МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Ольга Лунгол
Ольга Габорець

ІННОВАЦІЙНІ МЕТОДИКИ ТА СУЧАСНІ ПРАКТИКИ В ДІЯЛЬНОСТІ ПОЛІЦІЇ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ

Науково-практичні рекомендації

2026

УДК 351.74:343.9.02:004.056(477)(072)
Л 84

Рекомендовано до друку Вченою радою
Донецького державного університету внутрішніх справ
протокол № 4 від 28 жовтня 2026 року

Укладачі:

ЛУНГОЛ Ольга Миколаївна – завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, кандидат педагогічних наук, доцент

ГАБОРЕЦЬ Ольга Андріївна – доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор філософії, доцент

Рецензенти:

Тичина Дмитро Михайлович - провідний науковий співробітник науково-дослідної лабораторії з проблем протидії злочинності Національної академії внутрішніх справ, доктор юридичних наук, професор.

Бабенко Андрій Миколайович - завідувач кафедри кримінально-правових дисциплін інституту права та безпеки Одеського державного університету внутрішніх справ, доктор юридичних наук, професор.

Л 84 **Лунгол О.М., Габорець О.А.**

Інноваційні методики та сучасні практики в діяльності поліції у сфері протидії організованій кіберзлочинності: науково-практичні рекомендації. _____, 2026. 96 с.

У науково-практичних рекомендаціях висвітлено теоретико-правові та прикладні засади діяльності правоохоронних органів у сфері протидії організованій кіберзлочинності. Проаналізовано сучасний стан, тенденції розвитку та специфіку функціонування організованої кіберзлочинності, а також нормативно-правове регулювання й передовий міжнародний досвід діяльності поліції щодо протидії їй. Розкрито інноваційні методики та сучасні практики виявлення, документування й розслідування кіберзлочинів, зокрема використання інструментів розвідки на основі відкритих джерел (OSINT) і цифрової криміналістики, можливості застосування систем штучного інтелекту та аналітичних платформ для предиктивної аналітики, а також алгоритми виявлення, збору, аналізу та процесуального закріплення цифрових слідів (доказів). Сформульовано практичні рекомендації, спрямовані на підвищення ефективності протидії організованій кіберзлочинності в сучасних умовах.

Науково-практичні рекомендації призначено для працівників підрозділів стратегічних розслідувань, кіберполіції та інших підрозділів Національної поліції України, діяльність яких пов’язана із запобіганням, виявленням, документуванням і розслідуванням проявів організованої кіберзлочинності, а також для науково-педагогічних працівників і здобувачів освіти закладів вищої освіти зі специфічними умовами навчання.

УДК 351.74:343.9.02:004.056(477)(072)

© Донецький державний університет внутрішніх справ, 2026

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ	8
1.1. Сучасний стан, тенденції розвитку та специфіка функціонування організованої кіберзлочинності	8
1.2. Нормативно-правове регулювання та передовий міжнародний досвід діяльності поліції щодо протидії кіберзагрозам	25
РОЗДІЛ 2.ІННОВАЦІЇ ТА СУЧАСНІ ПРАКТИКИ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ Й РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ	35
2.1. Використання інструментів розвідки на основі відкритих джерел (OSINT) та цифрової криміналістики в діяльності поліції	35
2.2. Можливості застосування систем штучного інтелекту та аналітичних платформ для предиктивної аналітики та протидії організованим кіберзлочинним угрупованням	53
2.3. Алгоритми виявлення, збору, аналізу та процесуального закріплення цифрових слідів (доказів)	69
ВИСНОВКИ	80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	88

ВСТУП

Стрімка цифровізація суспільних відносин, державного управління, фінансової системи, економіки та комунікацій зумовила не лише появу нових можливостей для розвитку держави, а й істотну трансформацію сучасної злочинності. Інформаційно-комунікаційні технології дедалі активніше використовуються для підготовки, координації та вчинення кримінальних правопорушень, приховування їх слідів, легалізації одержаних доходів і забезпечення анонімної взаємодії між учасниками злочинної діяльності. Особливої небезпеки за таких умов набуває організована кіберзлочинність, яка поєднує ознаки традиційної організованої злочинності з технологічними можливостями кіберпростору, має переважно мережевий і транснаціональний характер та здатна швидко адаптуватися до змін у правоохоронній практиці й механізмах захисту інформації.

Сучасні організовані кіберзлочинні угруповання не завжди функціонують як локалізовані та жорстко ієрархічні структури. Їх діяльність може ґрунтуватися на дистанційній взаємодії учасників, функціональному розподілі ролей, використанні псевдонімів, зашифрованих каналів зв'язку, спеціалізованих цифрових платформ, віртуальних активів та послуг інших суб'єктів кримінального середовища. Розробники шкідливого програмного забезпечення, брокери первинного доступу, адміністратори серверів, оператори програм-вимагачів, фахівці із соціальної інженерії, продавці викрадених даних і посередники з виведення коштів можуть перебувати в різних юрисдикціях, не мати безпосередніх особистих контактів, однак діяти як взаємопов'язані елементи єдиного кримінального механізму.

Поширення моделі «кіберзлочинність як послуга» сприяє подальшій професіоналізації та масштабуванню протиправної діяльності. Окремі складові кібероперації, такі, як шкідливе програмне забезпечення, доступ до скомпрометованих інформаційних систем, фішингові комплекти, серверні потужності, засоби анонімізації, бази викрадених даних, механізми проведення фінансових операцій і т.д., пропонуються як самостійні продукти або послуги. Унаслідок цього знижується технологічний бар'єр входження до кримінального середовища, прискорюється відновлення злочинної інфраструктури після її блокування, а один постачальник незаконних сервісів може одночасно забезпечувати діяльність значної кількості кримінальних мереж.

Для України проблема протидії організованій кіберзлочинності має особливе значення в умовах правового режиму воєнного стану та триваючої збройної агресії проти України. Кіберпростір став одним із середовищ реалізації загроз національній безпеці, а межі між корисливою кіберзлочинністю, діяльністю організованих кримінальних угруповань, хактивістськими кампаніями та операціями, що здійснюються в інтересах держави-агресора, можуть бути недостатньо чіткими. Кібератаки на органи державної влади, об'єкти критичної інфраструктури, підприємства, фінансові

установи та громадян здатні спричиняти не лише майнову шкоду, а й порушення функціонування інформаційних систем, витік даних, дестабілізацію суспільних процесів і зниження довіри до державних інституцій.

Зазначені обставини ставлять перед органами та підрозділами Національної поліції України нові завдання. Традиційний підхід, орієнтований переважно на реагування на окремий завершений епізод і встановлення його безпосереднього виконавця, не завжди дає змогу виявити всю структуру організованої кіберзлочинної діяльності. Результативна протидія потребує дослідження сукупності цифрових, фінансових, інфраструктурних, комунікаційних і поведінкових зв'язків; встановлення організаторів, координаторів, постачальників злочинних послуг та інших учасників; визначення повторюваних способів дій; виявлення спільної технічної інфраструктури та каналів легалізації кримінальних доходів.

Важливого значення у зв'язку із цим набуває впровадження в діяльність поліції сучасних методів кримінального аналізу, розвідки на основі відкритих джерел, цифрової криміналістики, аналізу віртуальних активів, систем штучного інтелекту, спеціалізованих інформаційно-аналітичних платформ та інструментів предиктивної аналітики. Їх комплексне застосування дає змогу опрацьовувати значні обсяги різнорідної інформації, встановлювати неочевидні зв'язки між особами, подіями, цифровими ідентифікаторами та об'єктами інфраструктури, визначати найбільш значущі вузли кримінальної мережі, формувати обґрунтовані аналітичні версії та своєчасно виявляти ознаки підготовки або продовження протиправної діяльності.

Водночас використання інноваційних технологій у правоохоронній діяльності повинно здійснюватися з дотриманням принципів законності, верховенства права, пропорційності втручання, захисту персональних даних, поваги до прав і свобод людини, а також установлених кримінальним процесуальним законодавством вимог. Результати автоматизованої обробки даних, застосування аналітичних алгоритмів або систем штучного інтелекту не можуть автоматично визнаватися достовірними чи підміняти собою професійну оцінку уповноваженої особи. Такі результати повинні перевірятися, зіставлятися з іншими відомостями та використовуватися як допоміжний інструмент для прийняття обґрунтованих процесуальних і управлінських рішень.

Окремою умовою ефективності протидії організованій кіберзлочинності є належна робота із цифровими слідами та доказами. Їх мінливість, розподіленість між різними пристроями, інформаційними системами й юрисдикціями, залежність від налаштувань цифрових платформ і можливість швидкого видалення зумовлюють необхідність оперативного виявлення, фіксації, вилучення, копіювання, збереження та дослідження відповідної інформації. Недотримання встановленого порядку роботи із цифровими даними може призвести до втрати важливої інформації, порушення її цілісності або виникнення сумнівів щодо достовірності й допустимості

отриманих доказів. Саме тому технічні засоби мають застосовуватися у нерозривному зв'язку із процесуальними правилами та належним документуванням усіх виконаних дій.

Актуальність підготовки цих науково-практичних рекомендацій зумовлена необхідністю формування комплексного підходу до організації діяльності поліції у сфері протидії організованій кіберзлочинності, поєднання теоретико-правових засад із сучасними аналітичними та технічними інструментами, а також адаптації передового міжнародного досвіду до потреб національної правоохоронної практики.

Метою науково-практичних рекомендацій є узагальнення сучасних наукових підходів і практик та розроблення орієнтованих на практичне застосування положень щодо вдосконалення діяльності органів і підрозділів Національної поліції України у сфері запобігання, виявлення, документування та розслідування проявів організованої кіберзлочинності.

Для досягнення поставленої мети передбачено наступні етапи:

- охарактеризувати сучасний стан, основні тенденції та специфіку функціонування організованої кіберзлочинності;
- визначити її найбільш небезпечні організаційні, технологічні та фінансові складові;
- проаналізувати нормативно-правові засади і міжнародний досвід протидії кіберзагрозам;
- розкрити можливості застосування інструментів розвідки на основі відкритих джерел та цифрової криміналістики;
- визначити перспективні напрями використання систем штучного інтелекту, аналітичних платформ і методів предиктивної аналітики;
- сформувати алгоритми виявлення, збору, аналізу, збереження та процесуального закріплення цифрових слідів і доказів.

Об'єктом дослідження є суспільні відносини, що виникають у процесі діяльності правоохоронних органів із протидії організованій кіберзлочинності.

Предмет дослідження становлять теоретико-правові, організаційні, аналітичні, технологічні та криміналістичні засади застосування інноваційних методик і сучасних практик у діяльності поліції щодо запобігання, виявлення, документування та розслідування кримінальних правопорушень, учинених організованими угрупованнями з використанням інформаційно-комунікаційних технологій.

Методологічною основою науково-практичних рекомендацій є поєднання загальнонаукових і спеціальних методів пізнання.

Застосування системного та структурно-функціонального підходів дало змогу розглянути організовану кіберзлочинність як складну кримінальну екосистему; формально-юридичного та порівняльно-правового методів – проаналізувати нормативне регулювання і міжнародні практики; методів аналізу, синтезу, узагальнення та моделювання – визначити взаємозв'язки між

окремими елементами злочинної діяльності й сформувати практичні алгоритми дій працівників поліції

Практичне значення науково-практичних рекомендацій полягає в можливості використання викладених положень під час:

- організації оперативно-розшукової, інформаційно-аналітичної та кримінальної процесуальної діяльності;
- проведення кримінального аналізу;
- пошуку й перевірки інформації у відкритих джерелах;
- дослідження цифрової інфраструктури та фінансових операцій;
- планування і проведення слідчих (розшукових) та інших процесуальних дій;
- забезпечення належного поводження із цифровими доказами.

Запропоновані положення також можуть використовуватися у професійній підготовці та підвищенні кваліфікації працівників поліції, а також у науковій і освітній діяльності закладів вищої освіти зі специфічними умовами навчання.

Структуру науково-практичних рекомендацій побудовано відповідно до поставленої мети та визначених завдань. У першому розділі висвітлено теоретико-правові засади діяльності правоохоронних органів у сфері протидії організованій кіберзлочинності, охарактеризовано сучасний стан, тенденції розвитку та специфіку її функціонування, а також проаналізовано нормативно-правове регулювання і передовий міжнародний досвід діяльності поліції щодо протидії кіберзагрозам. У другому розділі розкрито практичні можливості використання OSINT та цифрової криміналістики, систем штучного інтелекту й аналітичних платформ, а також запропоновано алгоритми виявлення, збору, аналізу та процесуального закріплення цифрових слідів і доказів.

РОЗДІЛ 1.
ТЕОРЕТИКО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ

1.1. Сучасний стан, тенденції розвитку та специфіка функціонування організованої кіберзлочинності

Цифровізація державного управління, економіки, фінансових послуг, комунікацій і повсякденної діяльності суттєво трансформувала структуру сучасної злочинності. Інформаційно-комунікаційні технології створили середовище, у якому кримінальні дії можуть готуватися, координуватися та реалізовуватися дистанційно, а наслідки одного епізоду одночасно проявлятися у кількох державах. За таких умов кіберзлочинність уже не може розглядатися виключно як сукупність поодиноких технічно складних посягань на комп'ютерні системи. Її найбільш небезпечний сегмент формують стійкі кримінальні мережі, здатні поєднувати спеціалізовані знання, цифрову інфраструктуру, фінансові ресурси, анонімізовані комунікації, послуги посередників та розподілену систему виконавців. Саме така сукупність властивостей дає підстави розглядати організовану кіберзлочинність як особливу форму сучасної організованої злочинності, яка функціонує переважно у цифровому середовищі, але породжує реальні майнові, економічні, безпекові та соціальні наслідки.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кіберзлочин визначається як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України[1]. Однак для характеристики саме організованої кіберзлочинності одного факту використання інформаційних технологій недостатньо. Визначальними є стійкість взаємодії, координація дій, функціональний розподіл ролей, спільність кримінальної мети, повторюваність операцій, наявність ресурсної або сервісної бази, а в багатьох випадках – спеціально створеної чи пристосованої цифрової інфраструктури. Важливо й те, що цифрова взаємодія дозволяє підтримувати організованість без постійної фізичної присутності учасників в одному місці, а тому традиційні просторові критерії виявляються недостатніми для оцінки такої діяльності.

У кримінологічному вимірі організовану кіберзлочинність доцільно розуміти не як самостійний перелік складів кримінальних правопорушень, а як особливий спосіб організації кримінальної діяльності у цифровому середовищі. Вона може охоплювати як кіберзалежні злочини – діяння, існування яких без комп'ютерних систем фактично неможливе, так і

[1] 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.

кіберпідсилені злочини – традиційні шахрайства, вимагання, легалізацію доходів, незаконний обіг даних та інші посягання, масштаб і результативність яких істотно посилюються завдяки цифровим технологіям. Такий підхід важливий тому, що сучасні організовані мережі дедалі частіше поєднують обидва сегменти: технічне проникнення або компрометація облікових даних стають лише початковою ланкою подальшого шахрайства, вимагання, викрадення інформації чи відмивання коштів.

Наукові дослідження останніх років послідовно акцентують увагу на високій латентності, професіоналізації, транснаціональності та тісному зв'язку кіберзлочинності з організованими формами кримінальної діяльності[2]. Проте сучасний етап характеризується тим, що зазначені ознаки вже не існують ізольовано. Вони утворюють цілісну модель функціонування, у якій технологічні засоби забезпечують масштабованість, а розподіл ролей і використання спеціалізованих сервісів – організаційну стійкість. У цьому сенсі організована кіберзлочинність дедалі більше нагадує нелегальний ринок, де доступ до технічних ресурсів, викрадених даних, серверної інфраструктури, засобів анонімізації та фінансових послуг може купуватися окремо, а кінцевий злочинний результат формується шляхом інтеграції декількох незалежних сервісів.

Ця модель суттєво відрізняється від традиційного уявлення про організовану групу як відносно стабільне коло осіб із жорсткою ієрархією. У цифровому середовищі організованість може ґрунтуватися на стійких економічних зв'язках, репутації у підпільному середовищі, повторюваних операціях, спільній інфраструктурі та спеціалізації учасників. Особа може не знати реальних установчих даних інших співучасників, однак системно виконувати визначену функцію, отримувати винагороду та усвідомлювати кримінальний характер спільної діяльності. Тому виявлення організованої форми потребує аналізу не лише особистих контактів, а й цифрових, інфраструктурних, фінансових та поведінкових зв'язків між учасниками.

Поточний стан кіберзлочинності характеризується не стільки появою принципово нових видів посягань, скільки безперервною модифікацією способів їх реалізації, масштабуванням уже відомих моделей та швидкою адаптацією злочинців до змін у технологіях захисту. Аналітичні матеріали європейських інституцій свідчать про збереження високої інтенсивності атак на доступність сервісів, значний вплив програм-вимагачів (ransomware), поширеність фішингу, експлуатації вразливостей, викрадення облікових даних та використання легітимної інфраструктури з протиправною метою. ENISA у Threat Landscape 2025 проаналізувала 4875 інцидентів за період із липня 2024 року до червня 2025 року, серед зафіксованих інцидентів DDoS-атаки становили 77 %, програми-вимагачі було визначено найбільш впливовою загрозою, а фішинг і експлуатація вразливостей – провідними

[2] Піщенко Г. І., Шопіна Ю. О. Кібербезпека та кіберзлочинність в Україні: сучасні тенденції. *Науковий вісник Ужгородського національного університету*. 2025. Том 4 № 92. С. 193-199. DOI: https://doi.org/10.24144/2307-3322.2025.92.4.26.

шляхами первинного проникнення. Ці показники не є тотожними структурі організованої кіберзлочинності, однак відображають середовище, у якому організовані актори формують і масштабують свої операції[3].

Висока питома вага DDoS-активності потребує обережної кримінологічної інтерпретації. Значна частина таких інцидентів має хактивістський або ідеологічно мотивований характер і не завжди пов'язана з класичною корисливою організованою злочинністю. Водночас організаційні моделі, які забезпечують масове залучення користувачів, використання бот-мереж, оренду потужностей, проксі-інфраструктури та анонімізованих каналів управління, демонструють важливу закономірність: кібероперація може бути технічно централізованою, але організаційно розподіленою. Для правоохоронної оцінки це означає необхідність відокремлювати ідеологічний мотив від способу організації діяльності та встановлювати, чи існує стійке ядро, яке координує учасників, забезпечує інструментарій, визначає цілі та підтримує інфраструктуру.

Програми-вимагачі залишаються особливо показовою формою організованої кіберзлочинності, оскільки в ній поєднуються технічне проникнення, викрадення даних, порушення доступності систем, психологічний тиск і фінансове вимагання. Сучасні операції з використанням програм-вимагачів дедалі частіше ґрунтуються на багатоступеневому вимаганні: злочинці можуть не обмежуватися шифруванням інформації, а погрожувати її оприлюдненням, зверненням до клієнтів або партнерів потерпілої організації, використанням регуляторних наслідків чи репутаційних ризиків. ENISA фіксує розвиток агресивних тактик тиску, повторне використання витеклих конструкторів програм-вимагачів та поширення спеціалізованих засобів, спрямованих на відключення або обхід систем Endpoint Detection and Response. Це свідчить, що цей вид кримінальної діяльності розвивається як комплексна операційна модель, а не як окремий вид шкідливого програмного забезпечення[4].

Паралельно з програмами-вимагачами зберігає значення масове викрадення облікових даних. Екосистема програм-викрадачів даних формує ресурсну базу для подальших атак: викрадені логіни, cookie-файли, токени сесій, дані браузера та інша інформація можуть використовуватися самими виконавцями або продаватися іншим учасникам кримінального ринку. Така вторинна реалізація цифрових даних підкреслює важливу властивість організованої кіберзлочинності – один епізод компрометації здатний породжувати декілька наступних кримінальних сценаріїв. Первинна крадіжка даних, несанкціонований доступ, шахрайство, вимагання і відмивання коштів можуть бути рознесені у часі та виконуватися різними суб'єктами, але становити ланки одного кримінального ланцюга.

---

[3]ENISA. ENISA Threat Landscape 2025. 1 October 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[4]ENISA. ENISA Threat Landscape 2025. Section 6.4 «Key cybercrime trends». URL: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

Фішинг і соціальна інженерія також еволюціонували від відносно примітивних масових розсилок до індустріалізованих сервісів, здатних підтримувати складні сценарії перехоплення автентифікації. У березні 2026 року міжнародна операція за підтримки Europol припинила роботу Tycoon 2FA – phishing-as-a-service платформи, яка надавала підписникам інструментарій для перехоплення активних сесій автентифікації та обходу багатофакторного захисту[5]. Цей приклад демонструє, що злочинний ринок пропонує вже не лише шаблон фішингової сторінки, а технологічно завершений сервіс, доступний користувачам із різним рівнем технічної підготовки.

Загальна картина сучасної кіберзлочинності визначається не однією домінуючою технологією, а взаємодією декількох сегментів: викрадення доступів, експлуатації вразливостей, malware-інфраструктури, соціальної інженерії, фінансового шахрайства, сервісів анонімізації та механізмів відмивання цифрових активів. Взаємозалежність цих сегментів формує стійкість організованої кіберзлочинності. Відповідно, оцінювання сучасного стану має здійснюватися за принципом кримінальної екосистеми: важливим є не лише те, який вид атаки переважає статистично, а які сервіси, посередники, канали доступу та фінансові механізми забезпечують повторюваність і масштабованість злочинної діяльності.

Однією з найбільш стійких тенденцій є перехід від жорстко ієрархічних структур до мережевих і модульних моделей. У такій системі організатор не обов'язково безпосередньо керує кожним виконавцем, а окремі учасники можуть вступати у взаємодію лише на певному етапі злочинного циклу. Розробники шкідливого програмного забезпечення, брокери первинного доступу, оператори програм-вимагачів, адміністратори серверів, фахівці із соціальної інженерії, продавці викрадених даних, особи, які забезпечують виведення коштів, та інші посередники можуть діяти автономно, але їх послуги інтегруються у спільний механізм одержання незаконного доходу. Це ускладнює традиційне встановлення організаційної структури, оскільки межі між учасником групи, постачальником послуги і клієнтом злочинного сервісу стають рухомими.

Мережева модель зменшує залежність кримінальної діяльності від окремої особи або технічного ресурсу. Якщо один виконавець вибуває, його функція може бути передана іншому. Якщо сервер вилучено, інфраструктуру можна розгорнути на новій платформі. Якщо домен заблоковано, використовуються інші доменні імена, IP-адреси або канали поширення. За таких умов організована кіберзлочинність демонструє властивість оперативної регенерації. Відновлення може відбуватися під новою назвою, із частково зміненим складом учасників або через міграцію до іншого сервісу, але з використанням тих самих контактів, навичок, фінансових каналів і клієнтської бази.

[5] Europol. Global phishing-as-a-service platform taken down in coordinated public-private action. 4 March 2026. URL: https://www.europol.europa.eu/media-press/newsroom/news/global-phishing-service-platform-taken-down-in-coordinated-public-private-action.

Функціональна спеціалізація сприяє формуванню моделі «кіберзлочинність як послуга» (Cybercrime-as-a-Service), у межах якої окремі елементи кримінальної операції купуються або орендуються як самостійний продукт. Europol у матеріалах IOCTA 2026 характеризує сервіси забезпечення кіберзлочинності як один із ключових чинників сучасної кіберзлочинної екосистеми. До них належать стійкі підпільні майданчики, криптовалютні механізми розрахунків і багаторівнева інфраструктура, спрямована на уникнення виявлення. Такий ринок дозволяє відокремити технічну компетентність від кримінальної ініціативи: особа, яка планує шахрайство або вимагання, може не володіти навичками створення шкідливого програмного забезпечення чи побудови інфраструктури, оскільки відповідні компоненти доступні як сервіс[6].

Сервісна модель має декілька принципових наслідків. По-перше, вона знижує бар'єр входження до кіберзлочинності. По-друге, створює конкурентне середовище між постачальниками незаконних послуг, що стимулює підвищення їх технічної якості, зручності та підтримки. По-третє, забезпечує масштабування: один постачальник інфраструктури може одночасно обслуговувати значну кількість незалежних кримінальних кампаній. По-четверте, розділення функцій ускладнює доказування спільного умислу і ролі конкретного суб'єкта, особливо якщо взаємодія відбувається через псевдоніми, автоматизовані платформи та короткотривалі контакти.

Особливе місце в цій структурі посідають брокери первинного доступу – посередники, які спеціалізуються на отриманні первинного доступу до корпоративних або інших інформаційних систем і подальшому продажі такого доступу. Їх діяльність демонструє, що кримінальний продукт може існувати ще до визначення кінцевого виду атаки. Скомпрометований доступ до мережі однієї організації може бути придбаний групою операторів програм-вимагачів, шахрайською мережею або іншими суб'єктами. Для правоохоронної практики це означає, що розслідування фінального інциденту повинно охоплювати і попередні ланки доступу: спосіб компрометації, канал продажу, зв'язки продавця з іншими клієнтами та повторюваність використаної інфраструктури.

