виступають основою для визначення пріоритетів, стратегічних та оперативних цілей в галузі попередження і припинення злочинності та інших загроз безпеці. Це дає змогу обґрунтовано розподіляти ресурси із урахуванням напрямів і сфер активності серійних злочинців, організованих злочинних угруповань та кримінального середовища.

Отже, кримінальна аналітика передбачає насамперед виявлення, визначення пріоритетності для втручання у злочинну діяльність з метою «мінімізації ризику» для суспільства.

**Список використаних джерел**

1. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

2. Про затвердження Положення про Департамент кримінального аналізу Національної поліції України : наказ Національної поліції України від 29.12.2019 р. № 1354 (зі змінами).

***Темрієнко Валерій Дмитрович,***
старший викладач кафедри
оперативно-розшукової діяльності
та розкриття злочинів ННІ № 2
Харківського національного університету
внутрішніх справ

## ПІДГОТОВКА АНАЛІТИКІВ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА ВОЄННОГО СТАНУ

Еволюція безпекового середовища у фазі інтенсивного воєнного стану та глобальної цифровізації докорінно змінює архітектуру правоохоронної діяльності. Сучасний етап характеризується не просто збільшенням, а експоненційним зростанням обсягів неструктурованих даних, які безупинно генеруються як у фізичному, так і у віртуальному просторах. У цих складних умовах оперативні та слідчі підрозділи неминуче стикаються з проблемою «інформаційного перевантаження», коли критично важливі докази можуть загубитися у терабайтах цифрового шуму. Саме тому стратегічним пріоритетом державного рівня стає підготовка фахівців нової формації,

здатних здійснювати швидкий збір, систематизацію та глибокий аналіз даних. Як справедливо зазначають фахівці, кінцевою метою такої складної роботи є перетворення сирих масивів інформації на якісний інформаційний продукт, що слугуватиме надійним підґрунтям для прийняття виважених управлінських та процесуальних рішень [1, с. 42]. У цьому широкому контексті кримінальний аналіз поступово виходить за межі суто допоміжної функції та перетворюється на ядро протидії злочинності. Сучасна правоохоронна доктрина розглядає його як безперервний процес дослідження інформації про кримінальні явища, осіб та події, спрямований на проактивну підтримку правоохоронних органів у їхній щоденній діяльності [2, с. 24].

Тотальна міграція сучасного криміналітету в кіберпростір, використання анонімних мереж та інфраструктури криптовалют докорінно змінюють вимоги до кваліфікації аналітиків. Як слушно зазначає М. В. Карчевський, базовою компетенцією стає здатність до глибокої обробки цифрових доказів у середовищі автоматизованих систем кримінального аналізу, що вимагає від фахівця принципово нового рівня цифрової грамотності [3, с. 71]. Цей технологічний зсув логічно зумовлює потребу в новій, міждисциплінарній парадигмі підготовки. Н. П. Свиридюк та Ю. Р. Кардашевський аргументовано доводять, що вона має органічно синтезувати класичну юриспруденцію з інженерією даних, охоплюючи всі рівні аналітичної роботи: стратегічний, оперативний та тактичний [4, с. 56]. Відповідно, як підсумовує у своїх дослідженнях В. І. Василинчук, фокус навчання неминуче зміщується від простого накопичення даних до опанування методик глибинного інформаційного пошуку, жорсткої верифікації фактів та алгоритмічної побудови структурованих аналітичних звітів [5, с. 104].

Практичним інструментом реалізації такого глибинного пошуку в сучасних умовах стає розвідка на основі відкритих джерел (OSINT) та соціальних медіа (SOCMINT). Досліджуючи проблеми цифровізації, Д. І. Овсянюк переконливо доводить, що інтеграція цих технологій є одним із найпотужніших векторів інноваційної підготовки. За його висновками, автоматизована агрегація даних із відкритих корпоративних баз та геоінформаційних платформ дозволяє підрозділам кримінального аналізу формувати масив первинної орієнтуючої інформації. На відміну від роботи з державними реєстрами з

обмеженим доступом, яка вимагає наявності підстав згідно з п. 1 ч. 1 ст. 8 Закону України «Про оперативно-розшукову діяльність» (заведення ОРС), моніторинг відкритих джерел критично мінімізує ризики розшифровки інтересу правоохоронців до початку застосування класичних оперативно-розшукових заходів [6, с. 56]. Проте ефективність OSINT-розвідки прямо залежить від здатності фахівця розкривати приховані зв'язки. Тому слід підтримати позицію В. П. Захарова та К. Ю. Ісмайлова щодо необхідності опанування майбутніми аналітиками методів відстеження цифрових слідів, аналізу метаданих та парсингу відкритих баз [7, с. 224], з обов'язковим урахуванням того факту, що прямої норми щодо процесуального статусу результатів парсингу не існує, і відповідно до ч. 2 ст. 84 КПК України вони не є самостійним джерелом доказів до моменту їх легалізації.

