технологій, удосконалення нормативно-правової бази та підвищення рівня підготовки кадрів.

Список використаних джерел:

1. Федчак І. А. Основи кримінального аналізу. Львів : ЛьвДУВС, 2020. 240 с.

2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19

3. Кисельов А. О., Копилов Е. В. Кримінальний аналіз у діяльності правоохоронних органів. Дніпро : ДДУВС, 2023. 220 с.

4. Білоус Р.В., Василинчук В.І., Таран О.В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 1 (118). URL: https://philosophy.naiau.kiev.ua/ index.php/scientbul/ article/ download/1352/1351/.

КРИМІНАЛЬНИЙ АНАЛІЗ КІБЕРЗЛОЧИННОСТІ

Грезіна Олена Миколаївна
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ
Баглік Костянтин Костянтинович
здобувач вищої освіти
Інститут права та безпеки
Одеський державний університет внутрішніх справ

Стрімкий розвиток інформаційних технологій та повсюдна цифровізація суспільства зумовили появу якісно нових форм злочинної діяльності, що реалізуються у кіберпросторі. Кіберзлочинність сьогодні становить одну з найбільш динамічних і суспільно небезпечних загроз національній безпеці, економічній стабільності та правам громадян. За оцінками міжнародних аналітичних центрів, щорічні збитки від кіберзлочинів у світі сягають трильйонів доларів, а кількість зафіксованих кіберінцидентів невпинно зростає. В умовах повномасштабного збройного конфлікту в Україні

кіберзлочинність набуває додаткового виміру — вона нерозривно пов'язана з кібершпигунством, дезінформаційними кампаніями та атаками на критичну інфраструктуру, що значно ускладнює її виявлення, документування та розслідування. За цих обставин особливої актуальності набуває кримінальний аналіз як спеціалізований напрям аналітичної діяльності правоохоронних органів.

Кримінальний аналіз кіберзлочинності являє собою системну діяльність із збору, опрацювання та інтерпретації даних про злочини у сфері інформаційних технологій з метою підтримки оперативно-розшукової та слідчої практики, прогнозування злочинних проявів та вироблення превентивних заходів. Ця діяльність охоплює тактичний, оперативний і стратегічний рівні: від аналізу конкретних кіберінцидентів — до виявлення системних закономірностей і розробки рекомендацій для вдосконалення правової політики у сфері протидії кіберзлочинності. Методологічну основу кримінального аналізу складають прийоми кримінологічного моделювання, мережевого аналізу, профілювання злочинців і аналізу цифрових слідів [2].

Особливу роль у кримінальному аналізі кіберзлочинності відіграє типологія суб'єктів злочинної діяльності. Сучасна кримінологічна наука виробила декілька підходів до класифікації кіберзлочинців: за рівнем технічної підготовки, мотивацією, організаційною структурою злочинних угруповань та характером завданої шкоди. Дослідження П. П. Галушка свідчать, що в умовах стрімкої ескалації загроз у цифровому середовищі кримінологічні підходи до типології кіберзлочинців потребують постійного оновлення — адже сучасний кіберзлочинець поєднує технічні компетенції з розумінням соціальної інженерії, а злочинні угруповання дедалі частіше функціонують як добре організовані транснаціональні структури [1].

Одним із найбільш перспективних напрямів розвитку кримінального аналізу у сфері кіберзлочинності є впровадження сучасних технологій обробки та верифікації даних. Зокрема, технологія блокчейну відкриває можливості для забезпечення незмінності доказової бази та підвищення рівня довіри до цифрових доказів у кримінальному провадженні. Системи на основі штучного інтелекту дозволяють виявляти складні схеми шахрайства, відстежувати транзакції у криптоактивах і прогнозувати нові вектори атак. Водночас широке впровадження таких технологій у

правоохоронну діяльність супроводжується серйозними викликами: потребою у нормативному регулюванні, ризиками порушення прав людини при обробці персональних даних та необхідністю спеціальної підготовки аналітичного персоналу [2].

Суттєвою проблемою кримінального аналізу кіберзлочинності залишається латентність цього виду злочинів. Значна частина кіберінцидентів не фіксується офіційною статистикою через небажання постраждалих осіб і організацій звертатися до правоохоронних органів, труднощі з атрибуцією атак та специфіку цифрового середовища, яке дозволяє злочинцям ефективно приховувати сліди своєї діяльності. Ця обставина суттєво знижує повноту статистичних даних і ускладнює вироблення достовірних прогностичних моделей. Подолання латентності можливе шляхом запровадження обов'язкового повідомлення про кіберінциденти для суб'єктів критичної інфраструктури, розвитку механізмів публічно-приватного партнерства та розширення міжнародного інформаційного обміну між правоохоронними органами різних держав.

Кримінальний аналіз кіберзлочинності нерозривно пов'язаний із методологічними питаннями збору та оцінки цифрових доказів. На відміну від традиційних злочинів, кіберзлочини залишають цифрові сліди, що можуть бути легко знищені, модифіковані чи фальсифіковані. Забезпечення допустимості та достовірності таких доказів вимагає від аналітиків і слідчих розуміння технічних засад комп'ютерних систем, дотримання встановлених криміналістичних процедур і застосування спеціалізованого програмного забезпечення для вилучення та дослідження цифрових даних. Водночас транскордонний характер переважної більшості кіберзлочинів зумовлює потребу у координації зусиль на рівні міжнародних організацій, зокрема у межах Будапештської конвенції про кіберзлочинність та відповідних механізмів Інтерполу [1].

Перспективи розвитку кримінального аналізу кіберзлочинності в Україні пов'язані з декількома ключовими напрямами. По-перше, необхідне вдосконалення законодавчої бази шляхом імплементації актуальних положень міжнародного права у сфері кібербезпеки та гармонізації вітчизняного законодавства з нормами Європейського Союзу. По-друге, стратегічного значення набуває розвиток людського капіталу — підготовка фахівців, здатних поєднувати юридичні знання з технічними компетенціями у галузі

інформаційної безпеки. По-третє, критично важливою є розбудова інституційних спроможностей правоохоронних органів, зокрема підрозділів кіберполіції та спеціалізованих аналітичних центрів. Нарешті, ефективна протидія кіберзлочинності неможлива без активного залучення наукової спільноти до розробки нових методів кримінального аналізу, адаптованих до швидкозмінного технологічного середовища [2].

Таким чином, кримінальний аналіз кіберзлочинності є багатоаспектним явищем, що охоплює методологічні, технологічні, правові та організаційні виміри протидії злочинності у цифровому просторі. Подальший розвиток цього напряму потребує системного підходу, що передбачає інтеграцію сучасних аналітичних технологій, удосконалення нормативно-правової бази, розвиток міжнародного співробітництва та підвищення фахового рівня правоохоронних органів. Лише за умови комплексного розв'язання зазначених завдань можливо забезпечити ефективну протидію кіберзлочинності як одній із найбільш серйозних загроз сучасному суспільству.

Список використаних джерел:

1. Галушко П. П. Особа кіберзлочинця: кримінолого-типологічна характеристика. *Вісник Кримінологічної асоціації України.* 2025. Том 35. № 2. Ч. 1. С. 73–85. DOI: https://doi.org/10.32631/vca.2025.2.5 .

2. Кисельов А. Майбутнє кримінального аналізу: інтеграція технологій блокчейну, віртуальної реальності та квантових обчислень. *Universum.* 2025. № 21. С. 344–348. URL: https://archive.liga.science/index.php/universum/article/view/1997 .