Наукова новизна запропонованого підходу полягає у формуванні інтегрованої методологічної моделі, яка поєднує цикл аналітичної розвідки, структуровані аналітичні техніки та механізми управління когнітивними упередженнями як взаємопов'язані складові трансформації інформації в аналітичний продукт. Такий підхід дозволяє забезпечити простежуваність аналітичного процесу, підвищити якість аналітичних продуктів, посилити прогнозну складову аналітичної діяльності та створити методологічне підґрунтя для подальшого розвитку кримінального аналізу в правоохоронній сфері.

Список використаних джерел

1. Heuer Richards J. Jr. Psychology of Intelligence Analysis. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999. 184 pp.

2. Kahneman D., Slovic P., Tversky A. Judgment under uncertainty: Heuristics and biases. Science, 185 (4157). 1974. URL: https://doi.org/10.1126/science.185.4157.1124.

3. Сучасна аналітична розвідка : підручник. Львів : Львівський державний університет внутрішніх справ, 2026. 456 с.

Форос Ганна Володимирівна,
завідувач кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, кандидат юридичних наук

КІБЕРПРОСТІР ЯК ОБ'ЄКТ КРИМІНАЛЬНОГО АНАЛІЗУ

Сучасний етап цифрової трансформації суспільства характеризується динамічним перенесенням значної частини соціальних, економічних, фінансових та управлінських процесів у цифрове середовище. Одночасно з розширенням цифрових сервісів відбувається еволюція злочинної діяльності, яка дедалі частіше здійснюється із використанням інформаційно-комунікаційних технологій або безпосередньо в кіберпросторі. За таких умов традиційні підходи до кримінального аналізу потребують переосмислення, оскільки об'єктом дослідження стають не лише фізичні особи, матеріальні сліди чи територіальні характеристики злочинності, а й цифрові інформаційні потоки,

мережеві взаємозв'язки, електронні докази та віртуальні середовища функціонування злочинних груп [1].

Кіберпростір поступово трансформується із допоміжного середовища вчинення кримінальних правопорушень у самостійний об'єкт кримінального аналізу. Його особливістю є відсутність чітких територіальних меж, висока швидкість обміну інформацією, анонімність учасників цифрової взаємодії та можливість одночасного здійснення злочинної діяльності на території кількох держав. Саме ці характеристики ускладнюють встановлення закономірностей функціонування злочинних мереж, виявлення організаторів протиправної діяльності та прогнозування подальшого розвитку криміногенних процесів. У сучасній криміналістичній науці кіберпростір дедалі частіше розглядається як окрема обстановка вчинення кримінальних правопорушень, що має власні закономірності формування цифрових слідів та механізмів приховування злочинної діяльності [1].

Для кримінального аналізу принципового значення набуває розуміння того, що цифрові дані є не лише джерелом доказової інформації, а й основою побудови аналітичних моделей злочинної поведінки. Аналіз журналів подій інформаційних систем, мережевого трафіку, криптовалютних транзакцій, соціальних мереж, відкритих інформаційних ресурсів та електронних комунікацій дозволяє формувати цілісну картину функціонування злочинної діяльності. Саме інтеграція різнорідних цифрових джерел забезпечує можливість встановлення прихованих зв'язків між суб'єктами, виявлення центрів управління злочинними угрупованнями та прогнозування їх подальших дій.

Важливою особливістю кримінального аналізу у кіберпросторі є необхідність роботи з великими обсягами інформації. Традиційні методи аналітичної обробки вже не забезпечують належної ефективності через швидке накопичення цифрових даних. У зв'язку з цим дедалі ширше застосовуються інструменти аналізу великих даних (Big Data), алгоритми машинного навчання, графові моделі зв'язків, інтелектуальний аналіз даних та технології штучного інтелекту. Їх використання дозволяє автоматизувати виявлення нетипових моделей поведінки, встановлювати приховані закономірності розвитку кіберзлочинності та здійснювати оцінювання ризиків виникнення нових кримінальних загроз [2].

