в протидії корупції в слідчих підрозділах НПУ. Одним із них є низька заробітна плата слідчих, що може стимулювати до пошуку додаткових джерел доходів, у тому числі незаконних. Також соціальний тиск, взаємозалежність між різними структурами та явище "кругової поруки" можуть створювати перешкоди для розслідування корупційних справ всередині поліції. Нарешті, обмежені ресурси та технічна база ускладнюють діяльність слідчих підрозділів, що іноді сприяє розвитку корупційних практик.

Таким чином, протидія корупції в слідчих підрозділах Національної поліції України є багатокомпонентним процесом, що включає нормативно-правові, організаційні, соціальні та технічні заходи. Ефективність боротьби з корупцією залежить від взаємодії внутрішніх механізмів контролю, громадського нагляду та постійного вдосконалення професійних навичок поліцейських.

ПОРІВНЯЛЬНИЙ АНАЛІЗ НЕКОМЕРЦІЙНИХ МОДЕЛЕЙ ДЕТЕКТОРІВ ОБЛИЧ ІЗ ГЛИБИННИМ НАВЧАННЯМ

Носов Віталій Вікторович

кандидат технічних наук доцент

професор кафедри протидії кіберзлочинності

Навчально-наукового інституту №4

Харківського національного університету внутрішніх справ

Правоохоронними органами України станом на 31 січня 2025 року було відкрито 140956 кримінальних проваджень за фактами злочинів, скоєних військовими рф та їх пособниками на території України [1]. Для притягнення до відповідальності воєнних злочинців доцільна розробка і впровадження автоматизованої системи розшуку людей на основі використання даних з відкритих джерел (АСПЛ-OSINT), яка може складатися із трьох взаємопов'язаних модулів:

- накопичення, аналізу та систематизації даних;
- автоматичного пошуку інформації у відкритих джерелах за вихідними даними;
- розпізнавання облич у фото- та відео-матеріалі.

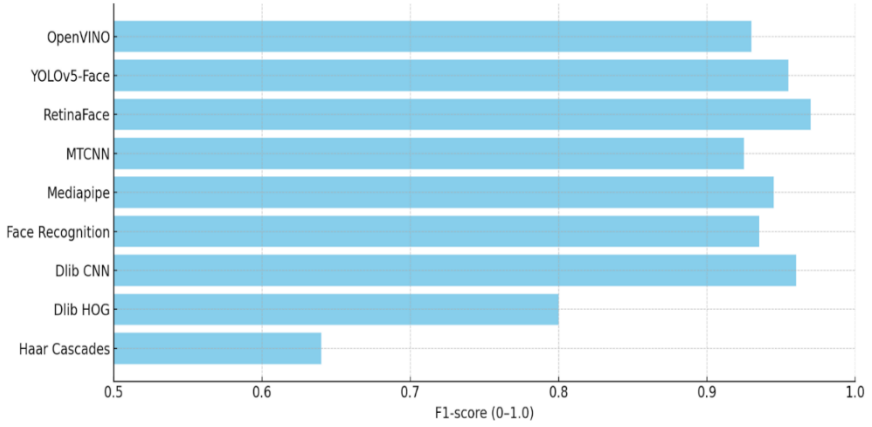
Модуль розпізнавання облич у фото- та відео-матеріалі АСПЛ-OSINT має включати конвеєри (pipelines) системи розпізнавання облич із чотирма стадіями [2]:

- виявлення облич на вихідних графічних даних (face detection) - локалізація та ізоляція людських облич на зображенні або у відеокадрі із формуванням обмежувальних рамок (bounding boxes) навколо кожного виявленого обличчя;
- вирівнювання облич (face alignment) – ідентифікація ключових точок обличчя (facial landmarks) та їх трансформація в стандартне положення та орієнтацію;
- представлення обличчя вектором (face embedding) - за допомогою загорткової нейронної мережі (Convolutional Neural Networks, CNN) вивчаються ідентифіковані ключові точки обличчя, вилучаються краї/текстури із наступним їх представленням числовим вектором визначеної довжини (ембедінгом);
- верифікація/ідентифікація (face matching) - здійснюється або порівняння двох ембедінгів облич для визначення належності одній і тій самій особі, або порівняння запитуваного обличчя з базою даних відомих ембедінгів облич для знаходження найближчої відповідності.