Схожу функцію виконують абузостійкий хостинг, проксі- та VPN-інфраструктури, сервіси масової реєстрації доменів, орендовані сервери та інші послуги, які навмисно або фактично забезпечують підвищену стійкість протиправної цифрової активності. Їх роль полягає не обов'язково у безпосередньому вчиненні атаки, а в забезпеченні операційної життєздатності кримінальної мережі. Саме такі допоміжні вузли нерідко обслуговують широке коло незалежних злочинних клієнтів, тому їх виявлення і нейтралізація може створювати значно ширший ефект, ніж припинення одного епізоду.

[6] Europol. IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. 28 April 2026. URL: https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape.

Стійкість організованих кіберзлочинних мереж значною мірою визначається децентралізацією технічної інфраструктури. Командно-контрольні сервери, резервні домени, файлові сховища, облікові записи, криптовалютні адреси та інші цифрові ресурси можуть бути розподілені між різними постачальниками і юрисдикціями. Така побудова знижує ефективність заходів, спрямованих лише на один технічний компонент. Навіть успішне вилучення сервера не гарантує припинення операції, якщо існують резервні канали управління, альтернативні точки доступу або можливість швидкого відновлення даних.

З огляду на це міжнародні операції останніх років дедалі частіше спрямовуються не на один об'єкт, а на одночасне порушення декількох складових інфраструктури: серверів, доменів, криптовалютних активів, адміністративних облікових записів і каналів комунікації. Показовим є Operation Endgame, у межах якої у травні 2025 року було вилучено криптовалюту на суму 21,2 млн євро, виведено з ладу близько 300 серверів поширення шкідливого програмного забезпечення і нейтралізовано 650 доменів. Europol розглядає цю операцію як удар по ланцюгу, що забезпечує атаки із застосуванням програм-вимагачів. Важливість такого підходу полягає в орієнтації на інфраструктурний рівень злочинної діяльності, а не лише на окремих виконавців[7].

Іншим прикладом є міжнародна операція Eastwood проти NoName057(16), проведена в липні 2025 року за координації Europol та Eurojust. Мережа використовувала стійке ядро та ширше коло прихильників у різних державах, які залучалися до DDoS-атак проти України та країн, що її підтримують[8]. Для оцінки організованої кіберзлочинності цей кейс важливий тим, що демонструє поєднання централізованої координації з масовою, відносно низькопороговою участю. Така модель дозволяє масштабувати активність без необхідності включення кожного учасника до формального ядра групи.

Після масштабного правоохоронного втручання кіберзлочинні мережі можуть змінювати назви, бренд, комунікаційні канали або склад учасників. Ребрендинг у цьому контексті є не маркетинговою деталлю, а способом збереження людського капіталу, довіри та клієнтських зв'язків у підпільному середовищі. Виявлення наступності між формально різними групами тому потребує аналізу повторюваних технічних рішень, мовних і поведінкових ознак, інфраструктурних зв'язків, фінансових адрес і контактів. Інакше правоохоронна оцінка ризику може штучно «обнулятися» після зникнення попередньої назви угруповання.

[7] Europol. Operation ENDGAME strikes again: the ransomware kill chain broken at its source. 23 May 2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source.

[8] Europol. Global operation targets NoName057(16) pro-Russian cybercrime network. 16 July 2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

Здатність до відновлення пояснює, чому результативність протидії не повинна оцінюватися виключно кількістю вилучених серверів або заблокованих доменів. Стратегічно важливішим є визначення того, чи втратила мережа доступ до клієнтів, фінансових каналів, інструментів, адміністраторів, початкових брокерів доступу або репутації на кримінальному ринку. Такі нематеріальні елементи часто визначають спроможність відновлення швидше, ніж технічне обладнання, яке може бути відносно легко замінене.

Транснаціональний характер організованої кіберзлочинності є не лише наслідком глобальності мережі Інтернет, а структурною умовою її функціонування. В одному кримінальному епізоді організатор може перебувати в одній державі, виконавець – в іншій, серверна інфраструктура – у третій, потерпілий – у четвертій, а обмін або виведення цифрових активів здійснюватися через сервіси, зареєстровані ще в декількох юрисдикціях. У результаті фактичний механізм правопорушення розщеплюється між просторовими, правовими та технологічними середовищами, що істотно ускладнює його цілісне документування.

Для організованих мереж така фрагментація є ресурсом. Відмінності у законодавстві, строках зберігання даних, процедурах доступу до електронної інформації, рівні регуляторного контролю і швидкості міжнародної правової допомоги можуть використовуватися для підвищення стійкості операцій. Технічне встановлення IP-адреси або сервера не гарантує своєчасного отримання відповідної інформації, якщо вона перебуває у володінні іноземного постачальника та може бути швидко видалена. Тому фактор часу у кіберрозслідуваннях набуває системного значення.

Транснаціональність впливає і на спосіб формування злочинної групи. Учасники можуть ніколи не зустрічатися особисто, спілкуватися через захищені месенджери, форуми або приватні канали та знати один одного лише за псевдонімами. Водночас відсутність фізичної взаємодії не означає відсутності організованості. Стійкість може підтримуватися репутацією у підпільному середовищі, повторюваними угодами, гарантійними механізмами кримінальних майданчиків, спільною інфраструктурою та економічною взаємозалежністю.

Ця обставина потребує відмови від надмірно територіального бачення організованої злочинності. У цифровому середовищі ядром групи може бути не місце, а сукупність стійких зв’язків, інфраструктурних залежностей і функціональних ролей. Тому встановлення географічного місцезнаходження учасника є важливим процесуальним завданням, але для кримінального аналізу не менш значущим є визначення його місця у мережі: які ресурси він контролює, які послуги надає, з ким взаємодіє і які наслідки матиме припинення його діяльності.

Міжнародний характер кіберзлочинності закономірно посилює значення спільних операцій, механізмів швидкого обміну даними та синхронізації правоохоронних заходів. Ефективне втручання часто потребує одночасних

обшуків, арештів, вилучення серверів, блокування доменів і заморожування активів у декількох країнах. Якщо такі дії не узгоджені в часі, учасники мережі можуть попередити один одного, перенести інфраструктуру або активи й мінімізувати наслідки операції. Отже, міжнародна координація є не додатковим елементом, а функціональною умовою ефективної протидії транснаціональним кібермережам.

Економічний компонент є системоутворювальним для більшості організованих кіберзлочинних моделей. Навіть технічно складна атака потребує ресурсів на інфраструктуру, доступи, домени, проксі, розробку або придбання програмного забезпечення, оплату виконавців та підтримання каналів комунікації. Отриманий злочинний дохід, своєю чергою, повинен бути переміщений, розподілений і легалізований. Тому фінансова інфраструктура є таким самим критичним елементом злочинної мережі, як і сервери або шкідливий код.

Віртуальні активи стали одним із важливих інструментів транскордонного переміщення коштів, однак їх використання потребує точного наукового трактування. Віртуальні активи не забезпечують повної анонімності розрахунків, оскільки публічні блокчейни зберігають історію транзакцій, що створює можливості для аналітичного простеження. Водночас злочинці використовують складні ланцюги адрес, міжмережеві операції (cross-chain operations), децентралізовані сервіси, міксери, рахунки підставних осіб (mule accounts) та інші інструменти, спрямовані на ускладнення атрибуції. FATF у 2025 році окремо наголосила на транскордонних ризиках кримінального використання віртуальних активів і на тому, що прогалини регулювання в одній юрисдикції можуть мати глобальні наслідки[9].

Показовим прикладом є міжнародна операція проти сервісу «AudiA6», який, за даними Europol, використовувався ransomware-групами та іншими кіберзлочинними мережами для відмивання криптовалютних доходів. Слідство пов'язало цей сервіс із понад п'ятнадцятьма міжнародними кіберрозслідуваннями та підозрювало у відмиванні понад 336 млн євро у 2022–2025 роках[10]. Важливим є не лише масштаб, а сама бізнес-модель: сервіс позиціонувався як професійний засіб «очищення» криптовалюти, використовував складні ланцюги транзакцій, мережу фіктивних облікових записів та стягував комісію. Це наочно ілюструє перетворення відмивання злочинних доходів на окремий спеціалізований сервіс кіберзлочинної екосистеми.

Для правоохоронного аналізу фінансові потоки мають подвійну цінність. По-перше, вони дозволяють реконструювати розподіл доходів і встановлювати ролі учасників. По-друге, фінансова інфраструктура часто є

[9] FATF. Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. 26 June 2025. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html.

[10] Europol. Ransomware gangs cut off from EUR 336 million "AudiA6" crypto laundering pipeline. 11 June 2026. URL: https://www.europol.europa.eu/media-press/newsroom/news/ransomware-gangs-cut-eur-336-million-audia6-crypto-laundering-pipeline.

більш стабільною, ніж технічна: домени та сервери змінюються швидко, тоді як перевірені механізми одержання і переміщення коштів можуть використовуватися тривалий час. Саме тому зіставлення фінансових адрес, біржових акаунтів, mule-мереж, контактів і часових параметрів транзакцій здатне виявляти зв'язки між зовні не пов'язаними епізодами.

При цьому неприпустимо автоматично криміналізувати саме використання віртуальних активів, інструментів конфіденційності або децентралізованих сервісів. Аналітичний висновок має ґрунтуватися на контексті: походженні коштів, структурі транзакцій, зв'язку з відомими адресами або сервісами, повторюваності поведінки та інших незалежних індикаторах. Такий підхід одночасно підвищує доказову якість висновків і зменшує ризик хибної атрибуції легітимної активності як кримінальної.

Однією з найбільш суттєвих сучасних тенденцій є конвергенція кіберзлочинності з традиційними формами транснаціональної організованої злочинності. Цифрові технології дедалі частіше використовуються не лише для атак на інформаційні системи, а як інфраструктура шахрайства, торгівлі людьми, незаконного обігу товарів, відмивання коштів, експлуатації потерпілих та управління кримінальними підприємствами. UNODC у дослідженнях 2024–2025 років звертає увагу на зближення cyber-enabled fraud, underground banking, virtual assets і технологічних сервісів у межах великих транснаціональних кримінальних мереж[11]. Такий процес свідчить про поступове стирання меж між «кіберзлочинністю» і «традиційною» організованою злочинністю.

Особливо показовими є масштабні шахрайські центри, у діяльності яких цифрова інфраструктура поєднується з вербуванням і примусовою експлуатацією людей, нелегальними фінансовими каналами, корупційним захистом та міжнародними мережами відмивання. У цих моделях кіберкомпонент не існує автономно, він є частиною складнішого кримінального підприємства, що може контролювати фізичні об'єкти, персонал, фінансові потоки та інфраструктуру. Для кримінологічної характеристики це важливо, оскільки протидія таким мережам вимагає одночасного застосування інструментів кіберрозслідування, фінансового аналізу, протидії торгівлі людьми та міжнародної взаємодії.

Конвергенція проявляється і у використанні кіберзлочинних сервісів традиційними організованими групами. Викрадені або підроблені цифрові ідентичності можуть використовуватися для відкриття рахунків, оренди інфраструктури, реєстрації сервісів та маскування руху коштів. Скомпрометовані облікові записи можуть слугувати засобом шахрайства або збору інформації, а шифровані комунікації – підтримувати координацію інших видів злочинності. У результаті технічні сервіси кіберпідпілля

[11] UNODC. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. 2024. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

перетворюються на універсальні засоби забезпечення організованої злочинності.

Зворотний процес також має місце. Кіберзлочинні мережі залучають традиційні кримінальні ресурси – money mules, підставних осіб, фізичну логістику, фальшиві документи, корумповані зв'язки або інші механізми, які забезпечують завершення цифрової операції у реальному світі. Саме тому модель «повністю віртуального злочину» є часто спрощеною. Навіть дистанційне шахрайство або ransomware у певний момент стикається з необхідністю монетизації, обміну активів, придбання інфраструктури чи використання реальних ідентичностей.

Наслідком такої конвергенції стає зростання ролі міждисциплінарного кримінального аналізу. Інформація про цифрові ідентифікатори повинна співвідноситися з фінансовими, корпоративними, комунікаційними та іншими відомостями. Виявлення одного технічного індикатора рідко дає повне уявлення про кримінальну структуру. Значно більшу цінність має встановлення того, як він пов'язаний із конкретними особами, рахунками, компаніями, пристроями, фізичними адресами та попередніми епізодами.

Сучасна організована кіберзлочинність дедалі активніше поєднує технічні засоби з методами соціальної інженерії. Посилення технічного захисту інформаційних систем підвищує цінність легітимних облікових даних, токенів сесій та прав доступу. Унаслідок цього людина, яка має доступ до системи, перетворюється на одну з основних цілей атаки. Фішингове повідомлення, телефонний дзвінок, підроблений вебінтерфейс, компрометація корпоративної переписки або підміна цифрової ідентичності можуть бути лише початковим етапом складнішої операції, яка завершується несанкціонованим доступом, викраденням даних, фінансовим шахрайством або ransomware.

Поширення автоматизації дозволяє організованим групам одночасно працювати з великою кількістю цілей. Скрипти, боти, автоматизовані системи перевірки облікових даних, масове сканування вразливостей і модульні комплекти шкідливого програмного забезпечення зменшують потребу у ручній роботі. UNODC у матеріалах 2025 року підкреслює, що автоматизація стала важливим чинником трансформації кіберзлочинності від ізольованих дій до масштабних операцій організованих мереж, а інтеграція штучного інтелекту додатково підвищує швидкість і адаптивність таких процесів[12].

Штучний інтелект у цьому контексті доцільно розглядати передусім як мультиплікатор уже відомих загроз. Генеративні моделі можуть полегшувати створення фішингових повідомлень різними мовами, персоналізацію сценаріїв соціальної інженерії, формування синтетичного аудіо- та відеоконтенту, а також пришвидшувати окремі етапи підготовки технічних засобів. Водночас

[12] UNODC. Emerging threats: the intersection of criminal and technological innovation in the use of automation and AI. 2025. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf.

переоцінювати автономність таких технологій не слід: кримінальний ефект визначається тим, як вони інтегруються в організовану модель, де існують виконавці, інфраструктура, фінансовий канал і механізм монетизації.

Europol у IOCTA 2026 прямо пов'язує сучасну еволюцію кіберзлочинності з одночасним розвитком шифрування, проксі-сервісів та штучного інтелекту (encryption, proxies and AI). Для організованої кіберзлочинності важливим є саме поєднання цих факторів: штучний інтелект підвищує масштаб і правдоподібність атак, проксі- та інші інфраструктурні сервіси ускладнюють ідентифікацію джерела активності, а шифрування захищає комунікацію між учасниками. Сукупно це збільшує часові та аналітичні витрати правоохоронних органів[13].

Разом із тим технології автоматизації створюють для злочинців і нові вразливості. Масове використання однакових шаблонів, скриптів, інфраструктури або сервісів може генерувати повторювані цифрові ознаки, які полегшують виявлення серійності. Саме тому аналітична робота повинна бути спрямована не лише на унікальні елементи атаки, а й на стандартизовані компоненти: структуру доменів, шаблони комунікації, конфігурації серверів, повторювані гаманці, часові закономірності та інші індикатори, що відображають «виробничу» модель злочинної діяльності.

Високий рівень латентності організованої кіберзлочинності зумовлений сукупністю факторів. Потерпілі можуть не виявляти факт компрометації протягом тривалого часу, не повідомляти про інцидент через репутаційні ризики або не усвідомлювати, що окремі події є елементами ширшої злочинної кампанії. Крім того, одна атака може залишати сліди у декількох інформаційних системах, які належать різним суб'єктам і не обмінюються даними між собою. Відтак правоохоронні органи часто отримують лише фрагмент загальної картини, тоді як організатор злочинної операції бачить її структуру цілісно.

Інформаційна асиметрія посилюється тим, що один суб'єкт може фіксувати шахрайську транзакцію, інший – фішинговий домен, постачальник хмарних послуг – підозрілу інфраструктуру, а потерпілий – компрометацію облікового запису. Лише зіставлення цих фрагментів дозволяє встановити серійність, спільну інфраструктуру або роль одного злочинного сервісу в різних епізодах. З цієї причини аналітична цінність міжвідомчого та державно-приватного обміну інформацією полягає не лише у прискоренні реагування, а у формуванні повнішої моделі кримінальної мережі.

Складність атрибуції є окремою характеристикою кіберзлочинності[14]. IP-адреса, домен, зразок шкідливого програмного забезпечення, криптовалютна адреса або ім'я користувача є важливими цифровими

[13] Europol. IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. 28 April 2026. URL: https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape.

[14] Лунгол О. Методологічні засади атрибуції суб'єктів гібридної агресії в національному кіберпросторі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. Вип. 2, Жовтень 2025, с. 374-82, doi:10.28925/2663-4023.2025.30.904.

ідентифікаторами, однак жоден із них не повинен автоматично ототожнюватися з конкретною фізичною особою. Інфраструктура може бути орендованою, викраденою або спільно використовуватися декількома суб'єктами; шкідливий код – копіюватися чи модифікуватися; псевдонім – передаватися або імітуватися. Тому атрибуція повинна будуватися на сукупності незалежних ознак.

Умовно доцільно розмежовувати технічну, інфраструктурну, організаційну та персональну атрибуцію:

- технічна встановлює схожість інструментів і тактик;
- інфраструктурна – зв'язки між доменами, серверами, сертифікатами, адресами та іншими ресурсами;
- організаційна – належність епізодів до певної злочинної мережі;
- персональна – роль конкретної особи.

Методологічною помилкою є механічний перехід від першого рівня до останнього без достатньої доказової бази. Для організованої кіберзлочинності цей ризик особливо високий через орендовану інфраструктуру та сервісну модель.

Звідси випливає і значення довготривалого накопичення та кореляції даних. Окремий технічний збіг може бути випадковим, але повторюваність комбінації ознак – однакових серверів імен, часових моделей, способів входу, фінансових адрес, мовних конструкцій або контактів – суттєво підвищує аналітичну цінність. Унаслідок цього протидія організованій кіберзлочинності потребує не лише реагування на інциденти, а й системного формування кримінальної розвідувальної картини, яка дозволяє зіставляти нові події з уже відомими моделями.

Для України сучасна організована кіберзлочинність функціонує в особливому безпековому середовищі, сформованому повномасштабною збройною агресією Російської Федерації. Кіберпростір одночасно використовується корисливими злочинними групами, хактивістськими мережами, державними та пов'язаними з державою суб'єктами. У результаті подібні технічні інструменти – DDoS, malware, фішинг, компрометація облікових записів, експлуатація вразливостей – можуть застосовуватися з різною мотивацією і мати різну правову природу. Для правоохоронного аналізу це створює потребу особливо ретельно відмежовувати кримінально корисливу, ідеологічно мотивовану та державно керовану активність.

Водночас між цими сегментами можливе використання спільної інфраструктури, інструментів і сервісів. ENISA у Threat Landscape 2025 фіксує випадки, коли суб'єкти, пов'язані з державами (state-nexus actors) використовували кіберзлочинні інструменти та інфраструктуру, а також перетиналися з екосистемами програм-вимагачів і програм-викрадачів даних. Така конвергенція ускладнює атрибуцію і демонструє, що походження

конкретного технічного засобу не завжди безпосередньо визначає мотивацію суб'єкта, який його застосував[15].

Для України особливе значення має також стійкість масових DDoS-мереж, які орієнтуються на державні органи, критичні сервіси та партнерів України. Операція Eastwood проти NoName057(16) показала, що такі структури можуть поєднувати відносно невелике організаційне ядро з широкою географією прихильників і технічними механізмами масового залучення. Це вимагає оцінювати не лише виконавців атак, а й організаторів, адміністраторів інфраструктури, канали координації та механізми стимулювання участі.

Воєнний контекст створює додаткове середовище для соціальної інженерії. Підвищена суспільна увага до гуманітарних виплат, волонтерства, військової тематики, державних сервісів, мобілізаційних процесів і термінових повідомлень формує інформаційні приводи, які можуть використовуватися у фішингових та шахрайських сценаріях. Організовані групи здатні швидко адаптувати легенди до актуальних подій, а це підвищує переконливість повідомлень і ускладнює превентивне інформування населення.

Разом із тим воєнний контекст не повинен призводити до надмірного розширення поняття організованої кіберзлочинності. Не кожна ворожа кібероперація є організованим кримінальним правопорушенням у кримінологічному сенсі, так само як не кожна групова кібератака має державне походження. Науково коректним є розмежування за встановленими ознаками суб'єкта, мотивації, механізму координації, способу фінансування та кінцевої мети, а не лише за технічним результатом атаки.

Для глибшого розуміння специфіки організованої кіберзлочинності доцільно розглядати її не лише через перелік окремих форм, а як послідовний життєвий цикл кримінальної операції. Такий цикл може включати підготовчу розвідку, пошук цілей, придбання або створення технічного інструментарію, отримання первинного доступу, закріплення у системі, розвиток атаки, одержання кримінального результату, монетизацію та подальше приховування доходів. На кожному етапі можуть діяти різні особи та використовуватися різні сервіси, а тому одна кримінальна операція фактично поєднує декілька мікроринків незаконних послуг. Така багатоланковість пояснює, чому припинення одного епізоду не обов'язково руйнує всю структуру.

Підготовчий етап часто починається зі збору відомостей про потенційні цілі, цифрову інфраструктуру, працівників, постачальників та можливі вразливості. Частина такої інформації може бути отримана з легально доступних джерел, частина – придбана у вигляді викрадених баз даних, а частина – сформована шляхом попереднього технічного зондування. Для організованих груп важливим є не саме володіння великим обсягом

[15]ENISA. ENISA Threat Landscape 2025. 1 October 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

відомостей, а здатність перетворити їх на придатну для атаки модель: визначити особу з потрібними правами доступу, вразливий зовнішній сервіс, підрядника або інший елемент, через який можна отримати первинний доступ.

Етап первинного доступу дедалі частіше відокремлюється від подальшої експлуатації. Це означає, що суб'єкт, який компрометує обліковий запис або інформаційну систему, може не мати наміру самостійно здійснювати атаку із застосуванням програми-вимагача чи фінансове шахрайство. Його кримінальним продуктом є сам доступ, який продається іншому учаснику. Така спеціалізація створює важливу точку взаємозалежності: одна й та сама група брокерів первинного доступу (initial access brokers) здатна забезпечувати декілька різних злочинних мереж, а тому встановлення її клієнтських зв'язків може мати значення для розкриття серії зовні не пов'язаних інцидентів.

Подальший розвиток атаки залежить від кінцевої кримінальної мети. У ransomware-моделі пріоритетом може бути розширення привілеїв, переміщення всередині мережі, виявлення резервних копій, ексфільтрація даних і підготовка до шифрування. У шахрайській схемі – встановлення контролю над платіжним або комунікаційним каналом. У крадіжці даних – пошук конкретних масивів інформації та їх непомітне копіювання. При цьому різні операції можуть використовувати однакові початкові інструменти, а відмінність проявляється лише на пізніших етапах. Саме тому рання технічна ознака не завжди дозволяє достовірно визначити кінцевий задум злочинної групи.

Стадія монетизації є критичною для розуміння організованої природи кіберзлочинності. Отриманий доступ, викрадені дані або контроль над системою повинні бути перетворені на економічну вигоду. Це може відбуватися через вимагання, продаж інформації, шахрайські транзакції, подальший перепродаж доступу або використання викрадених ідентичностей. На цьому етапі технічна кібероперація часто з'єднується з традиційними елементами організованої злочинності – mule-мережами, підставними компаніями, фіктивними документами, посередниками та відмиванням доходів.

Завершальний етап не обмежується приховуванням слідів. Організовані групи аналізують результативність кампанії, зберігають перевірені інструменти, формують бази вразливих цілей, переносять ресурси на нову інфраструктуру та повторно використовують успішні сценарії. Таким чином, кожний завершений епізод може підвищувати організаційну спроможність мережі. Саме ця здатність до навчання відрізняє стійке кримінальне підприємство від випадкового правопорушення: накопичений досвід, репутація і технічні напрацювання перетворюються на ресурс для наступних атак.

Окремим системним сегментом організованої кіберзлочинності є ринок викрадених даних. Облікові записи, бази клієнтів, платіжні реквізити, cookie-файли, токени автентифікації, персональні документи та інші цифрові відомості можуть мати самостійну товарну вартість незалежно від первинного

способу їх отримання. Це означає, що наслідки витоку не завершуються моментом компрометації. Дані можуть перепродаватися, агрегуватися, доповнюватися інформацією з інших джерел і використовуватися у нових шахрайських або соціально-інженерних сценаріях протягом тривалого часу.