Зібрані масиви даних потребують надзвичайно швидкої інтерпретації, що набуває особливої ваги в умовах правового режиму воєнного стану. У цьому руслі доречно навести позицію С. В. Албула та В. В. Шендрика, які зауважують, що гібридні загрози вимагають від правоохоронної системи переходу від ретроспективної констатації фактів до предиктивної (прогнозної) аналітики. Сучасний аналітик мусить вміти моделювати ймовірні сценарії дій злочинних угруповань, виявляти аномалії в поведінкових патернах фігурантів та математично розраховувати їхній деструктивний вплив на безпеку регіону [8, с. 109, 121]. Зважаючи на складність обробки значних масивів неструктурованих даних, Д. І. Овсянюк зазначає, що технології штучного інтелекту та обробки великих масивів даних (Big Data) виступають важливим мультиплікатором ефективності, здатним автоматизувати виявлення неочевидних закономірностей [6, с. 146]. Логічним завершенням формування цієї архітектури підготовки, спираючись на дослідження А. С. Тімошина, є впровадження практичних модулів із використання нейромереж для семантичного аналізу текстів [9, с. 11]. При цьому необхідно враховувати, що прямої норми щодо процесуального закріплення автоматизовано згенерованих зведень не існує, і відповідно до вимог КПК України такі матеріали можуть слугувати виключно як орієнтуюча інформація в межах оперативно-розшукової діяльності.

Проте будь-який інноваційний інструментарій, чи то алгоритми машинного навчання, чи то парсери метаданих, залишається лише теоретичним концептом без жорсткого

закріплення в умовах, що максимально імітують реальний оперативний тиск. Зіштовхуючись із мінливістю бойової обстановки, постійним інформаційним шумом та свідомою протидією з боку злочинців, аналітик має діяти безпомилково і швидко. Екстраполюючи цю думку на сучасні реалії підготовки, стає зрозумілим, що закладам вищої освіти необхідно створювати закриті симуляційні середовища та кіберполігони. У таких умовах курсанти зможуть трансформувати теоретичні знання у практичні навички, працюючи з деперсоніфікованими датасетами та прикладним апаратним інструментарієм (зокрема, інтегруючи концепт «цифрової криміналістичної валізи» на базі модулів ESP32/Flipper для захоплення MAC-адрес). Це дозволить відпрацьовувати схеми виявлення ворожих мереж без ризику компрометації реальної оперативної інформації та з суворим дотриманням Закону України «Про захист персональних даних».

Водночас навіть найдосконаліші навички індивідуального моделювання неминуче втрачають свою ефективність, якщо аналітичний підрозділ функціонує в умовах відомчої ізоляції. Сучасна транснаціональна злочинність, кібертероризм і масштабні корупційні мережі мають чітко виражений децентралізований характер, що вимагає симетричної і скоординованої відповіді на рівні всієї держави. У площині підготовки кадрів це означає, що сучасний аналітик має стати своєрідним комунікаційним та інформаційним хабом. Він повинен розуміти юридичні протоколи доступу до міжвідомчих інформаційно-телекомунікаційних систем (ІТС) Національної поліції, СБУ, ДБР, а також специфіку інформаційної підтримки спільних слідчих груп (JIT). Відповідно до ч. 1, 2 ст. 571 КПК України аналітик не є самостійним процесуальним суб'єктом такої групи, тому інформаційний обмін має здійснюватися суворо в межах, визначених процесуальним керівником, з дотриманням ст. 222 КПК України щодо недопустимості розголошення відомостей досудового розслідування. Його завдання полягає у формуванні об'єктивного аналітичного продукту, який забезпечуватиме уповноважених суб'єктів єдиним розумінням оперативної обстановки без порушення режиму таємниці досудового розслідування та законодавства у сфері охорони державної таємниці.