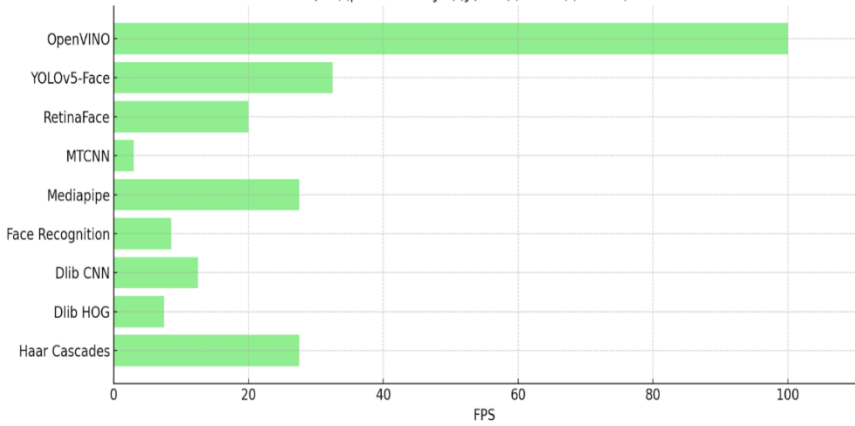
Аналіз результатів актуальних досліджень дозволив виділити наступні некомерційні моделі детекторів облич, що використовують моделі глибинного навчання і реалізовані як відкриті бібліотеки або фреймворки у Python: Haar Cascades [3,4], Dlib HOG [5,6,7], Dlib CNN [5,6,7], Face Recognition (Dlib HOG + CNN) [7], Mediapipe [7], MTCNN [8], RetinaFace [9], YOLOv5-Face [10], OpenVINO Face Detection [11], та здійснити їх порівняння за наступними параметрами (рис. 1):

- F1-score:
 - $$F1\text{-score} = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall};$$
 - $$Precision = \frac{\text{Кількість правильно виявлених облич (TP)}}{\text{Усі знайдені обличчя (TP + FP)}},$$
 TP (True Positives) – виявленні справжні обличчя; FP (False Positives) - виявленні несправжні обличчя;
 - $$Recall = \frac{\text{Кількість правильно виявлених облич (TP)}}{\text{Загальна кількість справжніх облич (TP + FN)}},$$
 FN (False Negatives) – не виявленні справжні обличчя;
- FPS (Frames Per Second) - кількість зображень (кадрів), що можуть оброблятися за секунду;
- Latency — затримка на обробку 1 зображення.