Ринок цифрових ідентичностей змінює сам механізм злочинної підготовки. Замість створення фіктивної легенди з нуля злочинець може використати реальні персональні дані, історію комунікації, скомпрометований акаунт або платіжний профіль. Це істотно підвищує правдоподібність шахрайського сценарію. Крім того, компрометація одного облікового запису може відкривати доступ до інших сервісів через повторне використання паролів, федеративну автентифікацію (federated login) або збережені сесії. Відтак цифрова ідентичність стає багаторівневим активом, а її викрадення може створювати каскадний ефект.

Комерціалізація даних також пояснює, чому організовані групи можуть спеціалізуватися винятково на їх отриманні, не здійснюючи подальшого шахрайства самостійно. Для них кримінальний результат настає в момент продажу масиву даних або доступу до акаунтів. Інші суб'єкти використовують цей ресурс для фінансових операцій, вимагання, таргетованого фішингу чи обходу процедур ідентифікації. Такий поділ функцій формує ланцюг, у якому одна потерпіла особа або організація може зазнати декількох хвиль вторинної віктимізації.

Особливої уваги потребує співвідношення масових витоків і таргетованої злочинної діяльності. Великі масиви даних створюють можливість автоматизованого відбору потенційно цінних цілей за професією, фінансовим статусом, місцем роботи, доступом до корпоративних систем або іншими ознаками. У такий спосіб первинно масова компрометація перетворюється на інструмент точкового відбору жертв. Це демонструє, що масштаб і персоналізація не є взаємовиключними характеристиками сучасної кіберзлочинності: автоматизація дозволяє поєднувати обидва підходи.

Сучасний стан організованої кіберзлочинності не може бути якісно оцінений лише за кількістю зареєстрованих кримінальних правопорушень. Кількісний показник залежить від виявлення, повідомлення, правової кваліфікації та можливості об'єднати взаємопов'язані епізоди. Значно більш інформативним є поєднання статистичних даних із оцінюванням спроможностей злочинних суб'єктів: доступності кримінальних сервісів, появи нових інструментів, активності підпільних майданчиків, зміни фінансових маршрутів і результатів міжнародних операцій. Саме такий підхід дозволяє відрізняти тимчасове зниження кількості інцидентів від реального зменшення спроможностей злочинної екосистеми.

Динаміка кримінального ринку залежить і від правоохоронного тиску. Ліквідація великого сервісу може створити короткостроковий дефіцит певної послуги, підвищити її вартість, викликати міграцію клієнтів або появу нових постачальників. Водночас успішна операція може мати довгостроковий ефект, якщо вона підриває довіру між учасниками, компрометує анонімність,

розкриває інфраструктурні зв’язки або призводить до втрати значних фінансових ресурсів. Тому оцінка ефективності потребує аналізу поведінки кримінального середовища після втручання, а не лише формальної фіксації його первинних результатів.

Важливою ознакою зрілості організованого кіберзлочинного ринку є його здатність до заміщення дефіцитних ресурсів. Після блокування одного майданчика користувачі переходять до іншого; після припинення діяльності певної ransomware-групи частина афіліатів може перейти до конкурентів; після вилучення серверів розгортаються резервні. Водночас кожна така міграція залишає сліди наступності – повторні контакти, фінансові адреси, стилі комунікації, конфігурації інфраструктури та часові закономірності. Саме ці ознаки мають особливе значення для стратегічного кримінального аналізу.

Отже, стратегічна оцінка організованої кіберзлочинності повинна відповідати не лише на питання «скільки злочинів учинено», а й на питання «які спроможності має кримінальна екосистема», «які її вузли є критичними», «які сервіси забезпечують масштабування», «як швидко мережі відновлюються» та «які зміни відбуваються після правоохоронного втручання». Така постановка питання є більш придатною для визначення пріоритетів діяльності поліції та узгоджується з сучасною логікою оцінювання загроз (threat assessment), що використовується європейськими та міжнародними правоохоронними структурами.

Сукупність наведених тенденцій змінює сам предмет правоохоронного пізнання. Якщо під час розслідування одиничного кіберінциденту увага природно концентрується на конкретному потерпілому, пристрої або інформаційній системі, то протидія організованій кіберзлочинності потребує переходу до реконструкції мережі. Практичне значення мають не тільки окремі цифрові сліди, а їх системні взаємозв’язки: хто контролює інфраструктуру, які ресурси повторно використовуються, яким чином розподіляються функції, хто забезпечує первинний доступ, як відбувається монетизація і які ланки є критичними для стійкості всієї операції.

Такий підхід обґрунтовує необхідність поєднання реактивного і проактивного компонентів. Реактивний спрямований на документування вже вчиненого кримінального правопорушення, встановлення потерпілих і підозрюваних, збереження цифрових доказів. Проактивний полягає у виявленні інфраструктури, спільних індикаторів, повторюваних моделей, кримінальних сервісів і фінансових каналів до того, як вони будуть використані у нових епізодах. Організований характер кіберзлочинності робить другий компонент особливо важливим, оскільки один інфраструктурний вузол може підтримувати значну кількість майбутніх атак.

Особливу роль у цьому процесі відіграє кримінальний аналіз. Його завданням є не механічне накопичення великої кількості даних, а перетворення розрізнених відомостей на перевірене знання про структуру, спроможності та поведінку злочинної мережі. Для цього інформація з кримінальних проваджень має зіставлятися з цифровими ідентифікаторами,

відкритими джерелами, фінансовими даними, результатами технічного аналізу й інформацією міжнародних партнерів. На рівні такої інтеграції можуть бути встановлені зв'язки між епізодами, які окремо виглядають незалежними.

Оцінювання загрози організованої кіберзлочинності доцільно здійснювати у декількох взаємопов'язаних вимірах:

- суб'єктному – хто контролює та забезпечує діяльність;
- інфраструктурному – які цифрові ресурси використовуються;
- операційному – якими є тактики і послідовність дій;
- фінансовому – як формується та переміщується дохід;
- географічному – у яких юрисдикціях перебувають учасники, потерпілі та дані;
- часовому – як змінюється активність і як швидко відновлюється мережа після втручання.

Комплексне використання цих вимірів дозволяє уникнути спрощеного висновку, коли масштаб злочинної мережі оцінюється лише за кількістю зафіксованих епізодів.

Окремого значення набуває аналіз сервісів забезпечення кіберзлочинності (cybercrime enablers) – сервісів і ресурсів, які безпосередньо не завжди є самостійним злочинним продуктом, але забезпечують функціонування великої кількості кримінальних операцій. Сучасна практика Europol дедалі виразніше орієнтується на порушення функціонування (disruption) інфраструктури та сервісів, які обслуговують широке коло злочинних суб'єктів. Для Національної поліції України такий підхід є методологічно важливим: пріоритетним об'єктом аналітичної уваги мають бути вузли, нейтралізація яких здатна порушити діяльність не одного виконавця, а цілого сегмента злочинної екосистеми[16].

Отже, сучасна організована кіберзлочинність є динамічною, мережевою та сервісно орієнтованою формою кримінальної діяльності, що характеризується функціональною спеціалізацією учасників, транснаціональністю, високою адаптивністю, інфраструктурною децентралізацією та професіоналізацією фінансового забезпечення. Її розвиток супроводжується конвергенцією з іншими формами організованої злочинності, поширенням моделі «кіберзлочинність як послуга», активним використанням засобів анонімізації, віртуальних активів, автоматизації та штучного інтелекту. У результаті традиційна модель, орієнтована переважно на встановлення конкретного виконавця окремого епізоду, є недостатньою.

Ефективна протидія такому явищу потребує переходу до системного виявлення і руйнування злочинної екосистеми: її організаційного ядра, критичної цифрової інфраструктури, каналів одержання первинного доступу, сервісів забезпечення, фінансових механізмів і транскордонних зв'язків. Саме ця специфіка визначає потребу у належному нормативно-правовому

[16] Europol. How cybercrime enablers are facilitating crime: live expert session. 13 May 2026. URL: https://www.europol.europa.eu/publications-events/events/how-cybercrime-enablers-are-facilitating-crime.

регулюванні, міжнародній взаємодії та узгодженні повноважень суб'єктів протидії кіберзагрозам, що логічно переходить до наступного підрозділу науково-практичних рекомендацій.

1.2. Нормативно-правове регулювання та передовий міжнародний досвід діяльності поліції щодо протидії кіберзагрозам

В умовах дії особливого правового режиму воєнного стану ключового значення набуває проблема посилення ефективності захисту національної безпеки. Така ефективність може вимірюватись низкою різних критеріїв, одним із яких є стан протидії кримінально протиправній діяльності взагалі та кримінальним правопорушенням, які виокремлені в межах міжнародних та європейських документів зокрема. До таких суспільно небезпечних діянь відносяться кіберзлочини.

Наведене підтверджується положенням ст. 22 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, де вказано, що Сторони співробітничають у боротьбі з кримінальною та незаконною організованою чи іншою діяльністю, а також з метою її попередження. Таке співробітництво спрямовується на вирішення, таких проблем:

a) незаконне переправлення через державний кордон нелегальних мігрантів, торгівля людьми і вогнепальною зброєю та незаконний обіг наркотиків;

b) контрабанда товарів;

c) економічні злочини, зокрема злочини у сфері оподаткування;

d) корупція як у приватному, так і в державному секторі;

e) підробка документів;

f) кіберзлочинність[17].

Одночасно із цим, вивчення статистичної інформації, викладеної на сайті Офісу Генерального прокурора вказує на наявність системних проблем у сфері правоохоронної діяльності: у 2025 році розслідувалось 76555 кримінальних правопорушень у сфері кібербезпеки, підозри особам було вручено у 5680 кримінальних правопорушеннях; станом на квітень 2026 року розслідувалось 74932 кримінальних правопорушень у сфері кібербезпеки, підозри особам було вручено у 2879 кримінальних правопорушеннях[18]. Отже, такі кількісні показники стану кримінально протиправної діяльності у сфері кібербезпеки та дисбаланс у співвідношенні розпочатих кримінальних проваджень та вручення повідомлення про підозру свідчить про те, що на

[17] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

[18] Офіс Генерального прокурора. Статистика. URL: https://www.gp.gov.ua/ua/posts/pro-rezultati-diyalnosti-organiv-pravoporyadku-shodo-stanu-zapobigannya-ta-protidiyi-pravoporushennyam-yaki-vchineno-u-sferi-kiberbezpeki-kiberzlochini

сьогоднішній день стан нормативно-правового забезпечення протидії кіберзлочинам може бути оцінений як незадовільний. Зокрема це стосується заходів кримінально-правової протидії.

Традиційно під нормативно-правовим забезпеченням розуміється сукупність законодавчих та інших актів, які регулюють певну діяльність. Логічним висновком є те, що ефективність правоохоронної діяльності перебуває у безпосередній кореляції із ефективністю правового регулювання, особливо – в умовах трансформації держави та суспільства.

Усі нормативно-правові акти можуть бути диференційовані за ієрархічною ознакою на такі:

1) Конституція України;

2) міжнародні та європейські документи, які визначають засади певної діяльності;

3) національні законодавчі акти;

4) національні підзаконні нормативно-правові акти.

У контексті діяльності Національної поліції України щодо протидії кіберзагрозам, необхідно відзначити, що правове регулювання такої діяльності має також охоплювати супутні напрями, такі як, наприклад, захист прав та свобод громадян у сфері інформаційної безпеки, адміністративно-правове та кримінально-правове забезпечення протидії кіберзлочинності тощо.

Конституційне забезпечення протидії кіберзагрозам. Відповідно до ст. 17 Конституції України, захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом[19].

Право на належний рівень інформаційної безпеки також є конституційно визначеним та фрагментарно закріпленим у ст.ст. 31-32 Конституції України, у яких визначено, що кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України[20]. Разом із цим, в умовах дії особливого правового режиму воєнного стану із урахуванням того, що захист інформаційної безпеки набуває особливого значення із огляду на чисельні інформаційні атаки, Конституцією передбачені окремі випадки, коли права та свободи можуть бути обмежені.

---

[19]Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

[20]Там само.

Зокрема, наприклад, у ст. 64 Основного закону держави визначено, що В умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень. До них також відносяться і ті, що передбачені у ст. 31 та ст. 32[21]. Отже, протидія кіберзагрозам забезпечується приписами Конституції шляхом визначення обов'язку правоохоронних органів забезпечувати інформаційну безпеку.

Міжнародні та європейські документи, які визначають засади певної діяльності. До основних міжнародних та європейських документів у сфері протидії кіберзлочинності доцільно віднести Конвенцію про кіберзлочинність, Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Директиву Європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2).

У 2005 році Україна ратифікувала Конвенцію про кіберзлочинність. У розділі II угоди розглянуто заходи матеріального кримінального права та викладено види кримінальних правопорушень, які диференційовано на декілька груп:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

2) правопорушення, пов'язані з комп'ютерами;

3) правопорушення, пов'язані зі змістом;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав[22].

У 2006 році було ратифіковано додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, у якому було встановлено заборону на такі злочини як:

1) поширення расистського та ксенофобного матеріалу через комп'ютерні системи;

2) погроза з расистських та ксенофобних мотивів;

3) образа з расистських та ксенофобних мотивів;

4) заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства[23].

---

[21] Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

[22] Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

[23] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text

Обидва документи мають на меті запобігання вчиненню кримінальних правопорушень із використанням комп'ютерних систем. Разом із тим, якщо Конвенція криміналізує суто комп'ютерні кримінальні правопорушення, що має на меті забезпечення кібербезпеки, то додатковий протокол встановлює заборону на використання комп'ютерних систем з мотивів нетерпимості та дискримінації. Проте, із огляду на визначене у Законі України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України» поняття кіберзлочину (комп'ютерного злочину) під яким законодавець пропонує розуміти суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України[24], доцільно стверджувати, що для запобігання таким протиправним діянням положення і Конвенції і додаткового протоколу до неї мають важливе значення, зокрема з точки зору потреби у гармонізації національного законодавства та правоохоронної практики до європейського законодавства.

Наступним документом, який було ратифіковано у 2010 році стала Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Зокрема у Конвенції вказано на те, що для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, уживають відповідних заходів безпеки, спрямованих на запобігання випадковому чи несанкціонованому знищенню або випадковій утраті, а також на запобігання несанкціонованим доступу, зміні або поширенню. Кожна Сторона зобов'язується встановити відповідні санкції та засоби правового захисту стосовно порушень положень внутрішнього права, що запроваджують основоположні принципи захисту персональних даних, визначені в цій главі[25].

В умовах поступової інформатизації та діджиталізації суспільних відносин положення наведеного правового документа надали можливість підвищити ефективність захисту персональної інформації осіб під час роботи з автоматизованими системами.

У Директиві Європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) визначено, що кожна держава-член ухвалює національну стратегію кібербезпеки, що визначає стратегічні цілі, ресурси, необхідні для досягнення цих цілей, доречні інструменти політики та регулятивні інструменти з метою досягнення та підтримання високого рівня кібербезпеки. Національна стратегія кібербезпеки включає:

[24] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/rada/show/2163-19#Text

[25] Директива Європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

- цілі та пріоритети стратегії кібербезпеки держави-члена, що, зокрема, охоплюють сектори, зазначені в додатках I та II;

- управлінську систему для досягнення цілей і пріоритетів, зазначених у пункті (a) цього параграфа, включно з політикою, вказаною в параграфі 2;

- управлінську систему, що роз'яснює функції та обов'язки відповідних стейкхолдерів на національному рівні, закладаючи основу для співпраці й координації на національному рівні між компетентними органами, єдиними контактними пунктами та групами CSIRT за цією Директивою, а також для координації та співпраці між цими органами і компетентними органами за секторальними правовими актами Союзу;

- механізм ідентифікації відповідних активів і оцінювання ризиків у дотичній державі-члені;

- визначення інструментів, що забезпечують підготовленість до інцидентів, реагування на них та відновлення після них, зокрема співпрацю публічного і приватного секторів;

- перелік різних органів влади та стейкхолдерів, залучених до реалізації національної стратегії кібербезпеки;

- засади політики для посиленої координації між компетентними органами згідно з цією Директивою та компетентними органами згідно з Директивою (ЄС) 2022/2557 з метою обміну інформацією щодо ризиків, кіберзагроз та інцидентів, а також ризиків, що не стосуються кібербезпеки, загроз та інцидентів і виконання наглядових завдань, залежно від випадку;

- план, включно з необхідними заходами, для посилення загального рівня обізнаності про кібербезпеку серед громадян[26].

Забезпечення єдиного підходу до формування стратегії протидії кіберзагрозам, у першу чергу, є важливим з огляду на поступову євроінтеграцію держави та приведення національного законодавства у відповідність до законодавства Європейського Союзу. Разом із цим, стратегія кожної держави має бути орієнтована на внутрішню безпекову ситуацію, а також умови функціонування державних інституцій та їх взаємодії із суспільством. В умовах збройної агресії російської федерації для України проблема забезпечення кібербезпеки значно загострилась, що зумовлено формуванням нових – зовнішніх загроз, які мають військово-політичний характер.

У вищенаведеній Директиві також відзначено, що у межах національної стратегії кібербезпеки держави-члени, зокрема, ухвалюють політики, які:

- регулюють питання кібербезпеки в ланцюгу постачання продуктів ІКТ і послуг ІКТ, використовуваних суб'єктами для надання послуг;

- включають і конкретизують пов'язані з кібербезпекою вимоги до продуктів ІКТ і послуг ІКТ під час публічних закупівель, зокрема щодо

[26] Директива Європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

сертифікації кібербезпеки, шифрування та використання продуктів у сфері кібербезпеки із відкритим вихідним кодом;

- управляють вразливостями, охоплюючи просування і спрощення скоординованого оприлюднення інформації про вразливості згідно зі статтею 12(1);

- стосуються підтримання загальної доступності, цілісності та конфіденційності публічного ядра відкритого інтернету, включно з кібербезпекою підводних комунікаційних кабелів, де це доречно;

- сприяють розвитку й інтеграції актуальних передових технологій з метою впровадження найсучасніших заходів управління ризиками кібербезпеки; просувають і розвивають освіту та професійну підготовку у сфері кібербезпеки, навички у сфері кібербезпеки, ініціативи з підвищення обізнаності, досліджень і розробок у сфері кібербезпеки, а також настанови з належних практик кібергігієни і відповідних механізмів контролю, спрямовані на громадян, стейкхолдерів та суб'єктів;

- підтримують науково-дослідні установи в розробленні, вдосконаленні та просуванні розгортання інструментів кібербезпеки і захищеної мережевої інфраструктури;

- включають відповідні процедури та належні інструменти обміну інформацією для підтримання добровільного обміну інформацією щодо кібербезпеки між суб'єктами відповідно до права Союзу;

- посилюють базовий рівень кіберстійкості та кібергігієни малих і середніх підприємств, зокрема не включених до сфери застосування цієї Директиви, шляхом надання легкодоступних настанов і допомоги відповідно до їхніх конкретних потреб;

- сприяють активному кіберзахисту[27].

Отже, міжнародні та європейські правові документи утворюють платформу для формування єдиних тенденцій розвитку держав за напрямом забезпечення кібербезпеки. Більшість положень спрямовані на унеможливлення посягань на персональну інформацію, а також на створення умов, які спрощують перешкоджання нормальній роботі інформаційних та телекомунікаційних мереж.

Національні законодавчі акти. Основними законодавчими актами, які регулюють діяльність із забезпечення кібербезпеки є:

- Закон України від 05.07.1994 № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах[28];

[27] Директива Європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

[28] Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

- Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України», 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[29];

- Закон України від 01.06.2010 № 2297-VI «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних[30].

Правові відносини, пов'язані із захистом і обробкою персональних даних регулюються. Відповідно до Закону від 01.06.2010 № 2297-VI «Про захист персональних даних», *під персональними даними* необхідно розуміти відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Відповідно до ст. 11, підставами для обробки персональних даних є:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси[31].

Окремі аспекти обробки та захисту персональної інформації регулюються також Законами України «Про інформацію», «Про електронні комунікації», «Про доступ до публічної інформації», а також низкою підзаконних нормативно-правових актів. Вони визначають особливості

[29] 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

[30] Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

[31] Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

функціонування інформаційних систем, вимоги до захисту інформації, порядок використання електронних сервісів та відповідальність за порушення встановлених вимог.

У ст. 11 Закону України «Про інформацію» визначено, що не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом. Центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних[32].

У ст. 119 Закону України «Про електронні комунікації» вказано, що постачальники електронних комунікаційних послуг повинні забезпечувати і нести відповідальність за схоронність даних щодо кінцевого користувача, отриманих при укладенні договору про надання електронних комунікаційних послуг та наданні електронних комунікаційних послуг, у тому числі щодо: 1) персональних даних споживача…[33].

У ст. 10-1 Закону України «Про доступ до публічної інформації» зазначено, що публічна інформація, що містить персональні дані фізичної особи, оприлюднюється та надається на запит у формі відкритих даних у разі додержання однієї з таких умов:

1) персональні дані знеособлені та захищені відповідно до Закону України «Про захист персональних даних»;

2) фізичні особи (суб'єкти даних), персональні дані яких містяться в інформації у формі відкритих даних, надали свою згоду на поширення таких даних відповідно до Закону України «Про захист персональних даних»;

3) надання чи оприлюднення такої інформації передбачено законом;

4) обмеження доступу до такої інформації (віднесення її до інформації з обмеженим доступом) заборонено законом[34].

Отже, система захисту персональних даних утворена міжнародними, європейськими на національними правовими документами. Одночасно із цим, активний розвиток інформаційно-комунікаційних систем, які спрощують збір, обробку та передачу персональних даних формує нові ризики та загрози у сфері забезпечення їх безпеки. Більшість із них пов'язані із кіберзагрозами, які

[32] Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

[33] Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

[34] Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

можуть призводити до порушення вимог щодо конфіденційності, коректності чи доступності персональних даних.

До основних підзаконних нормативно-правових актів доцільно віднести такі:

– Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», затверджена Указом Президента України від 26.08.2021 року № 447/2021[35];

– Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.2016 року № 242/2016[36];

– Стратегія інформаційної безпеки, завтерджена Указом Президента України від 28.12.2021 року № 685/2021[37];

– Національний план реагування на кіберінциденти, кібератаки та кіберзагрози, затверджений постановою Кабінету Міністрів України від 26.11.2025 року № 1533[38];

– Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності, затверджений постановою Кабінету Міністрів України від 13.11.2025 року № 1471[39];

– Порядок здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, затверджений постановою Кабінету Міністрів України від 17.12.2025 № 1668[40];

– Порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури, затверджений постановою Кабінету Міністрів України від 31.12.2025 № 1799[41];

---

[35] Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», затверджена Указом Президента України від 26.08.2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[36] Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.2016 року № 242/2016. URL:https://zakon.rada.gov.ua/laws/show/242/2016#Text

[37] Стратегія інформаційної безпеки, завтерджена Указом Президента України від 28.12.2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

[38] Національний план реагування на кіберінциденти, кібератаки та кіберзагрози, затверджений постановою Кабінету Міністрів України від 26.11.2025 року № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text

[39] Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності, затверджений постановою Кабінету Міністрів України від 13.11.2025 року № 1471. URL: https://zakon.rada.gov.ua/laws/show/en-sk/1471-2025-%D0%BF?lang=uk#Text

[40] Порядок здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, затверджений постановою Кабінету Міністрів України від 17.12.2025 № 1668. URL: https://zakon.rada.gov.ua/laws/show/1668-2025-%D0%BF#Text

[41] Порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури, затверджений постановою Кабінету Міністрів України від 31.12.2025 № 1799. URL: https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF#Text

– Положення про організаційно-технічну модель кіберзахисту, затверджене постановою Кабінету Міністрів України від 29.12.2021 № 1426[42].

– Порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього, затверджений постановою Кабінету Міністрів України від 28.04.2023 № 415[43];

– Порядок організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку, затверджений постановою Кабінету Міністрів України від 14.05.2015 № 303[44];

– Порядок передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об'єктів кіберзахисту, затверджений наказом Адміністрації Держспецзв'язку від 24.06.2022 № 284[45];

– Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу, затверджені наказом Адміністрації Держспецзв'язку від 30.08.2023 № 773[46].

Таким чином, аналіз нормативно-правового забезпечення протидії кіберзлочинності надає підстави для узагальнюючого висновку щодо того, що в Україні сформовано розгалужену систему нормативно-правових актів, спрямованих на регулювання суспільних відносин у сфері запобігання та виявлення кіберзагроз, реагування на кіберінциденти й кібератаки, захисту інформаційних та інформаційно-комунікаційних систем, а також організації діяльності суб'єктів, уповноважених здійснювати протидію кіберзлочинності.