Забезпечення зазначеного рівня професійних компетентностей вимагає системного перегляду як матеріально-

технічного, так і нормативного забезпечення освітнього процесу в системі Міністерства внутрішніх справ України. У цьому контексті фундаментальною та об'єднуючою є позиція М. А. Погорецького щодо нерозривної єдності правових основ оперативно-розшукової діяльності та її сучасного інформаційно-аналітичного забезпечення [10, с. 356]. Навчальні заклади мають інтегрувати в освітній процес спеціалізовані аналітичні платформи та апаратно-програмні комплекси цифрової криміналістики, безпосередньо узгоджуючи прикладну підготовку з вимогами ч. 1 ст. 99 КПК України щодо збирання, фіксації та дослідження електронних документів як джерел доказів.

Підсумовуючи викладене, слід констатувати, що нова концептуальна парадигма підготовки покликана забезпечити підрозділи Національної поліції фахівцями з інформаційно-аналітичного забезпечення, здатними до комплексного управління оперативними ризиками. Системне поєднання навичок кримінального аналізу, OSINT-розвідки, предиктивного моделювання та організації безпечного міжвідомчого обміну даними є тією основою, яка здатна забезпечити правоохоронним органам оперативну перевагу в умовах цифрової трансформації та правового режиму воєнного стану.

**Список використаних джерел**

1. Користін О.Є., Свиридюк Н.П. Кримінальний аналіз : навчальний посібник. Київ : ВАІТЕ, 2023. 296 с.

3. Дараган В. В. Основи кримінального аналізу в діяльності правоохоронних органів : навчальний посібник. Дніпро : ДДУВС, 2022. 198 с.

4. Карчевський М. В. Цифрова трансформація правоохоронної діяльності: сучасні виклики та перспективи : монографія. Київ : РВВ МВС України, 2024. 248 с.

5. Свиридюк Н. П., Кардашевський Ю. Р. Аналітичні продукти. Методи, інструменти та трендові новації кримінального аналізу в Україні. Київ, 2024. 215 с.

6. Василинчук В. І. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності підрозділів Національної поліції України : монографія. Київ : Національна академія внутрішніх справ, 2021. 312 с.

7. Овсянюк Д. І. Інформаційно-аналітичне забезпечення діяльності правоохоронних органів в умовах цифровізації : монографія. Київ : Юрінком Інтер, 2025. 276 с.

8. Захаров В. П., Ісмайлов К. Ю. OSINT у правоохоронній діяльності: теорія та практика застосування : навчальний посібник. Київ : Ліра-К, 2024. 224 с.
9. Албул С. В., Шендрик В. В. Інформаційно-аналітична діяльність підрозділів кримінальної поліції в умовах воєнного стану : монографія. Одеса : ОДУВС, 2025. 287 с.
10. Тімошин А. С. Використання технологій штучного інтелекту та Big Data у правоохоронній діяльності : монографія. Київ: Юридична думка, 2025. 241с.
11. Погорецький М. А. Оперативно-розшукова діяльність: правові основи та інформаційно-аналітичне забезпечення : монографія. Київ : Алерта, 2020. 356 с.

***Тищук Віктор Володимирович,***
доцент кафедри спеціальних дисциплін
факультету правоохоронної діяльності
Національної академії Державної
прикордонної служби України
імені Богдана Хмельницького,
доктор філософії в галузі права

## МЕТОДОЛОГІЧНЕ РОЗМЕЖУВАННЯ СИТУАТИВНОГО ТА СТРАТЕГІЧНОГО КРИМІНАЛЬНОГО АНАЛІЗУ ЯК ПЕРЕДУМОВА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

В умовах трансформації безпекового середовища, зростання транснаціональної організованої злочинності, активного використання злочинними угрупованнями сучасних інформаційно-комунікаційних технологій та збільшення обсягів оперативної інформації кримінальний аналіз набуває особливого значення як складова інформаційно-аналітичного забезпечення роботи правоохоронних органів України. Його застосування забезпечує своєчасне виявлення закономірностей злочинної діяльності, прогнозування розвитку криміногенних процесів і визначення пріоритетних напрямів оперативно-службової діяльності.

На сучасному етапі розвитку правоохоронної системи кримінальний аналіз виконує значно ширші функції, ніж лише інформаційне забезпечення оперативно-розшукової діяльності.