F1-score моделей детекції облич



FPS (кадрів за секунду) моделей детекції облич



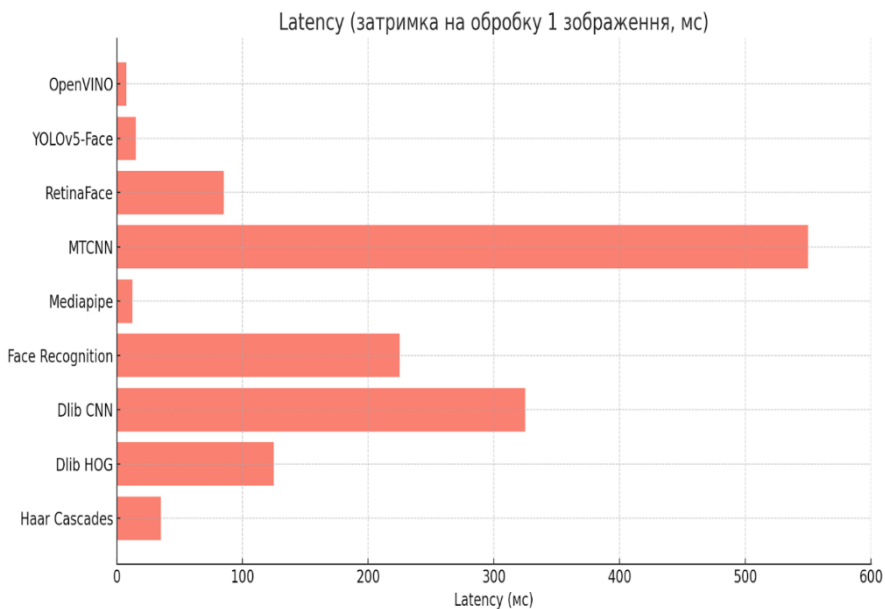


Рис. 1. Діаграми порівняння моделей детекторів облич за параметрами F1-score, FPS, Latency

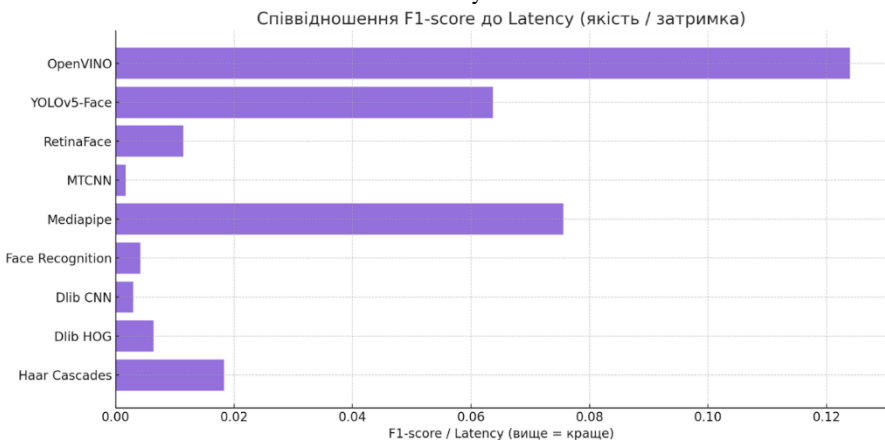


Рис. 2. Діаграма порівняння моделей детекторів облич за співвідношенням якість/затримка

Моделі детекторів облич OpenVINO, YOLOv5-Face і Mediapipe мають найкраще співвідношення якість/затримка (рис.2), що обґрунтовує саме їх застосування у реалізації модуля розпізнавання облич у фото- та відео-

матеріалі АСПЛ-OSINT як підсистеми, що може функціонувати у режимі реального часу.

Список використаних джерел

1. Офіційний вебсайт МВС України. Російські воєнні злочини: оновлені дані станом на 31 січня 2025 року. URL: <https://mvs.gov.ua/news/zlocini-vcineni-viiskovimi-rf-pid-cas-povnomasstabnogo-vtorgnennia-v-ukrayinu-stanom-na-31012025> (дата звернення 17.05.2025).

2. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, Deepface: Closing the gap to human-level performance in face verification - meta research, Jun. 2014. URL: <https://research.facebook.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/> (дата звернення 17.05.2025).

3. OpenCV: Cascade Classifier. Open Source Computer Vision. URL: https://docs.opencv.org/4.x/db/d28/tutorial_cascade_classifier.html (дата звернення 17.05.2025).

4. Antipona, Clarence & Magsino, Romeo. (2024). An Enhancement of Haar Cascade Algorithm Applied to Face Recognition for Gate Pass Security. URL: <http://dx.doi.org/10.13140/RG.2.2.34675.75045> (дата звернення 17.05.2025).

Adrian Rosebrock. Face recognition with OpenCV, Python, and deep learning. URL: <https://pyimagesearch.com/2018/06/18/face-recognition-with-opencv-python-and-deep-learning/> (дата звернення 17.05.2025).

5. Hetvi Gunjan Shah1, Vraj Bhavesh Suthar, Shital P. Thakkar, Vinay M. Thumar. Real-time Performance Comparison of Face Detection Algorithms using Raspberry Pi. (2024). International Research Journal on Advanced Engineering Hub (IRJAEH), 2(10), 2440-2445. URL: <https://doi.org/10.47392/IRJAEH.2024.0334> (дата звернення 17.05.2025).