---

[42] Положення про організаційно-технічну модель кіберзахисту, затверджене постановою Кабінету Міністрів України від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

[43] Порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього, затверджений постановою Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

[44] Порядок організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку, затверджений постановою Кабінету Міністрів України від 14.05.2015 № 303. URL: https://zakon.rada.gov.ua/laws/show/303-2015-%D0%BF#Text

[45] Порядок передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об'єктів кіберзахисту, затверджений наказом Адміністрації Держспецзв'язку від 24.06.2022 № 284. URL: https://zakon.rada.gov.ua/laws/show/z0758-22#Text

[46] Методичні рекомендації щодо підвищення рівня кіберзахисту систем електронного документообігу, затверджені наказом Адміністрації Держспецзв'язку від 30.08.2023 № 773. URL: https://zakon.rada.gov.ua/rada/show/v0773519-23#Text

РОЗДІЛ 2.
ІННОВАЦІЇ ТА СУЧАСНІ ПРАКТИКИ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ Й РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

2.1. Використання інструментів розвідки на основі відкритих джерел (OSINT) та цифрової криміналістики в діяльності поліції

Сучасний етап розвитку правоохоронної діяльності характеризується докорінною трансформацією інформаційного середовища, у якому здійснюється попередження, виявлення, припинення та розслідування кримінальних правопорушень. Стрімкий розвиток інформаційно-комунікаційних технологій, глобальна цифровізація суспільних процесів, поширення електронних сервісів, соціальних мереж, хмарних технологій, мобільних комунікацій та технологій штучного інтелекту зумовили не лише зміну характеру суспільних відносин, а й появу нових механізмів учинення кримінальних правопорушень. Практично будь-яка діяльність людини сьогодні так чи інакше пов’язана з використанням цифрових технологій, а тому залишає інформаційні відображення у цифровому середовищі. За таких умов цифрові дані перетворилися на один із найважливіших об’єктів криміналістичного дослідження та інформаційно-аналітичного забезпечення діяльності правоохоронних органів[47].

Традиційно діяльність поліції ґрунтувалася на роботі з матеріальними слідами кримінального правопорушення, показаннями учасників кримінального провадження, речовими доказами та іншими джерелами доказової інформації. Проте цифровізація суспільства змінила не лише способи вчинення кримінальних правопорушень, а й характер інформації, що використовується під час їх документування та розслідування. Якщо ще двадцять років тому цифрові дані переважно розглядалися як допоміжне джерело відомостей, то сьогодні вони нерідко становлять основу доказової бази. Саме цифрові сліди дозволяють встановити маршрути комунікації між співучасниками, місце перебування особи у певний момент часу, джерела походження електронних документів, механізми поширення шкідливого програмного забезпечення, шляхи руху віртуальних активів, зв’язки між інформаційними ресурсами, а також інші обставини, що мають істотне значення для кримінального провадження[48].

---

[47] OSINT Open Source Intelligence. Інструменти та методи : навчальний посібник / О. Користін, С. Демедюк, К. Ісмайлов, Д. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 7БЦ, 2025. 460 с.; OSINT Open Source Intelligence. Теорія та методологія : монографія / О. Користін, С. Демедюк, О. Барановський, Д. Ланде та ін. Київ : 7БЦ, 2025. 304 с.; Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / В.Ю. Шепітько, ГК. Авдєєва, В.М. Шевчук та ін. ; за заг. ред. В.Ю. Шепітька ; НДІ вивчення проблем злочинності ім. акад. В.В. Сташиса НАПрН України. Харків : Право, 2024. 208 с.

[48] Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / В.Ю. Шепітько, Г.К. Авдєєва, В.М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; НДІ вивчення проблем злочинності ім. акад. В.В. Сташиса НАПрН України. Харків : Право, 2024. 208 с.

Особливість сучасного цифрового середовища полягає в тому, що інформація про діяльність людини формується безперервно. Використання мобільного телефону, авторизація в інформаційній системі, здійснення банківської операції, відвідування вебресурсу, використання навігаційного сервісу, публікація повідомлення у соціальній мережі або навіть автоматична синхронізація мобільного пристрою з хмарним сховищем супроводжуються створенням значної кількості цифрових даних. Значна частина цих даних формується автоматично без активної участі користувача, що суттєво підвищує їх криміналістичну цінність. Водночас саме така особливість цифрового середовища обумовлює необхідність застосування спеціальних методів пошуку, аналізу, верифікації та дослідження інформації, оскільки її обсяг постійно зростає, а структура стає дедалі складнішою.

У сучасній правоохоронній практиці цифрові дані використовуються не лише під час розслідування кіберзлочинів. Аналіз матеріалів кримінальних проваджень свідчить, що інформація, отримана з цифрових джерел, має важливе значення під час розслідування шахрайств, злочинів проти основ національної безпеки України, кримінальних правопорушень, пов'язаних із незаконним обігом наркотичних засобів, торгівлею людьми, легалізацією доходів, одержаних злочинним шляхом, корупційних кримінальних правопорушень, воєнних злочинів та багатьох інших категорій кримінальних правопорушень. У кожному із зазначених випадків цифрові технології виступають або засобом учинення кримінального правопорушення, або способом його приховування, або джерелом інформації, що дозволяє встановити фактичні обставини події[49].

Саме тому сучасна діяльність поліції дедалі більше орієнтується на інформаційно-аналітичну модель роботи. Її сутність полягає не лише у використанні сучасних інформаційних технологій, а передусім у зміні підходів до прийняття управлінських і процесуальних рішень. Якщо раніше першочергове значення мало реагування на вже вчинене кримінальне правопорушення, то сьогодні ключову роль відіграють своєчасне виявлення інформаційних ознак протиправної діяльності, аналіз цифрових взаємозв'язків, прогнозування розвитку криміногенної ситуації та прийняття рішень на підставі комплексного аналізу інформації. Такий підхід відповідає сучасній міжнародній концепції Intelligence-Led Policing, яка передбачає, що інформація та результати її аналітичного опрацювання є основою планування діяльності правоохоронних органів[50].

У межах інформаційно-аналітичної моделі практичну цінність становить не накопичення максимального обсягу даних, а формування на їх основі перевіреного знання, придатного для прийняття управлінських, оперативних і процесуальних рішень. Тому ключовим завданням стає перетворення великих

[49] OSINT Open Source Intelligence. Теорія та методологія : монографія / О. Користін, С. Демедюк, О. Барановський, Д. Ланде та ін. Київ : 7БЦ, 2025. 304 с.; Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

[50] Там само.

масивів різнорідних цифрових даних на структуровану інформацію шляхом їх систематизації, зіставлення, перевірки та аналітичної інтерпретації.

Досягнення цієї мети забезпечується шляхом комплексного використання двох взаємопов'язаних напрямів роботи з цифровою інформацією – розвідки на основі відкритих джерел (Open Source Intelligence, OSINT) та цифрової криміналістики (Digital Forensics). Незважаючи на тісний взаємозв'язок, зазначені напрями виконують різні функції в механізмі правоохоронної діяльності. OSINT забезпечує пошук, збір, систематизацію, перевірку та аналітичне опрацювання інформації, що міститься у відкритих джерелах, тоді як цифрова криміналістика спрямована на виявлення, вилучення, дослідження, інтерпретацію та процесуальне використання цифрових даних, отриманих із електронних носіїв, інформаційних систем і мереж.

Практика діяльності підрозділів Національної поліції України свідчить, що ізольоване використання лише одного із зазначених інструментів суттєво обмежує можливості розслідування. Наприклад, результати OSINT-дослідження можуть дозволити встановити акаунти особи у соціальних мережах, пов'язані електронні адреси, цифрові псевдоніми, доменні імена або криптовалютні гаманці, однак підтвердження причетності конкретної особи до використання відповідних цифрових ресурсів потребує застосування методів цифрової криміналістики. У свою чергу результати дослідження мобільного телефону або комп'ютера нерідко містять нові цифрові ідентифікатори, які стають вихідними даними для подальшого OSINT-дослідження. Таким чином, відкрита розвідка та цифрова криміналістика не конкурують між собою, а утворюють єдину систему роботи з цифровою інформацією.

Використання зазначених інструментів є особливо актуальним в умовах стрімкого розвитку кіберзлочинності. За останні роки суттєво зросла кількість кримінальних правопорушень, пов'язаних із використанням соціальної інженерії, шкідливого програмного забезпечення, фішингових ресурсів, криптовалют, анонімних мереж, технологій маскування цифрової активності та інших сучасних інформаційних технологій. Такі кримінальні правопорушення характеризуються високим рівнем латентності, транснаціональним характером та складною цифровою інфраструктурою. За цих умов традиційні криміналістичні методи вже не забезпечують необхідного рівня ефективності, що обумовлює необхідність широкого впровадження сучасних інформаційно-аналітичних технологій у практичну діяльність поліції.

Особливого значення це набуває в Україні в умовах повномасштабної збройної агресії росії. Використання цифрових технологій для документування воєнних злочинів, виявлення осіб, причетних до їх учинення, аналізу інформаційних операцій, встановлення джерел поширення дезінформації, дослідження цифрових доказів та взаємодії з міжнародними правоохоронними органами суттєво розширило сферу практичного застосування OSINT та цифрової криміналістики. Накопичений досвід

переконливо засвідчив, що сучасна правоохоронна діяльність вже неможлива без системного використання цифрових інструментів пошуку та аналізу інформації[51].

Розширення сфери практичного застосування OSINT у діяльності поліції зумовлює необхідність системного розуміння інформаційного середовища, у межах якого здійснюються пошук, збирання, перевірка та аналітичне опрацювання відкритих даних. Результативність такого дослідження залежить не лише від володіння окремими пошуковими інструментами, а насамперед від правильного визначення інформаційної потреби, обґрунтованого вибору джерел, оцінювання їх надійності та здатності встановлювати змістовні зв'язки між розрізненими відомостями. Тому розгляд практичних можливостей OSINT доцільно розпочати з характеристики відкритих джерел інформації, їх особливостей та значення для вирішення конкретних завдань правоохоронної діяльності.

Однією з визначальних особливостей сучасного інформаційного суспільства є безперервне зростання обсягів інформації, що перебуває у відкритому доступі. Цифровізація державного управління, розвиток електронної демократії, функціонування відкритих державних реєстрів, активне використання соціальних мереж, інформаційних платформ, електронних засобів масової інформації, геоінформаційних сервісів та інших цифрових ресурсів суттєво розширили інформаційні можливості правоохоронних органів. Якщо ще кілька десятиліть тому значна частина відомостей про фізичних та юридичних осіб була доступною лише шляхом направлення офіційних запитів або проведення процесуальних дій, то сьогодні істотний обсяг інформації може бути отриманий із законних відкритих джерел із дотриманням вимог національного законодавства та міжнародних стандартів захисту прав людини.

Водночас необхідно усвідомлювати, що відкритість інформації не означає її автоматичної придатності для використання у правоохоронній діяльності. Відкриті джерела характеризуються значною неоднорідністю як за змістом, так і за рівнем достовірності, актуальності та повноти. Одні інформаційні ресурси містять офіційні відомості, отримані в результаті виконання державними органами своїх повноважень, інші формуються користувачами самостійно, без будь-якої перевірки достовірності оприлюднених матеріалів. Крім того, сучасний інформаційний простір активно використовується для поширення маніпулятивного контенту, інформаційно-психологічних операцій, дезінформації, фейкових повідомлень та інших інформаційних впливів, що значно ускладнює процес оцінювання отриманих відомостей.

[51] Пашковський М. І. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. *Концептуальні основи цифровізації кримінального провадження України* : монографія / за ред. Н. В. Глинської. Харків : Право, 2024. С. 233-274.; 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. New York ; Geneva : United Nations, 2022. 166 p.

Саме тому одним із ключових принципів використання відкритої інформації у діяльності поліції є *принцип критичної оцінки джерела*. Практичну цінність для правоохоронної діяльності має не лише зміст отриманої інформації, а й розуміння походження відповідних відомостей, способу їх формування, часу оприлюднення, можливих мотивів автора, умов поширення та потенційних ризиків викривлення змісту. У зв'язку з цим обов'язковою складовою OSINT-дослідження є оцінювання надійності джерел, перевірка походження отриманих відомостей, установлення їх актуальності та виявлення можливих ознак інформаційних маніпуляцій[52].

Варто наголосити, що відкриті джерела інформації сьогодні не обмежуються лише вебсайтами або соціальними мережами. Інформаційне середовище, доступне для аналізу, є значно ширшим і включає різноманітні категорії ресурсів, які відрізняються між собою за способом формування, функціональним призначенням, юридичним статусом та інформаційною цінністю. Саме тому їх систематизація є важливою передумовою ефективного застосування методів відкритої розвідки у практичній діяльності поліції.

З урахуванням сучасного стану розвитку інформаційного простору відкриті джерела, що використовуються в діяльності поліції, доцільно класифікувати за їх функціональним призначенням та характером інформації, яку вони містять. Такий підхід дозволяє не лише систематизувати різноманітні інформаційні ресурси, а й визначити особливості їх використання для вирішення конкретних правоохоронних завдань.

Першу групу становлять *офіційні державні інформаційні ресурси*. До них належать державні реєстри, офіційні вебпортали органів державної влади та місцевого самоврядування, електронні судові ресурси, відкриті набори даних, системи публічних закупівель, реєстри юридичних осіб, декларацій, ліцензій, судових рішень та інші інформаційні ресурси, що функціонують відповідно до законодавства України. Особливістю цієї категорії джерел є високий рівень достовірності інформації, офіційний характер її походження та можливість використання отриманих відомостей як орієнтуючої інформації під час планування слідчих (розшукових) дій і оперативно-розшукових заходів.

Другу групу становлять *ресурси соціальних медіа*, які в сучасних умовах перетворилися на одне з найінформативніших джерел відомостей про цифрову активність особи. Публікації користувачів, фотографії, відеозаписи, коментарі, реакції, інформація про контакти, участь у спільнотах, професійні зв'язки, географічні позначки та інші цифрові відомості дозволяють формувати уявлення про соціальні зв'язки особи, її інтереси, коло спілкування, маршрути пересування, професійну діяльність та інші характеристики, які можуть мати значення для кримінального провадження. Разом із тим саме ця категорія джерел потребує найбільш ретельної перевірки,

[52] OSINT Open Source Intelligence. Теорія та методологія : монографія / О. Користін, С. Демедюк, О. Барановський, Д. Ланде та ін. Київ : 7БЦ, 2025. 304 с.; 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. New York ; Geneva : United Nations, 2022. 166 p.

оскільки значна частина інформації може бути навмисно змінена, прихована або сфальсифікована.

Важливу групу відкритих джерел становлять *інформаційно-медійні ресурси*, до яких належать електронні засоби масової інформації, інформаційні агентства, офіційні пресрелізи, публічні заяви, тематичні інформаційно-аналітичні платформи та інші ресурси, що відображають поточні події й суспільно значущі процеси. Їх використання дає змогу відстежувати розвиток подій у часовій послідовності, встановлювати первинні повідомлення про певний факт, зіставляти різні версії його висвітлення та виявляти інформаційні взаємозв'язки між подіями, особами й організаціями. Водночас інформація медійного походження потребує критичної перевірки, оскільки швидкість її поширення, конкуренція за увагу аудиторії, залежність від первинних повідомлень та можливість цілеспрямованого інформаційного впливу створюють ризики поширення неповних, викривлених або неперевірених відомостей. Тому під час OSINT-дослідження важливого значення набувають установлення першоджерела повідомлення, аналіз часу його появи, зіставлення з незалежними джерелами та відокремлення фактичних відомостей від оцінних суджень і припущень.

Окрему категорію становлять *геоінформаційні та картографічні ресурси*, значення яких останніми роками суттєво зросло. Використання супутникових знімків, цифрових карт, сервісів панорамного перегляду місцевості, відкритих навігаційних платформ, сервісів моніторингу транспортних засобів, авіаційного та морського руху створює додаткові можливості для встановлення місця перебування особи, аналізу маршрутів пересування, дослідження місця події, документування змін обстановки та перевірки показань учасників кримінального провадження. Особливо важливого значення геопросторовий аналіз набув під час документування воєнних злочинів, коли саме супутникові знімки та відкриті картографічні сервіси дозволяють підтвердити факт руйнування об'єктів цивільної інфраструктури, переміщення військової техніки або зміну обстановки на місцевості.

Не менш важливу роль відіграють *технічні відкриті джерела інформації*, які містять відомості про цифрову інфраструктуру мережі Інтернет. До них належать відкриті сервіси аналізу доменних імен, IP-адрес, автономних систем, цифрових сертифікатів, мережевих сервісів, відкритих портів, електронних поштових серверів, історичних записів DNS та інших технічних параметрів функціонування інформаційних систем. Аналіз таких відомостей є одним із базових напрямів сучасної кіберрозвідки та широко застосовується підрозділами кіберполіції під час документування фішингових кампаній, розслідування атак із використанням шкідливого програмного забезпечення, встановлення інфраструктури злочинних угруповань та ідентифікації серверів, що використовуються для вчинення кримінальних правопорушень.

Особливу категорію відкритих джерел становлять *ресурси, пов'язані з віртуальними активами та технологією блокчейн*. Незважаючи на

використання криптографічних механізмів захисту, більшість публічних блокчейн-мереж забезпечує відкритість інформації про транзакції, що дозволяє здійснювати аналіз руху цифрових активів, встановлювати взаємозв'язки між криптовалютними адресами, виявляти фінансові потоки та документувати незаконні операції. У сучасній практиці правоохоронних органів блокчейн-аналітика стала самостійним напрямом OSINT-досліджень і широко застосовується під час протидії фінансуванню тероризму, легалізації доходів, отриманих злочинним шляхом, онлайн-шахрайствам та іншим кримінальним правопорушенням, пов'язаним із використанням віртуальних активів.

Незважаючи на різноманітність відкритих джерел, їх ефективне використання можливе лише за умови системного підходу до пошуку та аналізу інформації. Саме тому в сучасній правоохоронній діяльності дедалі більшого значення набуває не окремий інформаційний ресурс, а методологія його використання. Працівник поліції повинен розуміти, яку інформацію доцільно шукати на певному етапі розслідування, які джерела можуть містити необхідні відомості, яким чином перевірити їх достовірність та як інтегрувати отримані результати у загальну систему доказування.

Практична реалізація OSINT-дослідження потребує використання інструментів, здатних забезпечити пошук, збирання, структурування, зіставлення, верифікацію та візуалізацію відкритих даних. Сучасний інструментарій охоплює пошукові системи, спеціалізовані сервіси й аналітичні платформи, засоби дослідження цифрових ідентифікаторів, метаданих, соціальних мереж, геопросторової та мережевої інформації, а також даних про рух віртуальних активів. Вибір конкретного засобу визначається характером вихідних даних, типом досліджуваного об'єкта та поставленим правоохоронним завданням. Тому, професійне OSINT-дослідження ґрунтується не на кількості використаних сервісів, а на обґрунтованій послідовності їх застосування.

Базовий рівень інструментального забезпечення OSINT становлять *універсальні та спеціалізовані пошукові системи*, можливості яких виходять далеко за межі звичайного введення ключових слів у пошуковий рядок. Результативний пошук відкритої інформації передбачає формування пошукової стратегії, використання точних словосполучень, альтернативних варіантів написання імен, назв та цифрових ідентифікаторів, застосування мовних і часових обмежень, а також операторів розширеного пошуку. Поєднання таких прийомів дає змогу звужувати інформаційний масив, виявляти документи певних форматів, здійснювати пошук у межах конкретного домену або вебресурсу, знаходити згадки про електронні адреси, номери телефонів, псевдоніми та інші ідентифікаційні ознаки.

У практичній діяльності важливо враховувати, що різні пошукові системи застосовують відмінні алгоритми індексації, ранжування та персоналізації результатів. Тому відсутність необхідної інформації у результатах одного пошукового сервісу не може розглядатися як підтвердження її відсутності у

відкритому інформаційному просторі. Комплексний пошук передбачає зіставлення результатів, отриманих за допомогою різних пошукових систем, варіювання формулювання запитів, використання синонімів, транслітерації, попередніх найменувань об'єктів, різних мовних версій та інших пошукових ознак. Особливого значення такий підхід набуває під час встановлення цифрової присутності особи, дослідження діяльності організації або виявлення інформаційних зв'язків між різними цифровими об'єктами.

Окремим напрямом є застосування *операторів розширеного пошуку*, які забезпечують цільове виявлення інформації за визначеними параметрами. Залежно від функціональних можливостей пошукової системи вони дають змогу обмежувати пошук конкретним вебресурсом, типом файлу, фрагментом URL-адреси, заголовком сторінки або точною словесною конструкцією. Для діяльності поліції цінність такого підходу полягає в можливості швидкого переходу від широкого інформаційного масиву до сукупності потенційно релевантних матеріалів, що підлягають подальшій перевірці, зіставленню та аналітичному опрацюванню.

Окреме місце в інструментарії OSINT посідають *засоби ретроспективного дослідження вебресурсів*. Динамічність цифрового середовища зумовлює ситуації, за яких інформація, що становить інтерес для правоохоронної діяльності, може бути змінена або видалена її власником, адміністратором ресурсу чи платформою, на якій вона була оприлюднена. Водночас припинення доступності певного матеріалу за первинною адресою не завжди означає його повне зникнення з інформаційного простору. Попередні версії вебсторінок, окремі публікації, зображення, документи та відомості про структуру ресурсу можуть зберігатися у вебархівах, пошукових індексах, републікаціях, цитуваннях та інших цифрових відображеннях.

Одним із найбільш відомих засобів ретроспективного аналізу вебконтенту є *Wayback Machine* – сервіс, що забезпечує доступ до архівних копій вебсторінок, збережених у різні періоди часу. Його використання дає можливість досліджувати зміни змісту вебресурсу, встановлювати попередні контактні дані, назви організацій, відомості про осіб, структуру сайту та іншу інформацію, яка була публічно доступною на момент архівування. Для діяльності поліції ретроспективний аналіз може мати значення під час дослідження історії функціонування шахрайських ресурсів, фішингових сторінок, вебсайтів фіктивних суб'єктів господарювання, інформаційних ресурсів, пов'язаних із поширенням протиправного контенту, а також для встановлення попередніх зв'язків між цифровими об'єктами[53].

Разом із тим результати вебархівування потребують критичного оцінювання. Архівна копія відображає стан вебресурсу на певний момент і може не містити всіх його елементів. Динамічний контент, інтерактивні компоненти, окремі зображення, відеоматеріали або зовнішні файли можуть зберігатися неповністю. Тому відсутність певної інформації в архівній копії не

[53] OSINT Open Source Intelligence. Інструменти та методи : навчальний посібник / О. Користін, С. Демедюк, К. Ісмайлов, Д. Ланде та ін. ; за заг. ред. О.Є. Користіна, С.В. Демедюка. Київ : 7БЦ, 2025. 460 с.

є достатньою підставою для висновку, що така інформація не була розміщена на відповідному ресурсі. Під час аналізу важливо враховувати дату архівування, повноту збереженої копії, структуру посилань та співвідносити отримані відомості з іншими незалежними джерелами.

Наступну групу *становлять інструменти пошуку та зіставлення цифрових ідентифікаторів*. У процесі OSINT-дослідження вихідними даними нерідко є окремі інформаційні ознаки: адреса електронної пошти, номер телефону, ім'я користувача, псевдонім, доменне ім'я, фотографія профілю або інший цифровий ідентифікатор. Кожен із таких об'єктів може використовуватися як початкова точка для встановлення пов'язаних інформаційних ресурсів і формування подальших пошукових гіпотез.

Особливе значення має *аналіз імен користувачів і цифрових псевдонімів*. Практика використання цифрових платформ свідчить, що користувачі нерідко застосовують однакові або схожі псевдоніми в різних соціальних мережах, форумах, сервісах обміну контентом, торговельних майданчиках та інших цифрових середовищах. Спеціалізовані засоби пошуку за ім'ям користувача дають змогу перевіряти наявність відповідного ідентифікатора на значній кількості платформ і формувати початкову карту цифрової присутності. Водночас збіг псевдоніма не може автоматично розглядатися як підтвердження належності різних облікових записів одній особі. Такий результат має характер пошукової ознаки й потребує перевірки за сукупністю інших характеристик: фотографіями, контактними даними, часовими параметрами активності, мовними особливостями, соціальними зв'язками та іншими незалежними індикаторами.

Пошук за адресою електронної пошти також може використовуватися для встановлення її відкритих згадок, зв'язків із вебресурсами, професійними профілями, публікаціями, доменами або іншими цифровими об'єктами. У цьому контексті важливого значення набуває не лише виявлення факту згадки електронної адреси, а й дослідження контексту її використання, часу появи, стабільності зв'язку з певним суб'єктом та відповідності іншим установленим відомостям.