Особливу роль у кримінальному аналізі відіграють відкриті джерела інформації (OSINT), які дозволяють отримувати значний масив відомостей без застосування спеціальних оперативно-розшукових заходів. Аналіз відкритих профілів соціальних мереж, доменних реєстрів, цифрових платформ, форумів, месенджерів, відкритих державних реєстрів та інших інформаційних ресурсів забезпечує можливість оперативного виявлення потенційних учасників злочинної діяльності, встановлення структури злочинних угруповань та прогнозування напрямів їх розвитку. Поєднання OSINT із класичними методами кримінального аналізу значно підвищує ефективність інформаційно-аналітичного забезпечення діяльності правоохоронних органів.

Водночас розвиток цифрового середовища породжує нові виклики для кримінального аналізу. Використання злочинцями технологій шифрування, анонімних мереж, віртуальних приватних мереж (VPN), криптовалют, децентралізованих платформ та засобів автоматизованої генерації контенту суттєво ускладнює ідентифікацію осіб та документування протиправної діяльності. Додатковою проблемою стає використання генеративного штучного інтелекту для створення дипфейків, автоматизованих фішингових кампаній та масових інформаційних атак, що потребує розроблення нових методів аналітичного супроводу кримінальних проваджень [2].

Не менш важливим аспектом залишається забезпечення належної роботи з цифровими доказами. Ефективність кримінального аналізу безпосередньо залежить від повноти збирання, автентичності, цілісності та допустимості цифрової інформації, яка використовується під час кримінального провадження. У сучасних дослідженнях наголошується, що дотримання процесуальних вимог щодо фіксації електронних доказів є необхідною умовою їх подальшого використання як джерела аналітичної інформації та доказової бази під час судового розгляду [3].

Отже, кіберпростір сьогодні доцільно розглядати як самостійний об’єкт кримінального аналізу, який характеризується специфічними інформаційними процесами, цифровими взаємозв’язками та особливими закономірностями функціонування злочинної діяльності. Подальший розвиток кримінального аналізу безпосередньо пов’язаний із впровадженням сучасних інформаційно-аналітичних технологій,

методів обробки великих даних, штучного інтелекту та автоматизованих систем підтримки прийняття рішень.

Саме інтеграція традиційних криміналістичних підходів із цифровими технологіями створює передумови для підвищення ефективності протидії кіберзлочинності, своєчасного виявлення кримінальних загроз та формування сучасної системи інформаційно-аналітичного забезпечення правоохоронної діяльності.

Список використаних джерел

1. Вуйма А. В. Цифровий вимір сучасної злочинності: кіберпростір як типова обстановка вчинення кримінальних правопорушень. *Архів кримінології та судових наук*. 2025. Т. 12, № 2. С. 64–70. DOI: 10.32353/acfs.12.2025.05.

2. Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. *Вісник Кримінологічної асоціації України*. 2025. № 1. DOI: 10.32631/vca.2025.1.66.

3. Сошенко Б. О. Виявлення та документування злочинів у кіберпросторі: проблеми допустимості цифрових доказів і процесуальної доброчесності. *Вісник кримінального судочинства*. 2026. № 1. DOI: 10.59835/2413-5372.2026.1/544-563.

Цуцкірідзе Максим Сергійович,
перший заступник Голови Національної поліції України – начальник Головного слідчого управління, доктор юридичних наук, професор

ІНТЕГРАЦІЯ РЕЗУЛЬТАТІВ КРИМІНАЛЬНОГО АНАЛІЗУ В СИСТЕМУ КРИМІНАЛЬНОГО СУДОЧИНСТВА УКРАЇНИ: СУЧАСНИЙ СТАН І НАПРЯМИ ВДОСКОНАЛЕННЯ

Стрімке ускладнення злочинності в Україні, її організований, транснаціональний та дедалі більш латентний характер, зростання кількості кримінальних проваджень щодо корупційних, кіберзлочинів, а також злочинів, пов’язаних зі збройною агресією РФ, об’єктивно зумовлюють необхідність переходу від традиційної моделі досудового розслідування до моделі, заснованої на аналітичному супроводі кримінального провадження.

Одним із ключових інструментів такого підходу є кримінальний аналіз, який визначається як діяльність, спрямована