6. Lin, Chun-Ling & Huang, Yi-Huai. (2022). The Application of Adaptive Tolerance and Serialized Facial Feature Extraction to Automatic Attendance Systems. Electronics. URL: <http://dx.doi.org/10.3390/electronics11142278> (дата звернення 17.05.2025).

7. Zamir, Muhammad & Ali, Nouman & Naseem, Amad & Frasteen, Areeb & Zafar, Bushra & Assam, Muhammad & Othman, Mahmoud & Attia, El-Awady. (2022). Face Detection & Recognition from Images & Videos Based on CNN & Raspberry Pi. Computation. URL: <http://dx.doi.org/10.3390/computation10090148> (дата звернення 17.05.2025).

8. Zhang, Ning & Luo, Junmin & Gao, Wufi. (2020). Research on Face Detection Technology Based on MTCNN. 154-158. URL: <https://doi.org/10.1109/ICCNEA50255.2020.00040> (дата звернення 17.05.2025).

9. Jiankang Deng, Jia Guo, Yuxiang Zhou, Jinke Yu, Irene Kotsia, Stefanos Zafeiriou. RetinaFace: Single-stage Dense Face Localisation in the Wild/ Computer Vision and Pattern Recognition (cs.CV). URL: <https://doi.org/10.48550/arXiv.1905.00641> (дата звернення 17.05.2025).

10. Delong Qi, Weijun Tan, Qi Yao, Jingfeng Liu. YOLO5Face: Why Reinventing a Face Detector/ Computer Vision and Pattern Recognition (cs.CV). URL: <https://doi.org/10.48550/arXiv.2105.12931> (дата звернення 17.05.2025).
11. Brown, Dane. (2021). Mobile Attendance based on Face Detection and Recognition using OpenVINO. 1152-1157. <https://doi.org/10.1109/ICAIS50930.2021.9395836> (дата звернення 17.05.2025).

ЗМІСТ

ШАНОВНІ УЧАСНИКИ КОНФЕРЕНЦІЇ!	3
АНАЛІТИЧНА ДІЯЛЬНІСТЬ ЯК СКЛАДОВА КРИМІНАЛЬНОЇ РОЗВІДКИ	4
Албул Сергій Володимирович	4
ОКРЕМІ ПИТАННЯ ПОШУКУ ВІДЕОКОНТЕНТУ ТА ФОТОМАТЕРІАЛІВ У DARK WEB: РИЗИКИ ТА ПРАВОВІ АСПЕКТИ	7
Афонін Дмитро Сергійович	7
ЗАСТОСУВАННЯ АРІ ДЛЯ ОТРИМАННЯ ДАНИХ З СОЦІАЛЬНИХ МЕРЕЖ	10
Бажура Вікторія Вікторівна	10
СЕКСУАЛЬНЕ НАСИЛЬСТВО ЯК ВОЄННИЙ ЗЛОЧИН	12
Березовська Вероніка В'ячеславівна	12
Резніченко Г. С.	12
OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ	15
Богдан Віталій Петрович	15
Свинаренко Ю. П.	15
ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT	18
Бойченко Вікторія Юріївна	18
Поляков Є. В.	18
АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ТА НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ	21
Бойчук Олександра Олександрівна	21
Тригуб С. М.	21
ІНСТИТУЦІЙНЕ СТАНОВЛЕННЯ ТА ФОРМУВАННЯ СТАНДАРТІВ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ	25
Боцу Тетяна Петрівна	25
Тригуб С. М.	25
РОЛЬ OSINT У СТВОРЕННІ ДОКАЗОВОЇ БАЗИ ЩОДО ВОЄННИХ ЗЛОЧИНІВ	27
Волобєєв А. О.	27
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ: ВИКЛИКИ, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ	30
Головкін Сергій Вікторович	30
КРИМІНАЛЬНИЙ АНАЛІЗ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: СПЕЦИФІКА ТА СУЧАСНІ ВИКЛИКИ	33
Григор'єва Валерія Михайлівна	33
Албул С. В.	33
OSINT – ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ	35
Єйбог Олександр Ігорович	35
Тригуб С. М.	35
РОЛЬ OSINT У ВИЯВЛЕННІ ДЕЗІНФОРМАЦІЇ ТА ЦИФРОВИХ ЗАГРОЗ: ІНСТРУМЕНТИ Й АНАЛІТИЧНІ ПІДХОДИ	38