Аналогічний підхід застосовується до номерів телефонів. Відкриті згадки номера можуть міститися в оголошеннях, профілях, публічних каталогах, комерційних пропозиціях, повідомленнях про шахрайство та інших ресурсах. Проте результати такого пошуку потребують особливо обережної інтерпретації, оскільки номер може змінювати власника, використовуватися кількома особами або бути неправдиво зазначеним стороннім користувачем. Тому встановлення факту відкритої згадки номера є лише елементом інформаційної моделі й не може ізольовано підтверджувати причетність особи до певної діяльності.

Серед спеціалізованих програмно-аналітичних засобів, що використовуються для дослідження цифрової присутності особи та пов'язаних із нею інформаційних об'єктів, окреме місце посідає програмно-пошуковий модуль Big Data People (Artellence). Його функціональні можливості

поєднують пошук за фотозображенням, аналіз текстової інформації, очищення та структурування значних масивів різнорідних даних, побудову графів зв'язків, геопозиціонування та часовий аналіз цифрової активності. На відміну від інструментів, орієнтованих на виконання однієї пошукової операції, Artellence забезпечує послідовне розширення дослідження: від первинного цифрового ідентифікатора до встановлення пов'язаних профілів, інформаційних зв'язків та інших об'єктів, що потребують подальшої перевірки[54].

Практично важливою функцією платформи є фотопошук. У цьому випадку вихідним об'єктом дослідження є зображення особи, за яким система здійснює пошук імовірних відповідностей у доступному їй інформаційному масиві. Результат подається не лише як факт можливого збігу: в описаних прикладах система пов'язує знайдені зображення із джерелами їх виявлення, зокрема соціальними профілями та Telegram-ресурсами, а результати можуть зіставлятися за датою, джерелом і ступенем відповідності. Це дозволяє використовувати фотозображення як початкову точку ширшого OSINT-дослідження – для пошуку пов'язаних цифрових профілів, аналізу історії появи зображення та встановлення інших інформаційних зв'язків.

Наступний рівень роботи пов'язаний із *побудовою графів зв'язків*. Після виявлення пов'язаних інформаційних об'єктів вони можуть бути представлені у вигляді мережі взаємозв'язків між профілями, контактами, цифровими ідентифікаторами та іншими елементами дослідження. Для діяльності поліції цінність такого підходу полягає в можливості перейти від аналізу окремої особи до дослідження її інформаційного оточення, виявлення повторюваних контактів і потенційно значущих вузлів мережі. Водночас візуалізований системою зв'язок має розглядатися як аналітична ознака, значення якої встановлюється шляхом подальшої перевірки, а не як самодостатнє підтвердження характеру відносин між особами.

Окремий функціональний напрям Artellence пов'язаний із семантичним аналізом текстової інформації. Платформа використовує методи обробки природної мови для виявлення повторюваних лексичних конструкцій і семантичних патернів у цифровому контенті. У дослідженні платформи описано можливість класифікації тематичної та ідеологічної спрямованості інформаційної активності користувачів, що може застосовуватися під час аналізу цифрових спільнот, інформаційних кластерів та мережевої взаємодії. Практична цінність такого функціоналу полягає не в автоматичному формуванні висновку щодо особи, а у виявленні інформаційних закономірностей, які можуть бути використані для формування й подальшої перевірки аналітичних гіпотез.

Важливим є також поєднання просторового та часового аналізу цифрової активності. Відомості про місце, час появи інформаційного об'єкта,

[54] Мовчан А.В., Крутік Ю.Ю., Горбенко Г.М. Інформаційне забезпечення кримінального аналізу // Інформаційно-аналітичне забезпечення діяльності Національної поліції України : монографія / за заг. ред. О.Є. Користіна. Київ : ВД «Дакор», 2024. Розд. 14.

послідовність цифрових подій і взаємодію між встановленими профілями можуть аналізуватися у взаємозв'язку. Це створює можливість не лише встановити наявність певного цифрового сліду, а й дослідити його місце у загальній хронології подій, зіставити з іншими інформаційними об'єктами та визначити напрями подальшої перевірки.

Практичне значення Artellence полягає у формуванні послідовно розширюваної інформаційної моделі досліджуваного об'єкта. Виявлений цифровий профіль може стати основою для встановлення пов'язаних інформаційних об'єктів, дослідження контактного оточення, просторово-часових характеристик та повторюваних моделей цифрової активності. Водночас результати автоматизованого пошуку й алгоритмічного аналізу потребують перевірки за незалежними джерелами та не можуть розглядатися як самодостатнє підтвердження встановлених зв'язків.

Дослідження цифрової присутності особи нерідко потребує переходу від аналізу її персональних цифрових ідентифікаторів до встановлення зв'язків із юридичними особами, фізичними особами-підприємцями, пов'язаними суб'єктами господарювання, судовими провадженнями, виконавчими провадженнями, публічними закупівлями, санкційними обмеженнями та іншими відомостями, доступними у формі відкритих даних. У цьому контексті важливого значення набувають українські аналітичні системи, які агрегують інформацію з офіційних державних джерел, структурують її та створюють можливості для комплексного дослідження зв'язків між особами, компаніями та іншими об'єктами.

Однією з таких систем є *YouControl* – інформаційно-аналітична платформа, що агрегує та структурує відомості з численних офіційних джерел і відкритих державних даних. Функціональні можливості системи дають змогу досліджувати реєстраційні відомості про юридичних осіб і фізичних осіб-підприємців, історію змін, структуру власності та керівництва, зв'язки між суб'єктами, судові рішення, виконавчі провадження, санкційні обмеження та інші інформаційні характеристики. Офіційний ресурс платформи зазначає агрегацію даних із понад 180 державних реєстрів та інших офіційних джерел.

Для правоохоронної діяльності цінність YouControl полягає передусім у можливості аналізувати не окрему реєстраційну картку суб'єкта, а сукупність взаємопов'язаних відомостей. Наприклад, дослідження юридичної особи може передбачати зіставлення часу її реєстрації зі змінами керівників і засновників, аналіз пов'язаних суб'єктів, перевірку судової історії, участі у публічних закупівлях, наявності санкційних та інших ризикових факторів. У результаті формується інформаційна модель, яка може сприяти виявленню нетипових корпоративних зв'язків, повторюваності одних і тих самих осіб у структурі різних юридичних осіб, одночасних або послідовних змін реєстраційних відомостей та інших обставин, що потребують подальшої перевірки.

Важливою перевагою аналітичних систем цього типу є можливість дослідження історичної динаміки даних. Поточний стан реєстраційних

відомостей не завжди відображає всю систему попередніх зв'язків досліджуваного суб'єкта. Зміна керівника, засновника, місцезнаходження, виду економічної діяльності або інших характеристик може мати аналітичне значення лише за умови їх розгляду в часовій послідовності та зіставлення з іншими подіями. Саме тому ретроспективний аналіз корпоративних даних може доповнювати результати пошуку за персональними цифровими ідентифікаторами та допомагати переходити від аналізу окремої особи до дослідження ширшої мережі пов'язаних суб'єктів[55].

Іншим важливим українським ресурсом роботи з відкритими державними даними є *Opendatabot*. Платформа забезпечує пошук та аналітичне представлення офіційних відомостей про українські компанії, фізичних осіб-підприємців та інші об'єкти, інформація про які міститься у відкритих державних даних. Сервіс також надає інструменти перевірки компаній, санкційних обмежень і юридичних ризиків, а його API забезпечує доступ до даних низки українських державних реєстрів.

Практична цінність Opendatabot у межах OSINT-дослідження полягає у швидкому переході від первинного ідентифікатора – назви юридичної особи, коду ЄДРПОУ, прізвища та імені фізичної особи-підприємця або іншої відомої ознаки – до структурованої сукупності відкритих даних. Отримані результати можуть використовуватися для уточнення реєстраційного статусу суб'єкта, встановлення пов'язаних відомостей, аналізу змін і визначення напрямів подальшої перевірки через первинні офіційні джерела[56].

Водночас використання YouControl, Opendatabot та інших агрегаторів відкритих державних даних потребує правильного розуміння їх місця в OSINT-дослідженні. Аналітична система полегшує пошук, структурування, зіставлення та візуалізацію інформації, однак її результати не повинні автоматично підміняти перевірку первинного джерела у випадках, коли походження, актуальність або точний юридичний статус відомостей мають істотне значення. У професійному OSINT-дослідженні агрегована інформація є ефективним засобом виявлення зв'язків і формування пошукових гіпотез, тоді як ключові обставини підлягають перевірці за першоджерелами та, залежно від характеру завдання, отриманню й закріпленню в установленому законом порядку.

Можливості OSINT не обмежуються встановленням відомостей про фізичних і юридичних осіб, аналізом їх цифрової присутності та виявленням взаємозв'язків між ними. Значний масив криміналістично значущої інформації може бути отриманий у процесі дослідження технічних компонентів цифрового середовища, які використовуються для створення, розміщення та функціонування вебресурсів, забезпечення електронних комунікацій і

[55] OSINT Open Source Intelligence. Інструменти та методи : навчальний посібник / О. Користін, С. Демедюк, К. Ісмайлов, Д. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 7БЦ, 2025. 460 с.; YouControl. Аналітична система для комплаєнсу, аналізу ринків, ділової розвідки та розслідувань URL: https://youcontrol.com.ua/about_us/

[56] Там само; Opendatabot. Сервіс моніторингу відкритих державних даних. URL: https://opendatabot.ua/open/about

реалізації протиправних схем у кіберпросторі. Доменне ім’я, URL-адреса, IP-адреса, DNS-записи, цифрові сертифікати та інші технічні ідентифікатори можуть виступати вихідними точками OSINT-дослідження та сприяти встановленню взаємозв’язків між окремими елементами цифрової інфраструктури.

Особливого значення дослідження таких об’єктів набуває під час виявлення та розслідування фішингу, онлайн-шахрайства, поширення шкідливого програмного забезпечення та інших кримінальних правопорушень, у механізмі яких використовуються вебресурси й мережева інфраструктура. У таких випадках завдання полягає не лише у встановленні актуальних характеристик конкретного домену або IP-адреси. Не менш важливим є дослідження історії їх використання, змін технічної конфігурації, пов’язаних піддоменів, серверів імен, цифрових сертифікатів та інших ознак, сукупний аналіз яких може виявити зв’язки між ресурсами, що на перший погляд функціонують незалежно один від одного.

Первинне дослідження доменного імені передбачає роботу з реєстраційними та технічними відомостями. Дані WHOIS і RDAP, а також результати аналізу DNS-записів дають змогу отримати інформацію про дату реєстрації домену, реєстратора, сервери імен, пов’язані адреси та інші характеристики. Проте практична цінність цих відомостей розкривається саме під час їх зіставлення. Наприклад, використання різними вебресурсами однакових серверів імен, повторюваних елементів реєстраційних даних або послідовної зміни IP-адрес може сформувати пошукову гіпотезу щодо можливого технічного зв’язку між ними. Такий зв’язок потребує подальшої перевірки й не може встановлюватися на підставі одиничного технічного збігу.

Для дослідження поточного та попереднього стану доменної інфраструктури застосовуються спеціалізовані сервіси, зокрема SecurityTrails, який дає змогу працювати з DNS-даними, піддоменами та історією змін окремих характеристик доменної інфраструктури. Практичне значення ретроспективного аналізу полягає в можливості простежити технічну історію ресурсу навіть після зміни його поточної конфігурації. У поєднанні з архівними копіями вебсторінок це дозволяє зіставляти зміни змісту ресурсу зі змінами його технічного середовища та формувати більш повну хронологію функціонування досліджуваного об’єкта.

Дослідження підозрілих вебресурсів може бути доповнене використанням urlscan.io, функціональні можливості якого дозволяють аналізувати технічні взаємодії, що виникають під час завантаження вебсторінки. Для аналітика важливим є те, що візуально простий вебресурс може звертатися до низки зовнішніх доменів, серверів і ресурсів, завантажувати сценарії та інші компоненти. Виявлення таких взаємодій розширює початкову інформаційну модель і може вказати на додаткові об’єкти, які потребують перевірки.

Для зіставлення різних типів технічних індикаторів доцільним є використання VirusTotal[57]. Його аналітичне значення полягає в можливості досліджувати взаємозв'язки між URL-адресами, доменами, IP-адресами та файлами. У практичному OSINT-дослідженні це дає змогу перейти від одного відомого індикатора до сукупності потенційно пов'язаних цифрових об'єктів. Водночас виявлені платформою технічні зв'язки потребують змістовної оцінки: спільна IP-адреса, звернення до одного зовнішнього ресурсу або інший технічний збіг самі по собі не підтверджують спільного адміністрування чи єдиного походження досліджуваних ресурсів.

Поряд із дослідженням цифрових ідентифікаторів та технічної інфраструктури важливим напрямом OSINT у діяльності поліції є перевірка цифрового контенту. Фотографії та відеозаписи, оприлюднені у соціальних мережах, месенджерах, засобах масової інформації та на інших цифрових платформах, можуть містити відомості про місце, час і обставини події, осіб та об'єкти, зафіксовані в кадрі, характер змін обстановки, а також інші фактичні дані, що становлять інтерес для правоохоронної діяльності. Водночас поширеність повторних публікацій, зміна контексту, редагування зображень, синтетичне генерування контенту та використання технологій штучного інтелекту істотно ускладнюють оцінювання походження й достовірності таких матеріалів.

Верифікація цифрового зображення передбачає не одну окрему перевірку, а послідовне дослідження його походження, історії поширення, змісту та контексту. Одним із початкових прийомів є зворотний пошук за зображенням, який дозволяє виявляти попередні публікації, візуально подібні матеріали, модифіковані версії фотографії та вебресурси, на яких вона з'являлася раніше. Зіставлення часу появи різних копій може сприяти встановленню ранніх публікацій і перевірці тверджень щодо місця та обставин створення матеріалу. Однак найраніша знайдена публікація не завжди є першоджерелом, оскільки частина попередніх матеріалів може бути видалена, не проіндексована пошуковими системами або поширюватися в закритих інформаційних середовищах.

Тому, результати зворотного пошуку мають поєднуватися з візуальним аналізом змісту зображення. Інформаційне значення можуть мати архітектурні об'єкти, дорожні знаки, назви установ, написи, особливості дорожньої розмітки, елементи ландшафту, рельєф місцевості, погодні умови, напрямок і довжина тіней та інші візуальні орієнтири. Сукупне дослідження таких ознак створює основу для геолокації – встановлення ймовірного місця створення фото- або відеоматеріалу шляхом зіставлення візуальних характеристик із картографічними матеріалами, супутниковими знімками, панорамами місцевості та іншими відкритими джерелами.

Для перевірки цифрового контенту застосовується комплекс взаємодоповнювальних інструментів. Зворотний пошук зображень може

[57] OSINT Open Source Intelligence. Інструменти та методи : навчальний посібник / О. Користін, С. Демедюк, К. Ісмайлов, Д. Ланде та ін. ; за заг. ред. О.Є. Користіна, С.В. Демедюка. Київ : 7БЦ, 2025. 460 с.

здійснюватися за допомогою Google Lens, TinEye та інших пошукових систем, алгоритми яких по-різному індексують і зіставляють візуальний контент. Їх використання дає змогу виявляти попередні публікації, копії та модифіковані версії зображень, а також встановлювати вебресурси, на яких відповідний матеріал поширювався раніше. Результати такого пошуку потребують зіставлення, оскільки відсутність збігу в одній системі не свідчить про відсутність матеріалу в цифровому середовищі.

Додатковим джерелом відомостей є метадані цифрових файлів, які можуть містити інформацію про дату й час створення, характеристики пристрою, параметри зйомки, програмне забезпечення, використане для обробки, а в окремих випадках – географічні координати. Для їх дослідження застосовуються спеціалізовані засоби, зокрема ExifTool. Водночас відсутність метаданих не є самостійною ознакою маніпуляції, оскільки соціальні мережі та месенджери можуть видаляти або змінювати їх під час обробки завантажених файлів.

Практичне встановлення географічної локалізації фото- і відеоматеріалів потребує послідовного зіставлення виявлених візуальних орієнтирів із картографічними матеріалами, супутниковими знімками та панорамними зображеннями місцевості. Інформаційне значення можуть мати конфігурація дорожньої мережі, характер забудови, рельєф, дорожні знаки, назви установ та інші стійкі орієнтири. Надійність результату підвищується за умови підтвердження місця не за однією ознакою, а за сукупністю взаємопов’язаних просторових характеристик.

Під час перевірки відеоматеріалів доцільним є виділення ключових кадрів для їх подальшого зворотного пошуку, візуального аналізу та геолокації. Для виконання таких завдань можуть використовуватися інструменти InVID-WeVerify. Просторова перевірка за потреби доповнюється встановленням часових характеристик матеріалу шляхом аналізу ранніх публікацій, погодних умов, сезонних змін місцевості, положення сонця, напрямку тіней та інших ознак, що можуть бути зіставлені з незалежними джерелами.

Отже, верифікація цифрового контенту має ґрунтуватися на поєднанні декількох методів: зворотного пошуку, аналізу метаданих, дослідження візуальних ознак, геолокації та перевірки часових характеристик. Результати такої роботи потребують належного документування із фіксацією джерел, часу доступу до них і послідовності проведеної перевірки.

Отримання інформації з відкритих джерел, її перевірка та аналітичне опрацювання становлять лише одну складову роботи поліції з цифровими даними. У багатьох випадках результати OSINT-дослідження визначають подальший напрям пошуку, однак установлення фактичних обставин кримінального правопорушення потребує дослідження цифрових даних, що містяться на електронних носіях, у мобільних пристроях, комп’ютерних системах, мережевому середовищі та хмарних сервісах. На цьому етапі ключового значення набувають методи та засоби цифрової криміналістики, застосування яких спрямоване не лише на виявлення інформації, а й на

забезпечення її цілісності, автентичності, відтворюваності результатів дослідження та належного документування всіх операцій із цифровими даними.

Специфіка роботи з цифровими даними визначається їх природою. На відміну від традиційних матеріальних слідів, цифрові дані можуть бути швидко змінені, скопійовані, переміщені або знищені, а частина інформації існує лише протягом обмеженого часу – у оперативній пам'яті пристрою, активних мережевих з'єднаннях, тимчасових файлах, журналах подій або хмарних сесіях. Тому помилки, допущені на початковому етапі роботи з цифровим об'єктом, здатні призвести не лише до втрати окремих відомостей, а й до зміни початкового стану досліджуваного середовища, що ускладнює перевірку походження та цілісності отриманих даних.

Саме тому цифрова криміналістика ґрунтується на контрольованій послідовності дій із цифровими об'єктами. Виявлення потенційних джерел інформації має передувати їх належній фіксації та збереженню; отримання даних – здійснюватися способом, що мінімізує зміну оригінального середовища; дослідження – проводитися на основі перевірюваних методів; кожна суттєва дія – документуватися. Така послідовність забезпечує можливість простежити шлях цифрових даних від моменту їх виявлення до використання результатів дослідження у кримінальному провадженні[58].

Одним із ключових завдань цифрової криміналістики є забезпечення незмінності цифрових даних у процесі їх отримання, збереження та дослідження. На практиці це означає необхідність чіткого розмежування оригінального носія інформації та створеної для дослідження копії, фіксації технічних параметрів цифрового об'єкта, умов його отримання та всіх операцій, що виконувалися під час подальшої роботи. Особливе значення при цьому має застосування криптографічних хеш-функцій, за допомогою яких формується унікальне контрольне значення цифрового об'єкта. Порівняння хеш-значень на різних етапах роботи дозволяє перевірити, чи залишився досліджуваний масив даних незмінним після копіювання, передавання або проведення дослідницьких операцій.

У цифровій криміналістиці принципово важливим є створення криміналістичної копії даних, яка відрізняється від звичайного копіювання файлів. Побітове копіювання передбачає відтворення вмісту носія на рівні секторів і дає змогу досліджувати не лише доступні користувачеві файли, а й видалені об'єкти, залишкові фрагменти інформації, нерозподілений простір, службові структури файлової системи та інші дані, які можуть мати значення для встановлення обставин кримінального правопорушення. Саме тому

[58] ДСТУ EN ISO/IEC 27037:2022. Інформаційні технології. Методи захисту. Настанови щодо ідентифікації, збирання, отримання та збереження цифрових доказів (EN ISO/IEC 27037:2016, IDT; ISO/IEC 27037:2012, IDT). Київ : ДП «УкрНДНЦ», 2022.; Кримінальний процесуальний кодекс України : Кодекс України; Закон, Кодекс від 13.04.2012 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651-17

дослідження, як правило, має проводитися не безпосередньо на оригінальному носії, а на належним чином створеній та перевіреній криміналістичній копії.

Практична складність роботи з цифровими об'єктами полягає також у необхідності правильно визначити пріоритетність отримання даних. Цифрове середовище містить інформацію з різним рівнем стійкості: одні дані зберігаються на постійних носіях протягом тривалого часу, інші можуть бути втрачені після завершення процесу, відключення пристрою від мережі або припинення його живлення. До нестійких даних можуть належати відомості оперативної пам'яті, активні мережеві з'єднання, запущені процеси, відкриті сесії користувача, тимчасові ключі та інші параметри поточного стану системи. Тому рішення щодо способу вилучення цифрової інформації повинно враховувати конкретний стан пристрою, характер події та ризик безповоротної втрати потенційно значущих даних.

Окремий напрям цифрової криміналістики становить дослідження мобільних пристроїв. Сучасний смартфон є не лише засобом зв'язку, а комплексним джерелом цифрової інформації, у якому можуть зберігатися відомості про комунікації, контакти, фотографії та відеозаписи, історію використання застосунків, дані геолокації, відомості про підключення до бездротових мереж, файли, документи та інші цифрові сліди. Особливість мобільної криміналістики полягає в різноманітності операційних систем, моделей пристроїв, механізмів шифрування та способів зберігання інформації, що зумовлює необхідність використання спеціалізованих методів і програмно-апаратних комплексів.

Спосіб отримання даних із мобільного пристрою визначає обсяг і характер інформації, доступної для подальшого дослідження. Залежно від технічних характеристик пристрою, версії операційної системи, стану блокування та застосованих механізмів захисту можуть використовуватися логічне отримання даних, екстракція файлової системи або фізичне отримання вмісту пам'яті. Логічне отримання забезпечує доступ до визначених категорій даних через доступні програмні механізми, тоді як дослідження файлової системи дає змогу працювати з базами даних застосунків, журналами, конфігураційними файлами та іншими системними артефактами. Фізичне отримання, за наявності технічної можливості, передбачає створення копії доступного вмісту пам'яті пристрою для поглибленого криміналістичного аналізу.

Для отримання, оброблення та аналізу даних мобільних пристроїв застосовуються спеціалізовані програмно-апаратні рішення, функціональні можливості яких охоплюють роботу з повідомленнями, журналами викликів, контактами, мультимедійними файлами, базами даних застосунків, відомостями про геолокацію та іншими цифровими артефактами. До поширених засобів цього класу належать Cellebrite UFED, Magnet AXIOM та інші спеціалізовані криміналістичні комплекси. Обсяг фактично доступних даних залежить від моделі пристрою, версії операційної системи, способу отримання інформації та застосованих механізмів захисту.

Аналітична цінність мобільної криміналістики полягає у можливості досліджувати цифрові артефакти у взаємозв'язку. Повідомлення, записи журналів викликів, геолокаційні дані, фотографії, відомості про активність застосунків і мережеві підключення можуть бути зіставлені за часовими та іншими характеристиками. Це дає змогу реконструювати послідовність цифрових подій, перевіряти окремі версії та виявляти зв'язки між даними, які під час ізольованого аналізу могли залишитися непоміченими.

Сучасне розслідування кримінальних правопорушень у цифровому середовищі дедалі рідше ґрунтується на дослідженні одного ізольованого джерела інформації. Практичну цінність становить зіставлення цифрових артефактів, отриманих із пристроїв та інформаційних систем, із відомостями з відкритих джерел. Виявлена в пам'яті мобільного пристрою електронна адреса, цифровий псевдонім, URL-адреса, доменне ім'я, номер телефону або інший ідентифікатор можуть стати вихідною точкою для OSINT-дослідження. У зворотному напрямі результати відкритої розвідки дають змогу визначити об'єкти, зв'язки та цифрові ідентифікатори, які потребують подальшої перевірки методами цифрової криміналістики.

Особливої цінності набуває побудова єдиної хронології цифрових подій. Дані про комунікації, створення та зміну файлів, авторизацію в облікових записах, мережеві з'єднання, геолокаційні відомості, публікації у відкритих джерелах та інші цифрові події можуть мати обмежене значення під час ізольованого дослідження. Їх зіставлення за часовими параметрами дозволяє встановлювати послідовність дій, виявляти часові збіги та суперечності, перевіряти висунуті версії й реконструювати окремі епізоди протиправної діяльності. При цьому необхідно враховувати часові пояси, системні налаштування пристроїв, особливості фіксації часу окремими застосунками та можливі відмінності між локальним і серверним часом.

Важливою тенденцією розвитку цифрової криміналістики є зміщення частини цифрових слідів за межі фізичного пристрою. Сучасні інформаційні екосистеми передбачають синхронізацію даних із хмарними сервісами, використання вебзастосунків, віддалених сховищ і розподіленої інфраструктури. Унаслідок цього відсутність певної інформації на вилученому пристрої не завжди свідчить про її відсутність у цифровому середовищі. Відомості про існування віддалених ресурсів, активність синхронізації, ідентифікатори облікових записів та інші пов'язані артефакти можуть визначати подальші напрями пошуку й отримання цифрових даних у передбаченому законом порядку.

Ефективність поєднання OSINT і цифрової криміналістики значною мірою залежить від якості аналітичної інтерпретації отриманих результатів. Наявність технічного зв'язку між цифровими об'єктами ще не визначає його змісту, так само як виявлення облікового запису, номера телефону або електронної адреси не підтверджує автоматично їх використання конкретною особою в певний момент часу. Тому обґрунтований висновок повинен формуватися на основі сукупності взаємопов'язаних даних, отриманих із

різних незалежних джерел, із чітким розмежуванням установлених фактів, аналітичних висновків та гіпотез, що потребують подальшої перевірки.

Отже, сучасна модель роботи поліції з цифровою інформацією передбачає циклічний характер дослідження: результати OSINT визначають напрями пошуку цифрових даних, цифрові артефакти формують нові вихідні точки для відкритої розвідки, а їх комплексний аналіз забезпечує послідовне уточнення інформаційної моделі досліджуваної події. Саме поєднання пошукових, криміналістичних і аналітичних методів дозволяє перейти від накопичення окремих цифрових відомостей до встановлення їх взаємозв'язків та формування обґрунтованого уявлення про механізм кримінального правопорушення.

За такого підходу ефективність роботи визначається не обсягом зібраної інформації та не кількістю використаних програмних засобів, а здатністю правильно сформулювати інформаційну потребу, визначити послідовність дослідження, критично оцінити отримані результати та встановити їх значення в контексті конкретної події. Окремий цифровий об'єкт набуває інформаційної цінності передусім у системі зв'язків з іншими даними, а сформований на його основі висновок має спиратися на сукупність взаємоузгоджених відомостей. Це зумовлює необхідність поєднання технічної компетентності з аналітичним мисленням, оскільки автоматизоване виявлення збігів, зв'язків і закономірностей саме по собі не забезпечує правильності їх змістовної інтерпретації.

Подальший розвиток цифрових технологій закономірно ускладнюватиме середовище, у якому здійснюється діяльність поліції. Зростання обсягів цифрових даних, їх розподілення між різними пристроями, платформами та інформаційними системами, поширення засобів автоматизованого створення й модифікації контенту та постійна зміна технологічних способів приховування цифрової активності потребують системного оновлення методів роботи з інформацією. За цих умов професійне застосування OSINT та цифрової криміналістики має ґрунтуватися на методологічній послідовності, критичному оцінюванні даних, належному документуванні результатів і постійному вдосконаленні професійних компетентностей працівників поліції. Такий підхід забезпечує перетворення розрізнених цифрових слідів на структуроване знання, необхідне для своєчасного виявлення протиправної діяльності, перевірки висунутих версій та встановлення фактичних обставин кримінального правопорушення.

2.2. Можливості застосування систем штучного інтелекту та аналітичних платформ для предиктивної аналітики та протидії організованим кіберзлочинним угрупованням

Сучасна організована кіберзлочинність функціонує як високотехнологічна індустрія, що характеризується розподілом ролей, транснаціональним характером, використанням моделі «злочин як послуга» та

здатністю швидко адаптуватися до заходів протидії. Згідно з оцінками Європолу, організовані кіберзлочинні угруповання дедалі частіше застосовують автоматизацію, шкідливе програмне забезпечення з елементами машинного навчання та генеративні моделі для масштабування атак, персоналізації фішингових кампаній і приховування слідів злочинної діяльності[59]. Для України ця проблема набуває особливого значення, оскільки в умовах повномасштабної збройної агресії кіберпростір перетворився на арену гібридного протистояння, а кількість зареєстрованих кіберзлочинів лише у 2023 році сягнула 61,4 тис., що вчетверо перевищило показник попереднього року[60]. За таких умов традиційні методи виявлення, документування та розслідування кіберзлочинів, які ґрунтуються переважно на ручному опрацюванні інформації, об'єктивно не здатні забезпечити необхідну оперативність реагування. Обсяги цифрових даних, що підлягають аналізу в межах протидії організованим кіберзлочинним угрупованням (мережевий трафік, журнали подій, фінансові та криптовалютні транзакції, комунікації у месенджерах і даркнеті тощо), вимірюються терабайтами, в той час як швидкість розгортання атак – хвилинами. Саме тому впровадження систем штучного інтелекту (далі – ШІ) та спеціалізованих аналітичних платформ у діяльність підрозділів Національної поліції України слід розглядати не як факультативну інновацію, а як необхідну умову збереження здатності держави ефективно протидіяти організованій кіберзлочинності.

Відповідно до Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р, штучний інтелект визначається як організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань[61].

У контексті протидії організованій кіберзлочинності практичне значення мають такі базові технології ШІ:

- *машинне навчання* (Machine Learning, ML) – алгоритми, що навчаються на основі аналізу даних, постійно вдосконалюючись та адаптуючись до змінного середовища, і використовуються для виявлення аномальних моделей поведінки та прогнозування можливих злочинів;

- *глибинне навчання* (Deep Learning, DL) – метод, що базується на багаторівневих нейронних мережах і дозволяє аналізувати складні

[59] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Luxembourg: Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

[60] Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322.

[61] Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text.

закономірності, розпізнавати обличчя, номерні знаки, аналізувати відеозаписи і т.д.;

- *обробка природної мови* (Natural Language Processing, NLP) – технологія розуміння та аналізу текстових і голосових даних, що застосовується для опрацювання перехоплених комунікацій, повідомлень у соціальних мережах та месенджерах з метою виявлення підозрілої активності;

- *комп'ютерний зір* (Computer Vision) – системи аналізу зображень і відеоматеріалів;

- *графовий (мережевий) аналіз*, що дозволяє моделювати зв'язки між особами, подіями, пристроями та фінансовими потоками[62].

Окрему групу становлять *технології аналізу великих даних* (Big Data), які забезпечують збирання, зберігання та кореляцію різнорідних масивів інформації в режимі, наближеному до реального часу.

Під *аналітичною платформою* у правоохоронній діяльності доцільно розуміти програмно-апаратний комплекс, що інтегрує інструменти збирання, нормалізації, зберігання, аналізу та візуалізації даних з різних джерел і забезпечує підтримку прийняття рішень аналітиком або слідчим. Принципова відмінність платформ нового покоління полягає у вбудованих модулях ШІ, які автоматизують виявлення закономірностей, аномалій та прихованих зв'язків, що недоступні для виявлення людиною в розумні строки. Як зазначається у фахових дослідженнях, системи ШІ здатні аналізувати поведінку користувачів і пристроїв, визначати аномалії у мережевому трафіку, ідентифікувати шкідливе програмне забезпечення та здійснювати автоматичне реагування – блокування загроз без втручання людини, що суттєво скорочує час реакції та має критичне значення для захисту об'єктів критичної інфраструктури[63].

Предиктивна (прогнозна) аналітика являє собою сукупність методів статистичного аналізу, машинного навчання та інтелектуального аналізу даних, спрямованих на прогнозування ймовірності настання певних подій на основі історичних та поточних даних. У поліцейській діяльності виокремлюють кілька *базових моделей прогнозування*:

- просторово-часове прогнозування (визначення місць і часу ймовірного вчинення правопорушень для оптимізації розподілу сил і засобів);

- прогнозування суб'єктів злочинної активності (оцінка ризику вчинення або повторного вчинення правопорушень конкретними особами чи групами);

- прогнозування віктимізації (визначення потенційних жертв або вразливих об'єктів атак)[64].

---

[62] Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. 2025. № 2 (42). С. 638-652.

[63] Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322.; Зоря І.С., Марущак А.В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. Матеріали конференції Вінницького національного технічного університету. Вінниця: ВНТУ, 2024. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf.

[64] Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. 2025. № 2 (42). С. 638-652.; Муравська Ю., Метельський І., Романів Р. Перспективи

При цьому у фаховій літературі наголошується на принциповій відмінності між просторово-орієнтованим та персонально-орієнтованим прогнозуванням. Помилки першого призводять здебільшого до неоптимального розподілу патрульних ресурсів, тоді як персональне прогнозування безпосередньо спрямовує увагу правоохоронних органів на конкретних осіб, які за визначенням є невинуватими у «спрогнозованих» щодо них діяннях, а тому є значно більш чутливим з погляду наслідків для прав людини та етично контроверсійним[65]. Саме ця обставина зумовила закріплення в європейському законодавстві заборони прогнозування злочинної поведінки виключно на основі профілювання особи, про що йтиметься далі.

Стосовно протидії організованій кіберзлочинності предиктивна аналітика набуває специфічного змісту:

- по-перше, це прогнозування кібератак: алгоритми машинного навчання, навчені на даних про попередні інциденти, індикатори компрометації та тактики, техніки і процедури (TTPs) відомих угруповань, дозволяють з високою ймовірністю передбачати вектори, цілі та часові параметри майбутніх атак;

- по-друге, це виявлення аномалій у мережевому трафіку та журналах подій, коли система фіксує відхилення від нормальних типів поведінки користувачів і систем ще до настання шкідливих наслідків – саме здатність ШІ ідентифікувати параметри, які раніше взагалі не враховувалися, дозволяє будувати ефективніші предикативні моделі[66];

- по-третє, це аналіз фінансових потоків, зокрема криптовалютних транзакцій: кластеризація адрес блокчейну, виявлення схем «міксування» та транзитних ланцюгів дає змогу прогнозувати канали легалізації доходів, одержаних злочинним шляхом, та оперативно блокувати їх;

- це також прогнозування розвитку самих злочинних угруповань – появи нових сервісів у даркнеті, ребрендингу ransomware-груп після припинення їхньої діяльності, міграції учасників між угрупованнями.

Досвід зарубіжних правоохоронних органів підтверджує практичну результативність цих підходів:

- Федеральне бюро розслідувань США використовує ШІ для розпізнавання правопорушників на відео з камер спостереження в режимі реального часу та для аналізу великих обсягів даних з метою прогнозування місця і часу наступного злочину;

використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства*. 2024. № 2 (38). С. 90-97.

[65] Lee Y., Bradford B., Posch K. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal*. 2024. Vol. 7, No. 2. P. 127-160. DOI: https://doi.org/10.1080/24751979.2024.2371781.

[66] Зоря І.С., Марущак А.В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. Матеріали конференції Вінницького національного технічного університету. Вінниця: ВНТУ, 2024. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf.

- поліція Великої Британії застосовує ШІ для аналізу соціальних мереж та інших відкритих джерел з метою виявлення загроз національній безпеці;

- у Німеччині аналітичні системи ШІ автоматично опрацьовують великі обсяги фінансової інформації, виявляючи ознаки відмивання грошей, корупції та шахрайства[67];

- у Лос-Анджелесі, Чикаго та Нью-Йорку системи класу PredPol аналізують злочинну активність і допомагають оптимально розподіляти патрульні ресурси;

- німецька система PRECOBS (Pre Crime Observation System) здійснює прогнозування загроз із дотриманням вимог Загального регламенту захисту даних (GDPR);

- за звітами поліцейських департаментів США, застосування предиктивних систем супроводжувалося відчутним зниженням злочинності у цільових зонах: операція LASER у Лос-Анджелесі – на 25 % щодо насильницьких злочинів, програма SARA у Мемфісі – на 20 % щодо майнових злочинів, використання PredPol у м. Кент (штат Вашингтон) – на 20 % щодо крадіжок зі зломом, а цільові втручання у Річмонді – на 40 % щодо збройного насильства протягом двох років[68]. Водночас слід зважати, що ці показники ґрунтуються переважно на самозвітах департаментів і не завжди підтверджені незалежними оцінюваннями;

- поліція Дубая (ОАЕ) впровадила систему «Oyoon», яка засобами ШІ-аналітики відеопотоків міської мережі камер сприяє розкриттю злочинів і виявленню прогалин у безпеці; за офіційними повідомленнями, в окремих районах міста завдяки їй досягнуто ефекту «нульової злочинності»[69].

Водночас зарубіжна практика виявила й системні *ризики предиктивного підходу*. Якщо алгоритми навчаються на історичних даних, що містять соціальні чи етнічні упередження, система автоматично відтворює і підсилює ці викривлення, що перетворює технологічну проблему на етичну та правову[70]. Механізм такого відтворення описується в літературі як «петля зворотного зв'язку»: прогноз системи зумовлює посилене патрулювання певної території чи підвищену увагу до певної групи осіб, що закономірно збільшує кількість зафіксованих там правопорушень і затримань, а нові дані, своєю чергою, «підтверджують» початковий прогноз і додатково зміщують наступні[71]. При

---

[67] Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.

[68] Raji I., Sholademi D. B. Predictive Policing: The Role of AI in Crime Prevention. *International Journal of Computer Applications Technology and Research*. 2024. Vol. 13, Issue 10. P. 66-78. DOI: https://doi.org/10.7753/IJCATR1310.1006.

[69] Al Shamsi H. R. S., Safei S. Artificial Intelligence Adoption in Predictive Policing to Predict Crime Mitigation Performance. *International Journal of Sustainable Construction Engineering and Technology*. 2023. Vol. 14, No. 3. P. 289–298. DOI: https://doi.org/10.30880/ijscet.2023.14.03.025.

[70] Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. 2025. № 2 (42). С. 638-652.

[71] Raji I., Sholademi D. B. Predictive Policing: The Role of AI in Crime Prevention. *International Journal of Computer Applications Technology and Research*. 2024. Vol. 13, Issue 10. P. 66–78. DOI:

цьому каузальний аналіз найвідоміших американських кейсів (Чикаго, Лос-Анджелес) засвідчив, що першоджерелом дискримінаційних результатів є не стільки самі алгоритми, скільки поліцейська практика, відображена у вхідних даних, – рішення про дислокацію сил та фіксацію затримань. Відтак навіть повна відмова від алгоритму не усуває упередженості, а аудиту має підлягати вся практика застосування системи, а не лише її програмний код[72].

Критичного значення набуває й оцінка доказової бази ефективності. Систематичний огляд 161 дослідження предиктивного поліціювання на основі великих даних (2007–2022 рр.) показав, що лише шість із них (3,7 %) передбачали перевірку алгоритмів у реальних польових умовах і лише три – тестування ефекту просторового витіснення злочинності. Решта (96 %) є ретроспективними перевірками точності моделей на історичних даних, результати яких додатково зазнають публікаційного зміщення. Автори огляду констатують, що наявних доказів поки недостатньо для твердження, що предиктивне поліціювання гарантовано знижує злочинність, а зафіксована ефективність обмежується конкретними комбінаціями виду злочину та поліцейського втручання[73]. Ця обставина має принципове значення для визначення допустимих меж застосування предиктивної аналітики, про що йтиметься далі.

Практичний інструментарій інформаційно-аналітичного забезпечення протидії організованій кіберзлочинності доцільно згрупувати за функціональним призначенням.

Платформи кримінального аналізу та візуалізації зв'язків забезпечують побудову й дослідження моделей «особа – подія – об'єкт – рахунок – пристрій». Класичним рішенням цього класу є IBM i2 Analyst's Notebook, що дозволяє аналітику інтегрувати дані з різних джерел, будувати схеми зв'язків, хронологічні шкали та виявляти посередників у злочинних мережах. Платформа Palantir (зокрема специфікація Palantir Gotham) спрямована на візуалізацію великих масивів інформації, встановлення причинно-наслідкових зв'язків при розслідуванні злочинів та прогнозування злочинної поведінки. Вона використовується, серед іншого, для боротьби з шахрайством і тероризмом у структурах Розвідувального співтовариства США. Поряд із нею у практиці американських правоохоронних органів застосовувалися й інші рішення для оцінки ймовірності вчинення злочинів та аналізу діяльності організованих груп – HunchLab, ShotSpotter, а також персонально-орієнтована система Strategic Subject List (SSL), розроблена Іллінойським технологічним інститутом для поліції Чикаго за грантом Міністерства юстиції США[74]. Слід

---

https://doi.org/10.7753/IJCATR1310.1006.; Hung T.-W., Yen C.-P. Predictive Policing and Algorithmic Fairness. *Synthese*. 2023. Vol. 201, No. 6. Article 206. 29 p. DOI: https://doi.org/10.1007/s11229-023-04189-0.

[72] Там само.

[73] Lee Y., Bradford B., Posch K. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal.* 2024. Vol. 7, No. 2. P. 127–160. DOI: https://doi.org/10.1080/24751979.2024.2371781.

[74] Вікторчук М.В., Багатко А.С. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 86, ч. 3. С. 257-263.; Hung T.-W., Yen C.-P. Predictive Policing and

підкреслити, що досвід практичної експлуатації таких систем засвідчив як періоди суттєвого зниження рівня насильницької злочинності, так і подальше зниження ефективності, що вкотре підтверджує допоміжний, а не самодостатній характер подібних інструментів[75].

Досвід SSL заслуговує на окрему увагу як наочна ілюстрація меж персонально-орієнтованого прогнозування. Система охоплювала базу з майже 400 тис. осіб, яким на підставі даних про затримання (а не обвинувальні вироки) присвоювався бал ризику причетності до збройного насильства за шкалою від 0 до 500. Незалежне емпіричне дослідження засвідчило, що бал ризику статистично прогнозував расову належність затриманої особи навіть за контролю просторових і соціально-економічних характеристик району[76]. Оцінювання програми не виявило її впливу на рівень збройної злочинності, натомість особи з переліку мали підвищену ймовірність затримання, і в листопаді 2019 року програму було офіційно припинено[77]. Аналогічні проблеми виявив аудит персонально-орієнтованої програми Chronic Offender Program поліції Лос-Анджелеса: 44 % осіб, включених до переліку «хронічних правопорушників», мали нуль або лише одне затримання за насильницькі злочини[78].

Платформи аналізу блокчейну та криптовалютних транзакцій (Chainalysis, Elliptic, TRM Labs та аналогічні) застосовують алгоритми машинного навчання для кластеризації криптовалютних адрес, атрибуції гаманців конкретним сервісам чи угрупованням, відстеження ланцюгів транзакцій через міксери та мости між блокчейнами. Для протидії організованим кіберзлочинним угрупованням, що використовують криптовалюти як основний засіб одержання викупів (ransomware) та розрахунків у даркнеті, такі рішення фактично не мають альтернативи, оскільки ручний аналіз публічних реєстрів транзакцій неможливий через їхній обсяг.

Системи класу SIEM/SOAR (Security Information and Event Management / Security Orchestration, Automation and Response) забезпечують централізований збір, аналіз та кореляцію подій безпеки в реальному часі. Показовим є досвід використання платформи Splunk Enterprise Security для моніторингу кіберінцидентів: система застосовує штучний інтелект та машинне навчання для виявлення загроз, автоматизації реагування та управління ризиками, інтегруючись із різними джерелами даних – мережевим трафіком, журналами подій, результатами поведінкового аналізу, що дозволяє

Algorithmic Fairness. *Synthese*. 2023. Vol. 201, No. 6. Article 206. 29 p. DOI: https://doi.org/10.1007/s11229-023-04189-0.

[75] Там само.

[76] DaViera A. L., Uriostegui M., Gottlieb A., Onyeka O. C. Risk, Race, and Predictive Policing: A Critical Race Theory Analysis of the Strategic Subject List. *American Journal of Community Psychology*. 2024. Vol. 73, No. 1–2. P. 91–103. DOI: https://doi.org/10.1002/ajcp.12671.

[77] Там само.; Hung T.-W., Yen C.-P. Predictive Policing and Algorithmic Fairness. *Synthese*. 2023. Vol. 201, No. 6. Article 206. 29 p. DOI: https://doi.org/10.1007/s11229-023-04189-0.

[78] Там само.

швидко ідентифікувати аномалії, пов'язані з кібератаками, та передавати їх відповідним командам реагування[79].

Інструменти OSINT з модулями ШІ (зокрема Maltego у поєднанні з інтелектуальними трансформаціями, системи моніторингу соціальних мереж і даркнету) детально розглянуто у підрозділі 2.1 цих рекомендацій. У контексті цього підрозділу наголосимо лише, що саме інтеграція ШІ-аналітики з розвідкою на основі відкритих джерел забезпечує синергетичний ефект: ШІ здатен опрацьовувати великі обсяги неструктурованих відкритих даних, виявляти ключові слова, теми та поведінкові закономірності, що вказують на потенційні загрози, істотно зменшуючи витрати часу аналітиків[80].

Платформи міжнародного рівня, розгорнуті Європолом, включають, зокрема:

- платформу SIRIUS, для обміну знаннями та інструментами доступу до електронних доказів, що зберігаються онлайн-сервісами;
- Europol Malware Analysis Solution, для автоматизованого аналізу зразків шкідливого програмного забезпечення, наданих державами-членами та партнерами;
- аналітичні проєкти Європейського центру боротьби з кіберзлочинністю (EC3), у межах яких здійснюється кореляція даних національних розслідувань щодо транснаціональних угруповань[81].

Доступ українських правоохоронців до цих ресурсів у межах угод про співробітництво з Європолом суттєво розширює аналітичні можливості національних підрозділів.

Окремо слід відзначити можливості великих мовних моделей як засобу аналітичної підтримки розслідувань для автоматизованого реферування великих обсягів документів, попереднього аналізу перехоплених комунікацій, перекладу багатомовних матеріалів, підготовки проєктів аналітичних довідок, узагальнення судової практики. Дослідники слушно відносять до переваг таких систем автоматизацію рутинних завдань, ефективний пошук інформації та підтримку прийняття рішень, водночас наголошуючи, що прогнози й висновки ШІ мають використовуватися лише як один із факторів під час ухвалення рішення, а не як його єдина підстава[82]. Не можна ігнорувати і «дзеркальний» аспект проблеми, оскільки ті самі генеративні моделі активно використовуються злочинцями для створення переконливих фішингових текстів, шкідливого коду шляхом розбиття завдання на нейтральні на вигляд

---

[79] Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322.

[80] Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.

[81] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Luxembourg: Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

[82] Муравська Ю., Метельський І., Романів Р. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства*. 2024. № 2 (38). С. 90-97.

частини та реалістичних deepfake-матеріалів[83], що додатково актуалізує потребу правоохоронних органів у власних інструментах ШІ, здатних виявляти згенерований контент.

Ключова особливість організованої кіберзлочинності – мережева, часто транснаціональна структура угруповань, учасники яких можуть не знати один одного особисто, взаємодіяти виключно через захищені канали зв'язку та виконувати вузькоспеціалізовані ролі: розробники шкідливого програмного забезпечення, оператори доступу, «дропи», фахівці з легалізації коштів, адміністратори інфраструктури і т.д. Саме тому центральним аналітичним завданням є не стільки фіксація окремих епізодів, скільки декомпозиція структури угруповання – встановлення його ієрархії, ролей учасників, каналів комунікації та фінансування.

Технології графового аналізу соціальних мереж у поєднанні з машинним навчанням дозволяють:

- будувати соціальні графи угруповання на основі даних про комунікації, транзакції, спільне використання інфраструктури (серверів, доменів, гаманців);
- обчислювати метрики центральності, що вказують на організаторів, координаторів та критичні вузли мережі, нейтралізація яких завдає угрупованню максимальної шкоди;
- виявляти приховані спільноти та посередників між різними злочинними осередками.

Алгоритми зв'язування злочинів забезпечують автоматизоване виявлення серійності – встановлення належності територіально та часово розпорошених епізодів одному угрупованню на основі збігів у тактиках, інструментах, інфраструктурі та цифрових слідах. Технології атрибуції атак, що ґрунтуються на аналізі коду шкідливого програмного забезпечення, мовних особливостей, часових закономірностей активності та повторного використання інфраструктури, дозволяють з певним ступенем імовірності пов'язувати атаки з відомими угрупованнями.

Ефективність цих підходів підтверджується вітчизняною методичною практикою[84]. Використання ШІ дозволяє правоохоронним органам відстежувати злочинців та злочинні групи, визначати їх місцезнаходження, аналізувати відео- та аудіозаписи, шукати співвідношення між різними злочинами та правопорушниками, виявляючи зв'язки між фактами, що можуть

[83] Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322.; Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.