Єфімкіна Ірина Миколаївна	38
Моргунова Т. І.....	38
OSINT – ТЕХНОЛОГІЇ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ.....	41
Журавель Андрій Владиславович	41
Поляков Є. В.	41
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ	44
Калугін Володимир Юрійович	44
АЛГОРИТМ ВИКОРИСТАННЯ МЕТОДОЛОГІЇ OSINT	46
Калугін Володимир Юрійович	46
Янковий Микола Олександрович	46
ДЕЯКІ ПИТАННЯ ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ У	49
ДІЯЛЬНОСТІ КРИМІНАЛЬНОГО АНАЛІТИКА	49
Кіреєва Ольга Сергіївна	49
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ	53
Коренчук Артем Віталійович.....	53
Поляков Є. В.	53
МЕТОДИ ФІКСАЦІЇ ТА ЗБЕРЕЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ	57
Кочин Владислав Дмитрович.....	57
Онищенко Ю. М.	57
OSINT ЯК ІНСТРУМЕНТ ПОПЕРЕДЖЕННЯ КІБЕРЗАГРОЗ У ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ	59
Кочман Костянтин Павлович.....	59
РОЛЬ OSINT У РОЗКРИТТІ КІБЕРЗЛОЧИНІВ ТА ІДЕНТИФІКАЦІЇ КІБЕРЗЛОЧИНЦІВ.....	63
Кривошея Данило Григорович	63
Рижков Едуард Володимирович.....	63
ІНТЕГРАЦІЙНИЙ ПОТЕНЦІАЛ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ПРИВАТНОГО СЕКТОРУ У МЕХАНІЗМАХ ПРЕВЕНЦІЇ ТА РОЗКРИТТЯ ПРАВОПОРУШЕНЬ.....	66
Лісніченко Дмитро	66
ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ.....	69
Лозован Катерина Валеріївна	69
Тригуб С. М.	69
АЛГОРИТМ ОТРИМАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В УМОВАХ ПОТЕНЦІЙНОГО САМОЗНИЩЕННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) СЛІДІВ	71
Майданевич Леонід Олександрович	71
Кирбят'єв Олег Олександрович.....	71
Тарасюк Микола Борисович	71

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ МЕРЕЖНИХ СПІВТОВАРИСТВ.....	76
Манжай Олександр Володимирович	76
АНАЛІЗ ЦИФРОВИХ ПЛАТФОРМ У СФЕРІ НЕЗАКОННОГО ОБІГУ НАРКОТИКІВ ДЛЯ УДОСКОНАЛЕННЯ МЕТОДІВ ДОСЛІДЖЕННЯ НАРКОТИЧНИХ ЗАСОБІВ	81
Матвеевський Олег Володимирович.....	81
Афонін Д. С.	81
OSINT ЯК ДЖЕРЕЛО ДОКАЗІВ У МІЖНАРОДНОМУ КРИМІНАЛЬНОМУ ПРОЦЕСІ 83	
Меликов Руслан	83
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК СКЛАДОВА ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ	87
Михайлішина Анастасія Русланівна	87
Албул С. В.	87
ВИКОРИСТАННЯ OSINT ДЛЯ МОНИТОРИНГУ ДАРКНЕТУ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ	89
Моргунова Тетяна Іванівна	89
АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT У ВИЯВЛЕННІ, ДОКУМЕНТУВАННІ ТА РОЗСЛІДУВАННІ НЕЗАКОННОГО ЗБУТУ ПСИХОАКТИВНИХ РЕЧОВИН	93
Морозов Д.А.....	93
Бондар В.С.	93
ОСОБЛИВОСТІ ВИКОРИСТАННЯ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ (OSINT) У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ	98
Мудрецька Г.	98
ІНСТРУМЕНТИ OSINT У ВИЯВЛЕННІ ФЕЙКОВИХ АКАУНТІВ І БОТ-МЕРЕЖ У СОЦІАЛЬНИХ МЕДІА	101
М'ясоєдова Анастасія Григорівна.....	101
Моргунова Тетяна Іванівна	101
ПЕРСПЕКТИВИ РОЗВИТКУ АНАЛІТИЧНОГО СУПРОВОДУ ПРОТИДІЇ НАРКОЗЛОЧИННОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ.....	105
Овсянюк Дмитро Іванович	105
АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ТА НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ	109
Омельян Ілля Федорович.....	109
Тригуб С. М.	109
СТВОРЕННЯ ПЕРЕДУМОВ ДЛЯ ЦИФРОВОГО ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ТА ПІДГОТОВКИ АНАЛІТИКІВ З МЕТОЮ ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ ЗАВДАНЬ З ВИЯВЛЕННЯ ТА РОЗШУКУ	