[84] Pashniev D.V., Shmatkov D.I., Kolomiitsev S.O., Manzhai O.V., Nosov V.V., Luchyk V.Ye., Serdiuk O.O. AI and OSINT tools and methods for tracing missing, deported or forcibly displaced children: Guidelines for the use of open source intelligence and new technologies, including facial recognition. Kharkiv: Ministry of Internal Affairs of Ukraine; Kharkiv National University of Internal Affairs, 2024. 80 p.

мати ключове значення для розслідування[85]. Водночас результати такого аналізу є орієнтуючою інформацією: питання їх процесуального закріплення та трансформації у докази розглядаються у підрозділі 2.3 цих рекомендацій.

Аналіз зарубіжної практики дозволяє виокремити кілька моделей інституціоналізації ШІ-аналітики у протидії організованій кіберзлочинності. Європол координує масштабні операції з ліквідації інфраструктури організованих кіберзлочинних угруповань: ботнетів, ransomware-сервісів, платформ даркнету тощо, у межах яких аналітичні підрозділи EC3 забезпечують кореляцію даних десятків національних розслідувань, автоматизований аналіз вилучених серверів та ідентифікацію учасників угруповань. За результатами таких операцій нейтралізовано низку потужних хакерських об'єднань, злочинна діяльність яких охоплювала країни всього світу, причому українська кіберполіція у 2024 році ініціювала та забезпечила участь у 17 міжнародних поліцейських операціях[86].

Інтерпол використовує аналітичні системи для відстеження організованих злочинних груп у міжнародному масштабі та розвиває глобальні платформи обміну даними про кіберзагрози[87].

У США, окрім згаданих систем предиктивного поліціювання, функціонує Центр скарг на інтернет-злочини ФБР (IC3), що виконує роль агрегатора даних про кіберінциденти, на основі яких формуються аналітичні моделі загроз[88].

Досвід окремих держав демонструє і межі допустимого: китайська система «Zero Trust», що впродовж 2012-2018 років допомогла викрити або запобігти протиправним діям майже 9 тисяч державних службовців, була критикована через непрозорість алгоритмів виявлення, а масштабні системи соціального рейтингу та тотального відеоспостереження є прикладом трансформації технологій безпеки у засіб контролю над суспільством, несумісний із демократичними стандартами[89]. Натомість литовський досвід застосування ШІ для виявлення дезінформації, коли система щоденно відстежує понад 10 000 матеріалів із сотень інтернет-доменів, а верифікацію підозрілих матеріалів здійснюють фахівці, ілюструє збалансовану модель «ШІ виявляє – людина перевіряє»[90].

---

[85] Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2023. № 3. С. 148-156.; Шевчук Т.А., Свистун Я.В. Використання штучного інтелекту у протидії злочинності. *Вісник кримінологічної асоціації України*. 2021. № 2 (25). С. 128-134.

[86] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Luxembourg: Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.; Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка.* 2025. № 3 (31). С. 309-322.

[87] Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. 2025. № 2 (42). С. 638–652.

[88] Там само.

[89] Там само. Вікторчук М.В., Багатко А.С. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 86, ч. 3. С. 257-263.

[90] Там само.

Для Національної поліції України імплементація міжнародного досвіду має відбуватися за такими напрямами:

- розширення участі в аналітичних проєктах Європолу та операціях з одночасною синхронізацією форматів даних;
- запозичення методології оцінювання загроз на кшталт щорічних звітів IOCTA для формування національної картини організованої кіберзлочинності[91];
- впровадження перевірених часом платформ кримінального аналізу з обов'язковою локалізацією та сертифікацією;
- врахування європейських правових запобіжників при проєктуванні власних систем.

Вітчизняна практика вже містить приклади результативного застосування інтелектуальних технологій. Національна поліція України використовує:

- системи розпізнавання обличчя, що допомагають виявляти правопорушників, попереджувати терористичні акти та встановлювати осіб, які перебувають у розшуку;
- функціонує система автоматичного розпізнавання номерних знаків транспортних засобів, задіяних у правопорушеннях[92].

В умовах збройної агресії російської федерації технологія розпізнавання облич Clearview AI, база даних якої налічує понад 20 мільярдів зображень, була надана Україні та застосовується, зокрема, для ідентифікації воєнних злочинців, загиблих і зниклих безвісти, причому Національна поліція України приєдналася до цього проєкту серед інших відомств[93].

Використовуються й вітчизняні розробки: система «Касандра» Міністерства юстиції України з елементами ШІ для аналізу ймовірності повторного порушення закону, спеціалізоване відомче інтелектуальне програмне забезпечення, комплекси «Безпечне місто» з алгоритмами аналізу відеоданих[94].

Департамент кіберполіції Національної поліції України демонструє зростаючу результативність: за 2023–2024 роки зареєстровано тисячі кіберзлочинів, повідомлено про підозру 1,7 тис. особам, потерпілим забезпечено відшкодування понад 168,6 млн грн, що становить 42,5 % від завданих збитків. Завдяки співпраці з Національним банком України та Держспецзв'язку обмежено доступ до доменних імен, які масово

---

[91] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Luxembourg: Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

[92] Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.

[93] Там само.

[94] Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. 2025. № 2 (42). С. 638-652.; Вікторчук М.В., Багатко А.С. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 86, ч. 3. С. 257-263.

використовувалися для фішингу; припинено діяльність організованих груп, що через шахрайські call-центри ошукали сотні громадян[95]. Водночас впровадження ШІ-рішень у діяльність кіберполіції стримується низкою системних проблем:

- критичною нестачею кваліфікованих фахівців, які поєднують компетентності у сферах інформаційної безпеки, аналізу даних та кримінального процесу, на тлі конкуренції з приватним сектором за ІТ-кадри;
- технічною застарілістю обладнання та програмного забезпечення, що не відповідає рівню сучасних кіберзагроз;
- відсутністю уніфікованих методик і стандартів застосування аналітичних інструментів;
- обмеженістю фінансових ресурсів на придбання ліцензій та розбудову інфраструктури обробки великих даних[96].

Розв'язання цих проблем потребує комплексного підходу через розроблення єдиної цифрової стратегії відомства, цільового фінансування, створення системи безперервної підготовки поліцейських аналітиків на базі закладів вищої освіти системи МВС, а також розвитку державно-приватного партнерства з вітчизняними технологічними компаніями.

Застосування систем ШІ правоохоронними органами перебуває у сфері підвищеного правового ризику, оскільки безпосередньо стосується прав людини – на приватність, захист персональних даних, справедливий суд, презумпцію невинуватості. Базовим міжнародним орієнтиром є Регламент (ЄС) 2024/1689 про штучний інтелект – AI Act, схвалений Європейським парламентом 13 березня 2024 року, який запроваджує ризик-орієнтований підхід до регулювання систем ШІ[97]. Для правоохоронної сфери принципове значення мають такі його положення:

- заборона систем біометричної категоризації за чутливими ознаками та нецільового збирання зображень облич з Інтернету чи камер відеоспостереження для створення баз розпізнавання;
- заборона дистанційної біометричної ідентифікації «в реальному часі» у загальнодоступних місцях, за винятком вичерпно визначених ситуацій (таких, як пошук жертв злочинів і зниклих дітей, відвернення загрози життю чи терористичного акту, переслідування за тяжкі злочини тощо) та лише за попереднім дозволом судового чи незалежного органу;
- заборона систем прогнозування вчинення правопорушень конкретними особами виключно на основі профілювання їхніх рис і

[95] Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322.

[96] Там само.; Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. 2025. № 2 (42). С. 638-652.

[97] Чигрина Г.Л. Допустимість використання штучного інтелекту у правоохоронній діяльності. Актуальні проблеми інноваційної економіки та права. 2024. № 2. С. 6-10.; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series, 12.7.2024.

характеристик, оскільки такі системи порушують людську гідність і презумпцію невинуватості[98].

Показово, що низка вимог чинного законодавства України вже кореспондує цим стандартам. Так, Кримінальний процесуальний кодекс України допускає проведення обшуків лише з дозволу слідчого судді, а частина 1 статті 88 КПК України визнає недопустимими докази щодо судимостей чи рис характеру особи на підтвердження її винуватості[99].

Регуляторні підходи інших юрисдикцій є менш централізованими, проте демонструють спільні тенденції. У США регулювання фрагментоване на рівні штатів (зокрема, каліфорнійський закон про захист прав споживачів CCPA вимагає прозорості збирання та використання даних), а Міністерство юстиції рекомендувало правоохоронним агенціям оцінювати потенціал упередженості й дискримінації алгоритмічних інструментів. У Великій Британії застосування таких систем підпорядковане Закону про захист даних 2018 року, настановам Управління комісара з інформації (ICO) щодо справедливості, підзвітності та прозорості ШІ, а також рекомендаціям Національної ради шефів поліції щодо етичних практик і залучення громад[100]. Спільним знаменником є принцип пропорційності: високоризикові технології спостереження можуть впроваджуватися лише за доведеної користі, яка переважає обумовлене ними втручання у права людини, – тим більше, що повноваження і технічні спроможності, одного разу надані поліції, надзвичайно важко відкликати[101].

Національну правову основу застосування інтелектуальних технологій у сфері протидії кіберзлочинності становлять:

- ратифікована Україною Конвенція про кіберзлочинність[102];
- Закон України «Про основні засади забезпечення кібербезпеки України»[103];
- Стратегія кібербезпеки України[104];
- Концепція розвитку штучного інтелекту в Україні[105];

---

[98] Там само.

[99] Чигрина Г.Л. Допустимість використання штучного інтелекту у правоохоронній діяльності. *Актуальні проблеми інноваційної економіки та права*. 2024. № 2. С. 6-10.; Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[100] Raji I., Sholademi D. B. Predictive Policing: The Role of AI in Crime Prevention. *International Journal of Computer Applications Technology and Research.* 2024. Vol. 13, Issue 10. P. 66–78. DOI: https://doi.org/10.7753/IJCATR1310.1006.

[101] Lee Y., Bradford B., Posch K. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal*. 2024. Vol. 7, No. 2. P. 127-160. DOI: https://doi.org/10.1080/24751979.2024.2371781.

[102] Конвенція про кіберзлочинність від 23.11.2001, ратифікована Законом України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575.

[103] 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.

[104] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

[105] Там само.

- закони України «Про Національну поліцію»[106] та «Про оперативно-розшукову діяльність»[107].

Водночас у науковій літературі обґрунтовано констатується відсутність спеціального нормативного регулювання застосування ШІ у правоохоронній діяльності та пропонується, зокрема, доповнити статтю 25 Закону України «Про Національну поліцію» положенням про право поліції застосовувати засоби ШІ для збору, обробки та аналізу інформації, а статтю 8 Закону України «Про оперативно-розшукову діяльність» – правом застосовувати засоби ШІ для отримання, обробки, перевірки та аналізу оперативної інформації[108]. Такі пропозиції заслуговують на підтримку за умови одночасного закріплення гарантій: вичерпного переліку цілей обробки, строків зберігання даних, механізмів аудиту алгоритмів та судового контролю.

Етичний вимір проблеми концентрується навколо кількох ризиків:

- алгоритмічної упередженості, оскільки ШІ не володіє моральними чи етичними переконаннями, а обробляє історичні дані, які можуть містити упередження, некритичне використання його висновків здатне відтворювати та посилювати дискримінацію[109];

- проблеми «чорної скриньки», оскільки більшість глибоких нейронних мереж не забезпечують пояснюваності рішень, через що ані слідчий, ані суд не можуть встановити, чому алгоритм визначив конкретну особу як причетну до угруповання; відсутність механізмів верифікації таких висновків може призвести до серйозних юридичних наслідків[110];

- конфіденційність – автоматизований аналіз трафіку чи відеоспостереження без належних правових підстав створює ризики масового стеження та зловживань[111].

Слід ураховувати також, що проблема алгоритмічної справедливості не має суто технічного розв'язання. У літературі математично доведено, що різні формальні критерії справедливості алгоритму (рівність часток хибнопозитивних результатів, рівність прогностичної цінності тощо) за відмінних базових показників для різних соціальних груп не можуть бути задоволені одночасно. Відтак вибір конкретного критерію справедливості є

---

[106] Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

[107] Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

[108] Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.

[109] Моргунова Т.І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології.* 2025. № 2 (42). С. 638-652.; Муравська Ю., Метельський І., Романів Р. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства.* 2024. № 2 (38). С. 90-97.

[110] Там само.

[111] Макаліш Б.Д., Мойко О.О., Лучик В.Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322.

нормативним рішенням, яке має ухвалюватися прозоро та бути предметом зовнішнього контролю, а не «зашиватися» розробником у програмний код[112].

Із цих ризиків випливає ключовий принцип, сформульований у вітчизняній доктрині: системи ШІ допомагають приймати рішення працівникам правоохоронних органів, а не приймають рішення замість них. Висновки (рішення) ШІ доцільно використовувати як привід для проведення додаткової перевірки, але не як підставу для прийняття визначального рішення правоохоронним чи правозастосовним органом[113]. Обов'язковість людського контролю над кожним юридично значущим рішенням, ухваленим за участю ШІ, має бути закріплена на рівні відомчих інструкцій. Питання допустимості результатів ШІ-аналітики як доказів у кримінальному провадженні, включно з вимогами до фіксації процесу їх одержання, докладно висвітлено у підрозділі 2.3 цих рекомендацій.

Узагальнення викладеного дозволяє запропонувати підрозділам, залученим до протидії організованій кіберзлочинності, такий алгоритм інтеграції ШІ-інструментів у службову діяльність

1) інвентаризацію та постановку завдань через визначення типових аналітичних завдань підрозділу (виявлення аномалій, аналіз зв'язків, відстеження транзакцій, атрибуцію атак), обсягів і джерел даних, що підлягають обробці, та вимірюваних показників очікуваного ефекту;

2) правовий аудит – перевірку наявності правових підстав для кожного виду обробки даних, визначення категорій персональних даних, строків зберігання, порядку доступу; недопущення використання інструментів, що підпадають під заборонені практики за стандартами AI Act;

3) вибір та верифікацію інструментів:

- надання переваги рішенням з пояснюваними алгоритмами і можливістю аудиту;
- тестування на історичних даних завершених проваджень з оцінкою частки хибнопозитивних і хибнонегативних результатів;
- у разі пілотування предиктивних моделей – дотримання вимог доказового тестування: наявність контрольних і експериментальних груп, чітко специфіковане поліцейське втручання, конкретизація видів злочинів, перевірка ефектів просторового витіснення злочинності та тестування моделі на диспропорційність результатів щодо окремих соціальних груп[114];
- сертифікацію та перевірку захищеності самих систем, оскільки вони можуть ставати мішенню атак і об'єктом маніпуляцій із вхідними даними[115];

---

[112] Hung T.-W., Yen C.-P. Predictive Policing and Algorithmic Fairness. *Synthese.* 2023. Vol. 201, No. 6. Article 206. 29 p. DOI: https://doi.org/10.1007/s11229-023-04189-0.

[113] Чигрина Г.Л. Допустимість використання штучного інтелекту у правоохоронній діяльності. *Актуальні проблеми інноваційної економіки та права*. 2024. № 2. С. 6-10.

[114] Lee Y., Bradford B., Posch K. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal*. 2024. Vol. 7, No. 2. P. 127–160. DOI: https://doi.org/10.1080/24751979.2024.2371781.

[115] Зоря І.С., Марущак А.В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. Матеріали конференції Вінницького національного технічного університету. Вінниця: ВНТУ, 2024. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf.

4) інтеграцію у процеси:

- через закріплення у відомчих методиках правила «ШІ виявляє – аналітик перевіряє – керівник санкціонує»;

- документування кожного етапу застосування системи (версія моделі, вхідні дані, параметри запиту, отриманий результат) для забезпечення подальшої перевірюваності;

- узгодження результатів ШІ-аналітики з матеріалами, одержаними засобами OSINT (підрозділ 2.1), та їх подальше процесуальне закріплення (підрозділ 2.3);

5) кадрове забезпечення – запровадження безперервного навчання працівників, при цьому навчальні центри мають оновити свої освітні програми, щоб забезпечити правоохоронцям навички використання інструментів штучного інтелекту[116]; емпіричним підтвердженням пріоритетності цього напряму є дослідження за даними опитування 316 працівників поліції Абу-Дабі: у регресійній моделі результативності протидії злочинності найбільшу вагу мало саме колаборативне навчання персоналу (β=0,510), тоді як власне факт впровадження предиктивних технологій – майже втричі меншу (β=0,194), що свідчить про неможливість досягти ефекту від технологій без системної підготовки кадрів[117];

6) контроль та вдосконалення:

- періодичний незалежний аудит алгоритмів на предмет упередженості;

- моніторинг ефективності за визначеними показниками;

- налагодження зворотного зв’язку з прокуратурою та судами щодо оцінки результатів ШІ-аналітики у провадженнях;

- участь у міжнародному обміні даними про загрози.

Отже, системи штучного інтелекту та аналітичні платформи є стратегічним ресурсом протидії організованій кіберзлочинності, який дозволяє перейти від реактивної моделі розслідування окремих епізодів до проактивної моделі виявлення, прогнозування та системної нейтралізації злочинних угруповань. Предиктивна аналітика, графовий аналіз злочинних мереж, автоматизоване відстеження криптовалютних потоків та кореляція даних про кіберінциденти в межах міжнародних платформ уже довели свою результативність у практиці Європолу, провідних держав та, дедалі більшою мірою, Національної поліції України. Водночас ефективність і легітимність застосування цих технологій визначаються не лише їхніми технічними можливостями, а й якістю правових та організаційних запобіжників. Висновки систем ШІ мають статус орієнтуючої інформації, що потребує обов’язкової

[116] Муравська Ю., Метельський І., Романів Р. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства*. 2024. № 2 (38). С. 90-97.; Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.

[117] Al Shamsi H. R. S., Safei S. Artificial Intelligence Adoption in Predictive Policing to Predict Crime Mitigation Performance. *International Journal of Sustainable Construction Engineering and Technology*. 2023. Vol. 14, No. 3. P. 289-298. DOI: https://doi.org/10.30880/ijscet.2023.14.03.025.

перевірки людиною, а їх використання повинно відповідати принципам законності, пропорційності, пояснюваності та людського контролю, закріпленим у європейських стандартах регулювання ШІ. Додатковим аргументом на користь такого підходу є сучасний стан доказової бази: емпірично підтверджена ефективність предиктивних систем залишається обмеженою та контекстно-залежною[118], а отже, їх впровадження має супроводжуватися власним доказовим оцінюванням, а не ґрунтуватися на презумпції результативності.

Пріоритетними завданнями на найближчу перспективу є:

- формування спеціальної нормативної основи застосування ШІ у діяльності поліції;
- модернізація технічної бази кіберпідрозділів;
- створення системи підготовки поліцейських аналітиків;
- інституціоналізація незалежного аудиту алгоритмів.

Лише за умови збалансованого поєднання технологічної спроможності та гарантій прав людини штучний інтелект стане дієвим і безпечним інструментом протидії організованим кіберзлочинним угрупованням.

2.3. Алгоритми виявлення, збору, аналізу та процесуального закріплення цифрових слідів (доказів)

Розглянуті у попередніх підрозділах інструменти розвідки на основі відкритих джерел (підрозділ 2.1) та системи штучного інтелекту й аналітичні платформи (підрозділ 2.2) забезпечують виявлення ознак діяльності організованих кіберзлочинних угруповань і формування орієнтуючої інформації. Проте юридична доля кримінального провадження вирішується не обсягом накопичених аналітичних даних, а якістю доказів, які сторона обвинувачення здатна подати суду. Специфіка кіберзлочинів полягає в тому, що практично вся доказова база має цифрову форму, є вразливою до знищення, модифікації та фальсифікації, а помилка, допущена на етапі збирання, як правило, не може бути виправлена в подальшому. Саме тому центральне місце в методиці розслідування посідають алгоритми – стандартизовані послідовності дій, що гарантують одночасно технічну коректність поводження з цифровими слідами та їхню процесуальну допустимість.

У криміналістичній доктрині *електронні (цифрові) сліди* кримінального правопорушення визначаються як комп’ютерні дані, що утворилися або зазнали змін у запам’ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов’язаних із вчиненням кримінального

[118] Lee Y., Bradford B., Posch K. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal*. 2024. Vol. 7, No. 2. P. 127–160. DOI: https://doi.org/10.1080/24751979.2024.2371781.

правопорушення[119]. Ці сліди містять інформацію про стан та результати роботи певної комп'ютерної системи, не можуть бути безпосередньо сприйняті органами відчуття людини та завжди потребують інтерпретації з використанням технічних засобів. Внаслідок стрімкої цифровізації електронні сліди стали єдиним можливим відображенням інформації про обставини правопорушення в електронному середовищі. При цьому електронний слід є поняттям ширшим відносно електронного доказу: електронні дані не є процесуальним джерелом доказів, доки не будуть верифіковані та отримані у порядку, визначеному кримінальним процесуальним законодавством. Електронний доказ, своєю чергою, є результатом процесуальної трансформації електронного сліду за умови дотримання вимог автентичності, цілісності та допустимості. Попри те, що чинний КПК України не виокремлює електронні докази як самостійне процесуальне джерело, актуальною залишається потреба закріплення дефініцій «електронних даних» та «електронного доказу» для забезпечення єдності правозастосовної практики, оскільки електронні сліди, як і комп'ютерні дані загалом, не мають жорсткої прив'язки до фізичного носія і можуть бути скопійовані без зміни їх змісту.

За місцем локалізації доцільно розрізняти такі групи цифрових слідів:

- *локальні* – містяться на кінцевих пристроях (комп'ютери, смартфони, зовнішні накопичувачі, IoT-пристрої тощо): файли та їх фрагменти, артефакти операційних систем і застосунків, журнали подій, історія браузерів, збережені сеанси месенджерів;

- *мережеві* – журнали (логи) серверів і мережевого обладнання, записи про з'єднання та трафік в операторів електронних комунікацій, дані сесій VPN, DNS-запити, метадані маршрутизації електронної пошти;

- *хмарні* – дані у хмарних сховищах, SaaS-сервісах, месенджерах та соціальних мережах, що фізично розміщені на серверах постачальників послуг, здебільшого за межами юрисдикції України;

- *сліди у публічних розподілених реєстрах* – записи блокчейнів про криптовалютні транзакції, які є загальнодоступними та незмінюваними, однак потребують атрибуції адрес конкретним особам чи сервісам.

За стійкістю розрізняють:

- *волатильні (енергозалежні) дані* – вміст оперативної пам'яті, активні мережеві з'єднання, запущені процеси, ключі шифрування у пам'яті, що безповоротно втрачаються після вимкнення живлення;

- *неволатильні дані*, які зберігаються на носіях тривалий час.

Самостійну доказову цінність мають *метадані* – відомості про час створення й модифікації файлів, геолокаційні позначки, ідентифікатори

[119] Коваленко А.В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка*. 2022. № 4. С. 226-236; Коваленко А.В. Електронні докази у кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2018. № 4. С. 237-245; Грищук В.Р. Електронні (цифрові) дані у кримінальному провадженні: від електронного сліду до доказу. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2026. Випуск 93, частина 5. С. 68-73.

пристроїв, службові заголовки повідомлень, які нерідко дозволяють установити обставини, що їх неможливо довести змістом самого файлу. Послідовність збирання має відповідати порядку волатильності, закріпленому, зокрема, у настанові IETF RFC 3227: першими фіксуються найменш стійкі дані.

Слідова картина діяльності організованих кіберзлочинних угруповань має особливості, які безпосередньо впливають на побудову алгоритмів: розподілена інфраструктура (орендовані сервери та віртуальні машини у різних юрисдикціях, bulletproof-хостинг), багаторівнева анонімізація (VPN, Tor, ланцюги проксі-серверів), наскрізне шифрування комунікацій, розрахунки у криптовалютах із використанням міксерів, автоматизоване знищення слідів[120]. Із цього випливають три практичні наслідки:

1) сліди навіть одного епізоду розпорошені між багатьма володільцями інформації у різних країнах;

2) вирішальне значення має чинник часу, оскільки дані про з'єднання зберігаються постачальниками послуг обмежений строк;

3) вилучення окремого пристрою рідко дає повну картину, тому збирання доказів планується як серія скоординованих дій щодо всіх вузлів інфраструктури угруповання.

Незалежно від виду слідів робота з цифровими доказами підпорядковується принципам, виробленим міжнародною практикою та стандартизованим у серії ISO/IEC 27037, 27041, 27042, 27043[121], настановах Інтерполу для лабораторій цифрової криміналістики[122] та посібнику ENISA для першого реагування[123]:

- *законність* – кожна дія має ґрунтуватися на нормі КПК та, за необхідності, на судовому рішенні;
- *цілісність* – із моменту фіксації дані не можуть бути змінені; будь-яке дослідження здійснюється на копіях;
- *автентичність* – можливість довести, що дані походять саме з указаного джерела та є тими самими, що були зафіксовані;
- *ланцюг зберігання доказів* – безперервне документування кожного факту доступу до носія та його передання від моменту вилучення до дослідження в суді;

---

[120] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Luxembourg: Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

[121] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva : ISO/IEC, 2012.; ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. Geneva : ISO/IEC, 2015.; ISO/IEC 27043:2015. Information technology – Security techniques – Incident investigation principles and processes. Geneva : ISO/IEC, 2015.