АКТИВІВ: АКТУАЛЬНІСТЬ І НАГАЛЬНІСТЬ СЬОГОДЕННЯ ТА ПИТАННЯ МАЙБУТНЬОГО	111
Паламарчук Іван Васильович.....	111
ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT... 115	115
Парушев Данило Михайлович.....	115
Поляков Євген Валентинович.....	115
«SSL STRIPPING» ТА «ARP POISONING» ЯК МЕТОДИ ОТРИМАННЯ ДОКАЗОВОЇ ІНФОРМАЦІЇ: ПРОБЛЕМНІ АСПЕКТИ.....	118
Пастух Дмитро Сергійович	118
Албул С. В.	118
ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT... 122	122
Перовський Микита Михайлович	122
Поляков Є. В.	122
СУЧАСНІ ПОТУЖНІ ІНСТРУМЕНТИ OSINT.....	123
Пядишев В. Г.....	123
ВИКОНАННЯ ОБОВ'ЯЗКУ ЩОДО ЗАХИСТУ ВІТЧИЗНИ, НЕЗАЛЕЖНОСТІ ТА ТЕРИТОРІАЛЬНОЇ ЦІЛІСНОСТІ УКРАЇНИ ЯК ОБСТАВИНА, ЩО ВИКЛЮЧАЄ КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ	127
Флоренко Ганна Олександрівна	127
Резніченко Г.С.....	127
ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT У ПРОТИДІЇ ОРГАНІЗОВАНИЙ ЗЛОЧИННОСТІ В УКРАЇНІ	130
Санакоев Дмитро Борисович	130
OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТОВАННІ ВОЄННИХ ЗЛОЧИНІВ	135
Сінчук Михайло Сергійович.....	135
Свинаренко Ю. П.....	135
ІНСТИТУЦІЙНЕ СТАНОВЛЕННЯ ТА ФОРМУВАННЯ СТАНДАРТІВ КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ	138
Стратулат Аріяна Русланівна.....	138
Тригуб С. М.	138
АЛГОРИТМ OSINT-АНАЛІЗУ ПУБЛІЧНОГО КОНТЕНТУ З МЕТОЮ ВИЯВЛЕННЯ ЗЛОЧИНІВ У СФЕРІ НЕЗАКОНОГО ОБІГУ НАРКОТИКІВ (СТ. 307 КК УКРАЇНИ)	141
Токолов Олександр	141
Афонін Дмитро	141
РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ	143
Толмачевська Єлизавета Сергіївна	143
Албул С. В.	143
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ .. 147	147
Толмаченко Єгор	147
Свинаренко Юрій Павлович	147

ЗНАЧЕННЯ OSINT-ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ	150
Третяк Софія Вікторівна.....	150
Квашук Олександр Дмитрович.....	150
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ ..	153
Трошев Андрій Дмитрович	153
Свинаренко Юрій Павлович	153
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ УКРАЇНИ.....	157
Федорощевська Анна Валеріївна	157
Свинаренко Ю. П.....	157
ВИКОРИСТАННЯ МЕТОДІВ OSINT З МЕТОЮ РЕАЛІЗАЦІЇ ЗАВДАНЬ СИСТЕМИ API/PNR	159
Фігура Віталій Олегович	159
Філіппов Станіслав Олександрович.....	159
ВИКОНАННЯ ОБОВ'ЯЗКУ ЩОДО ЗАХИСТУ ВІТЧИЗНИ, НЕЗАЛЕЖНОСТІ ТА ТЕРИТОРІАЛЬНОЇ ЦІЛІСНОСТІ УКРАЇНИ ЯК ОБСТАВИНА, ЩО ВИКЛЮЧАЄ КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ	162
Флоренко Ганна Олександрівна	162
Резніченко Г.С.....	162
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗАГРОЗАМ: АНАЛІЗ ТА ПЕРСПЕКТИВИ.....	165
Форос Ганна Володимирівна	165
ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT...	168
Хомік Софія Василівна	168
Тригуб С. М.	168
ПРОБЛЕМИ ІМПЛЕМЕНТАЦІЇ БУДАПЕШТСЬКОЇ КОНВЕНЦІЇ В УКРАЇНСЬКЕ ЗАКОНОДАВСТВО	172
Чорна Марина Василівна.....	172
Беліков Костянтин Аркадійович.....	172
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ ТА КІБЕРБЕЗПЕКИ УКРАЇНІ	175
Шавлай Максим Олександрович.....	175
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ УДОСКОНАЛЕННЯ OSINT- АНАЛІТИКИ.....	178
Шипрінський Нікіта Олегович	178
Моргунова Тетяна Іванівна	178
БЕЗПЕКА У КІБЕРСФЕРІ	182
Шоломіцький Артур Аркадійович	182
Гончаренко Ольга Анатоліївна.....	182
СУЧАСНИЙ СТАН ВЗАЄМОДІЇ ДЕРЖАВНИХ ОРГАНІВ ТА ГРОМАДСЬКИХ ОРГАНІЗАЦІЙ У ПРОЦЕСІ НАДАННЯ СОЦІАЛЬНОЇ ДОПОМОГИ.....	185
Алфьоров Сергій Юрійович.....	185

ДО ХАРАКТЕРИСТИКИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ МЕДІАТОРІВ В УКРАЇНІ	188
Глущенко Євген Володимирович	188
СОЦІАЛЬНА ІНКЛЮЗИВНІСТЬ, ЯК ВАЖЛИВИЙ ЧИННИК НЕОБХІДНОСТІ ДІДЖИТАЛІЗАЦІЇ СФЕРИ НАДАННЯ АДМІНІСТРАТИВНИХ ПОСЛУГ В УКРАЇНІ	191
Грачов Єгор Олегович	191
ДО ХАРАКТЕРИСТИКИ КЛЮЧОВИХ ПРИНЦИПІВ ЗДІЙСНЕННЯ ДЕРЖАВНОГО КОНТРОЛЮ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ	194
Пичурин Артем Анатолійович	194
ДО ХАРАКТЕРИСТИКИ ФУНКЦІЙ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ	197
Федоренко Роман Олександрович	197
РОЛЬ ЗВО МВС УКРАЇНИ У НАУКОВОМУ ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ	200
Кікінчук Василь Юрійович	200
ОСОБЛИВОСТІ ПРОТИДІЇ КОРУПЦІЇ У СЛІДЧИХ ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ	202
Музичук Едуард Олександрович	202
ПОРІВНЯЛЬНИЙ АНАЛІЗ НЕКОМЕРЦІЙНИХ МОДЕЛЕЙ ДЕТЕКТОРІВ ОБЛИЧ ІЗ ГЛИБИННИМ НАВЧАННЯМ	204
Носов Віталій Вікторович	204

**МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ**

**«Кримінальний аналіз і кібербезпека:
об'єднання зусиль для нових викликів»**

23 травня 2025 р.

Підписано до друку 23.05.2024. .Формат 60x84/16 Папір офсетний.

Гарн. «Times New Roman». Друк цифровий. Ум. друк .арк. 12,56

Надруковано з готового оригінал-макета.

Наклад 30 прим.

Видавництво ОДУВС

м. Одеса, вул. Успенська, 1

Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.