[122] INTERPOL. Global Guidelines for Digital Forensics Laboratories. Lyon : INTERPOL Global Complex for Innovation, 2019. URL: https://www.interpol.int.

[123] ENISA. Electronic evidence – a basic guide for First Responders. Heraklion : European Union Agency for Network and Information Security, 2014. URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders.

- *документованість і відтворюваність* – фіксація всіх дій, застосованих засобів та їх параметрів у обсязі, що дозволяє незалежному фахівцю повторити процедуру й одержати той самий результат;

- *мінімальне втручання* – обрання способу збирання, який найменше змінює стан системи-джерела; якщо зміни неминучі (робота з увімкненим пристроєм), вони документуються.

Наведені принципи не є суто технічними рекомендаціями: їх порушення суд оцінює крізь призму статей 86-89 КПК, а неможливість перевірити цілісність даних ставить під сумнів достовірність доказу та здатна знецінити результати всього розслідування[124].

Алгоритм виявлення цифрових слідів є цілеспрямованою діяльністю з установлення потенційних джерел доказової інформації та охоплює чотири етапи.

Етап 1. Аналіз первинної інформації про кіберінцидент. Джерелами може бути заява потерпілого, повідомлення CERT-UA та галузевих команд реагування, банків і платіжних систем, результати оперативно-розшукової діяльності, матеріали OSINT-моніторингу (підрозділ 2.1), інформація іноземних партнерів тощо. Завдання етапу – реконструювати механізм події та сформувати вихідний набір ідентифікаторів: вектор атаки, задіяні облікові записи, IP-адреси, доменні імена, адреси електронної пошти, криптовалютні гаманці, зразки шкідливого програмного забезпечення, індикатори компрометації.

Етап 2. Побудова карти джерел. На основі первинних даних складається перелік потенційних носіїв слідів:

- кінцеві пристрої потерпілих і фігурантів;
- власні та орендовані сервери, мережеве обладнання;
- бази даних операторів і постачальників електронних комунікаційних послуг;
- хмарні сервіси, месенджери, поштові та хостинг-провайдери;
- криптовалютні біржі й обмінні сервіси;
- публічні блокчейни тощо.

Для кожного джерела визначаються володілець (розпорядник) інформації, юрисдикція, ймовірний строк зберігання даних і необхідна процесуальна форма доступу; джерела ранжуються за волатильністю та ризиком знищення.

Етап 3. Невідкладне забезпечення збереження даних. Паралельно з процесуальним оформленням надсилаються запити про термінове збереження даних національним провайдерам та – щодо іноземних сервісів – через контактну мережу 24/7 (про що йтиметься нижче); загальнодоступний контент (вебсторінки, оголошення на тіньових майданчиках, публікації у

[124] Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13.; Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139.

месенджерах) фіксується оглядом із технічною фіксацією до його можливого видалення.

Етап 4. Планування скоординованого збирання. Для проваджень щодо організованих угруповань обов'язковими є одночасність обшуків та оглядів у всіх фігурантів, синхронізація з міжнародними партнерами при транскордонній інфраструктурі, завчасний розподіл спеціалістів і криміналістичної техніки, підготовка сценаріїв дій для типових ситуацій (увімкнений/вимкнений пристрій, ознаки шифрування, спротив і т.п.).

Алгоритм збору (фіксації) цифрових слідів здійснюється у процесуальних формах, передбачених КПК, вибір яких визначається правовим режимом доступу до інформації (узагальнено у табл. 2.1).

Таблиця 2.1

Процесуальні форми збирання цифрових слідів (доказів)

Процесуальна форма	***Умови застосування***	***Типові об'єкти та результат***
Витребування та отримання речей і документів (ч. 2 ст. 93 КПК)	Добровільне надання володільцем; відсутність охоронюваної законом таємниці	Довідки, лог-файли, записи камер спостереження, надані потерпілим або юридичною особою копії даних
Огляд, у т. ч. комп'ютерних даних (ст. 237 КПК)	Загальнодоступність даних або добровільно наданий доступ; огляд житла – за ухвалою чи добровільною згодою володільця	Вебсторінки, вміст добровільно виданого пристрою, попередньо зафіксовані копії даних
Тимчасовий доступ до речей і документів (ст. 159-166 КПК)	Ухвала слідчого судді; для даних операторів – із урахуванням п. 7 ч. 1 ст. 162 КПК	Дані про з'єднання, абонентів, надання послуг; банківські записи; копії комп'ютерних даних без вилучення систем
Обшук (ст. 234-236 КПК)	Ухвала слідчого судді; вилучення електронних систем – лише якщо вони прямо зазначені в ухвалі (ч. 2 ст. 168 КПК)	Пристрої та носії, посекторні криміналістичні копії, волатильні дані, зафіксовані на місці
Негласні слідчі (розшукові) дії (ст. 263, 264, 268, 271 КПК)	Ухвала слідчого судді апеляційного суду; за загальним правилом – тяжкі та особливо тяжкі злочини (ст. 246 КПК)	Зміст комунікацій у реальному часі, дані закритих систем, результати контролю за вчиненням злочину

Найбільш універсальною дією є *огляд*: стаття 237 КПК у редакції Закону № 2137-IX прямо передбачає огляд комп'ютерних даних[125]. Огляд

[125] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.; Про внесення змін до Кримінального процесуального

загальнодоступних інтернет-ресурсів проводиться з обов'язковим відображенням у протоколі URL-адреси, дати й точного часу, порядку доступу, застосованих програмно-технічних засобів, зі збереженням копій даних (знімки екрана та збережені копії сторінок як додатки) й обчисленням їх геш-значень. Огляд мобільного термінала, добровільно виданого особою, яка повідомила пароль доступу, не потребує ухвали слідчого судді: за позицією Касаційного кримінального суду Верховного Суду, добровільне розкриття учасником спілкування його таємниці виключає втручання у приватне спілкування, а частина друга статті 264 КПК допускає зняття інформації з електронних інформаційних систем без дозволу суду, якщо доступ до них не обмежується власником, володільцем або утримувачем чи не пов'язаний із подоланням системи логічного захисту[126]. Водночас добровільність надання доступу має бути належно задокументована (письмова заява, відеофіксація роз'яснення прав), інакше сторона захисту небезпідставно ставитиме її під сумнів.

Тимчасовий доступ до речей і документів є основним каналом одержання від операторів і постачальників електронних комунікаційних послуг відомостей про зв'язок, абонента, надання послуг, їх тривалість, зміст і маршрути передавання (п. 7 ч. 1 ст. 162 КПК). Обов'язок постачальників зберігати та надавати таку інформацію в установленому порядку кореспондує Закону України «Про електронні комунікації»[127]. Принципова новела Закону № 2137-IX полягає в тому, що тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів здійснюється шляхом зняття копії інформації без вилучення самих систем[128]. Типовими причинами відмов слідчих суддів у задоволенні клопотань є необґрунтованість значення конкретних даних для провадження, недоведеність неможливості довести відповідні обставини в інший спосіб щодо охоронюваної таємниці (ч. 6 ст. 163 КПК) та звернення неналежним суб'єктом[129]. Звідси практична рекомендація: період і перелік даних у клопотанні формулювати вузько й аргументовано, пов'язуючи кожну позицію з конкретною обставиною предмета доказування.

Під час *обшуку* пріоритет надається копіюванню інформації: частина друга статті 168 КПК допускає тимчасове вилучення електронних

кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

[126] Постанова Касаційного кримінального суду Верховного Суду від 21.11.2024. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/123314009.

[127] Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

[128] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text; Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

[129] Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13.

інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів лише тоді, коли вони прямо зазначені в ухвалі суду. В інших випадках інформація копіюється із залученням спеціаліста[130]. Тому в клопотанні про обшук слід заздалегідь індивідуалізувати техніку, що підлягатиме вилученню, та обґрунтовувати неможливість обмежитися копіюванням (застосування повнодискового шифрування, потреба дослідження апаратної частини, ризик активації механізмів самознищення даних). Ігнорування цієї вимоги залишається однією з найпоширеніших підстав визнання доказів недопустимими.

Доступ до закритих систем та комунікацій у реальному часі забезпечують *негласні слідчі (розшукові) дії*:

- зняття інформації з електронних комунікаційних мереж (ст. 263 КПК);
- зняття інформації з електронних інформаційних систем із подоланням системи логічного захисту (ч. 1 ст. 264 КПК);
- установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК);
- контроль за вчиненням злочину (ст. 271 КПК), зокрема у формі оперативної закупки на тіньових торговельних майданчиках.

Фіксація ходу й результатів здійснюється за статтею 252 КПК та міжвідомчою Інструкцією про організацію проведення негласних слідчих (розшукових) дій[131]. Слід ураховувати, що більшість цих дій проводиться лише у провадженнях щодо тяжких або особливо тяжких злочинів (ст. 246 КПК), що для типових проявів організованої кіберзлочинності, як правило, виконується.

Особливої алгоритмізації потребує робота з волатильними даними безпосередньо на місці проведення слідчої (розшукової) дії. Рекомендується така послідовність дій, здійснюваних слідчим спільно зі спеціалістом:

1) убезпечити обстановку: відсторонити присутніх від пристроїв, зафіксувати фото- та відеозйомкою стан техніки – вміст екранів, підключені кабелі й накопичувачі, серійні номери;

2) не вимикати увімкнені пристрої: за наявності ознак повнодискового шифрування (BitLocker, VeraCrypt, LUKS тощо) вимкнення живлення призведе до безповоротної втрати доступу до даних; спеціаліст знімає образ оперативної пам'яті, фіксує активні мережеві з'єднання, запущені процеси та змонтовані криптоконтейнери;

3) негайно ізолювати мобільні пристрої від мереж (режим польоту, екранувальні пакети Фарадея) для запобігання дистанційному стиранню або блокуванню;

---

[130] Там само.

[131] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ Генеральної прокуратури України, МВС України, СБУ, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.

4) вимкнені пристрої не вмикати: їх дослідження проводиться в лабораторних умовах;

5) виконати криміналістичне копіювання: посекторний (побітовий) образ носія з використанням апаратних блокаторів запису; подальша робота ведеться виключно з робочою копією, оригінал опечатується;

6) обчислити геш-значення оригіналу та копії за стійким алгоритмом (SHA-256) і зафіксувати їх у протоколі: збіг геш-значень є технічною гарантією цілісності й ідентичності даних;

7) упакувати та маркувати носії (антистатичне пакування, опечатування з підписами учасників) із відображенням у протоколі індивідуальних ознак кожного об'єкта;

8) започаткувати ланцюг зберігання: кожне наступне передання носія документується (від кого, кому, коли, з якою метою) відповідно до Порядку зберігання речових доказів[132].

Залучення спеціаліста (ст. 71 КПК) у наведеному алгоритмі не є факультативним: частина четверта статті 99 КПК визнає судом як оригінал документа лише ті копії інформації, у тому числі комп'ютерних даних, що виготовлені слідчим, прокурором саме із залученням спеціаліста[133]. Організаційні засади такого залучення визначено Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України[134].

Аналіз цифрових слідів здійснюється на двох рівнях: попереднє (орієнтуюче) дослідження та судова експертиза.

Попереднє дослідження криміналістичних копій виконується слідчим і аналітиком із залученням спеціаліста та охоплює індексацію й пошук за ключовими словами та ідентифікаторами, відновлення видалених файлів, аналіз артефактів операційних систем (журнали подій, системний реєстр, історія браузерів, кеш застосунків), побудову хронології подій шляхом кореляції часових позначок. Його результати мають орієнтуюче значення для висунення версій і планування подальших дій та не замінюють висновку експерта.

Судова експертиза призначається в порядку статей 242-243 КПК. Профільними є комп'ютерно-технічна експертиза та експертиза комунікаційних систем і засобів, а в частині фінансових потоків – судово-

---

[132] Порядок зберігання речових доказів стороною обвинувачення, їх реалізації, технологічної переробки, знищення, здійснення витрат, пов'язаних з їх зберіганням і пересиланням : постанова Кабінету Міністрів України від 19.11.2012 № 1104. URL: https://zakon.rada.gov.ua/laws/show/1104-2012-п#Text

[133] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.; Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

[134] Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

економічні дослідження. Підготовка матеріалів здійснюється з урахуванням Науково-методичних рекомендацій Міністерства юстиції України[135]. На дослідження передається криміналістична копія (образ) із зазначенням геш-значень. Типовими питаннями експертові є, зокрема:

- чи міститься на наданому носії (в образі) інформація щодо визначених обставин, у тому числі у видаленому, зашифрованому чи прихованому вигляді, і чи можливе її відновлення;
- коли та з використанням якого облікового запису створено, змінено, скопійовано або видалено відповідні файли;
- чи наявне на носії шкідливе програмне забезпечення, які його функціональні можливості та чи є сліди його застосування;
- чи здійснювався з пристрою доступ до визначених мережевих ресурсів (IP-адрес, доменів, облікових записів) і в які періоди;
- чи використовувався пристрій для адміністрування визначеної інфраструктури (серверів, гаманців, акаунтів);
- чи є ідентичними надані копії комп'ютерних даних і дані-зразки, чи збігаються їх геш-значення.

На рівні провадження щодо організованого угруповання аналіз спрямований на кореляцію даних із різних джерел:

- зіставлення журналів провайдерів із даними, вилученими у фігурантів;
- побудову графів зв'язків «особа – пристрій – обліковий запис – гаманець – сервер»;
- простеження криптовалютних транзакцій (кластеризація адрес, проходження через міксери) з подальшим закріпленням результатів шляхом тимчасового доступу до записів бірж і обмінних сервісів;
- часовий аналіз активності для встановлення ієрархії та ролей учасників.

Інструментальна база такого аналізу (аналітичні платформи, засоби блокчейн-аналізу, системи штучного інтелекту) розглянута в підрозділі 2.2. Принципово, що результати автоматизованого аналізу мають статус орієнтуючої інформації, а їх трансформація у докази відбувається виключно через процесуальні дії. Кожен висновок аналітичної системи підлягає верифікації людиною та підтвердженню первинними даними, здобутими у процесуальний спосіб.

Процесуальне закріплення полягає в наданні виявленим і зафіксованим слідам статусу доказів. Вимоги до протоколів слідчих (розшукових) дій визначені статтями 104-107 КПК: у протоколі послідовно відображаються всі дії, застосовані технічні засоби та програмне забезпечення (найменування, версії, налаштування), умови й порядок їх використання, отримані результати; носії з копіями комп'ютерних даних долучаються як додатки (ст. 105 КПК).

[135] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

Фіксування за допомогою технічних засобів (ст. 107 КПК) за клопотанням учасників є обов'язковим. Для дій із цифровими слідами суцільна відеофіксація доцільна в усіх випадках, оскільки саме вона дозволяє згодом продемонструвати суду коректність кожної операції.

Аналіз судової практики дозволяє виокремити типові помилки, що призводять до визнання цифрових доказів недопустимими на підставі статей 86-89 КПК[136]:

- вилучення комп'ютерної техніки, прямо не зазначеної в ухвалі про обшук, усупереч частині другій статті 168 КПК;
- копіювання комп'ютерних даних без залучення спеціаліста, що позбавляє копію статусу оригіналу за частиною четвертою статті 99 КПК;
- відсутність у протоколі відомостей про застосовані програмно-технічні засоби та геш-значення, що унеможливлює перевірку цілісності даних;
- подолання паролів і систем логічного захисту під виглядом огляду без ухвали слідчого судді, всупереч статті 264 КПК, або недоведеність добровільності наданого доступу;
- розрив ланцюга зберігання: неопечатані носії, недокументовані передання, дослідження оригіналу замість робочої копії.

Способи уникнення цих помилок є організаційними: запровадження у підрозділах контрольних переліків (чек-листів) для кожної процесуальної форми, типових шаблонів протоколів із «цифровими» реквізитами (геш-значення, ідентифікатори носіїв, версії програмного забезпечення), подвійна перевірка меж судових ухвал перед виконанням, залучення спеціаліста за замовчуванням, а в сумнівних ситуаціях – обрання більш суворої процесуальної форми з судовим контролем.

Транснаціональний характер організованої кіберзлочинності робить міжнародні механізми невіддільним елементом наведених алгоритмів. Базовим інструментом є Конвенція про кіберзлочинність[137], що передбачає термінове збереження комп'ютерних даних (ст. 16, 29), термінове розкриття збережених даних про рух інформації (ст. 17, 30), взаємну допомогу щодо доступу до збережених даних (ст. 31), транскордонний доступ до загальнодоступних даних або за добровільною згодою володільця (ст. 32) та цілодобову контактну мережу 24/7 (ст. 35), функції національного вузла якої за законом про ратифікацію покладено на Міністерство внутрішніх справ України і які практично реалізуються за участю Департаменту кіберполіції Національної поліції України. Стандартний алгоритм дій включає негайний запит про збереження даних через мережу 24/7 (збереження забезпечується на

[136] Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. Право і безпека. 2024. № 2 (93). С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13.; Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139; Гутник А.В., Хитра А.Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів : ЛьвДУВС, 2022. 204 с.

[137] Конвенція про кіберзлочинність від 23.11.2001, ратифікована Законом України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575.

строк до 90 діб із можливістю поновлення) з подальшим офіційним запитом про міжнародну правову допомогу для розкриття збережених даних.

Другий додатковий протокол до Конвенції (CETS № 224) про посилене співробітництво та розкриття електронних доказів, підписаний Україною 30 листопада 2022 року, запроваджує механізми прямої взаємодії з постачальниками послуг інших сторін щодо абонентської інформації та реєстраційних даних доменних імен, прискорені процедури для невідкладних випадків, спільні слідчі групи й допити відеоконференцією. Станом на середину 2026 року протокол не набув чинності (потребує п'яти ратифікацій), тож його ратифікація та імплементація залишаються актуальним завданням для України[138]. У поточній практиці застосовуються платформа SIRIUS Європолу зі стандартизованими формами прямих запитів до онлайн-сервісів, канали Europol та ІНТЕРПОЛу для обміну оперативними даними, процедури добровільного розкриття даних провайдерами у невідкладних випадках, а також спільні слідчі групи (ст. 571 КПК). При цьому дані, одержані неформальними або оперативними каналами, мають орієнтуюче значення: для використання як доказів вони підлягають легалізації в порядку міжнародної правової допомоги або закріпленню шляхом процесуальних дій на території України.

Отже, алгоритми виявлення, збору, аналізу та процесуального закріплення цифрових слідів (доказів) перетворює програмно-технічні можливості, описані в підрозділах 2.1 і 2.2, на допустиму доказову базу у провадженнях щодо організованих кіберзлочинних угруповань. Наскрізними вимогами всіх етапів є обов'язкове залучення спеціаліста, гешування та ланцюг зберігання, точний вибір процесуальної форми відповідно до правового режиму інформації, а також своєчасне задіяння механізмів міжнародного співробітництва з огляду на транскордонність слідової картини. Запропоновані алгоритми доцільно закріпити у типових чек-листах, а їх засвоєння зробити невід'ємним елементом службової підготовки правоохоронців, що мають відношення до сфери протидії організованої кіберзлочинності. Дотримання цих вимог гарантує, що інноваційні інструменти виявлення й аналізу не залишаться на рівні орієнтуючої інформації, а послідовно трансформуватимуться у стійку до оскарження доказову базу.

[138] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Strasbourg : Council of Europe, 12.05.2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol.

ВИСНОВКИ

Проведене дослідження теоретико-правових засад, актуальних тенденцій та сучасних практик діяльності поліції у сфері протидії організованій кіберзлочинності дало змогу сформувати цілісне уявлення про природу цього явища, закономірності його розвитку, особливості функціонування кіберзлочинних мереж, а також визначити пріоритетні напрями підвищення спроможності правоохоронних органів своєчасно виявляти, документувати та припиняти відповідну кримінальну діяльність.

Установлено, що організована кіберзлочинність не може розглядатися лише як сукупність відокремлених кримінальних правопорушень, учинених із використанням інформаційно-комунікаційних технологій. Вона являє собою складну, динамічну й адаптивну кримінальну екосистему, в якій взаємопов'язані людські, технологічні, інформаційні, інфраструктурні та фінансові ресурси. Визначальним є не сам факт застосування цифрових технологій, а системний спосіб організації кримінальної діяльності, що виявляється у стійкості взаємодії учасників, погодженості їхніх дій, функціональному розподілі ролей, повторюваності операцій, спільності кримінальної мети, використанні спеціалізованої інфраструктури та наявності механізмів одержання, переміщення й легалізації кримінальних доходів.

Організована кіберзлочинність охоплює як кіберзалежні кримінальні правопорушення, учинення яких неможливе без комп'ютерних систем, так і кіберпідсилені діяння, у межах яких цифрові технології забезпечують масштабування традиційного шахрайства, вимагання, незаконного обігу даних, заволодіння коштами, легалізації доходів та інших форм протиправної діяльності. На практиці такі діяння часто є послідовними елементами одного кримінального циклу: несанкціонований доступ до інформаційної системи або компрометація облікових даних створюють умови для викрадення інформації, шахрайства, вимагання, переміщення активів, приховування цифрових слідів і повторного використання скомпрометованої інфраструктури. Тому правова та кримінологічна оцінка має охоплювати весь механізм підготовки, ресурсного забезпечення, учинення, монетизації та приховування кримінальної діяльності.

Сучасні організовані кіберзлочинні угруповання здебільшого функціонують за мережевою, модульною та сервісно орієнтованою моделями, які істотно відрізняються від традиційної ієрархічної будови організованої групи. Учасники такої мережі можуть перебувати у різних державах, використовувати псевдоніми й зашифровані канали комунікації, не знати справжніх установчих даних інших співучасників та вступати у взаємодію лише на певному етапі кримінальної операції. Проте дистанційність і відсутність безпосередніх особистих контактів не виключають організованого характеру діяльності, якщо встановлено системність взаємодії, функціональну взаємозалежність виконуваних дій та усвідомлення учасниками їх спільної кримінальної спрямованості.

За таких умов установлення структури організованого кіберзлочинного угруповання потребує аналізу не лише особистих контактів, а й цифрових, комунікаційних, інфраструктурних, фінансових, поведінкових і часових зв'язків. Саме їх сукупність дає змогу визначити організаторів і координаторів, відтворити фактичний розподіл функцій, установити роль постачальників кримінальних послуг та довести внесок кожного учасника у досягнення спільного злочинного результату.

Однією з найбільш стійких тенденцій є поширення моделі «кіберзлочинність як послуга», у межах якої окремі складові кримінальної операції пропонуються на нелегальному ринку як самостійні продукти або сервіси. Доступи до скомпрометованих інформаційних систем, шкідливе програмне забезпечення, фішингові комплекти, викрадені дані, серверні потужності, засоби анонімізації, інструменти обходу механізмів захисту та послуги з переміщення віртуальних активів можуть надаватися різними суб'єктами й поєднуватися для досягнення єдиного кримінального результату.

Сервісна модель відокремлює кримінальну ініціативу від необхідної для її реалізації технічної компетентності, знижує бар'єр входження до кіберзлочинного середовища та забезпечує масштабованість кримінальних операцій. Водночас один постачальник незаконної послуги може обслуговувати значну кількість незалежних злочинних мереж. Це дає підстави вважати, що пріоритетними об'єктами правоохоронного впливу мають бути не лише безпосередні виконавці окремих атак, а й брокери первинного доступу, адміністратори підпільних платформ, оператори абузостійкої інфраструктури, розробники шкідливого програмного забезпечення, фінансові посередники та інші суб'єкти, які забезпечують життєздатність кримінальної екосистеми.

Організована кіберзлочинність характеризується високою адаптивністю та здатністю до оперативного відновлення. Блокування домену, вилучення серверів, припинення діяльності окремого підпільного майданчика або затримання частини учасників не завжди призводять до остаточного припинення кримінальної діяльності. Втрачені ресурси можуть бути замінені, функції передані іншим виконавцям, а інфраструктура відновлена під новою назвою або в іншій юрисдикції. Водночас кожне таке відновлення залишає ознаки наступності: повторно використовувані контакти, фінансові адреси, елементи програмного коду, конфігурації серверів, мовні особливості комунікації, часові закономірності та поведінкові шаблони. Їх виявлення й зіставлення дає змогу пов'язати між собою формально відокремлені кримінальні епізоди та встановити приховану сталість злочинної мережі.

Центральним результатом дослідження є обґрунтування інтегрованої екосистемної моделі протидії організованій кіберзлочинності. Її зміст полягає у переході від розслідування ізольованих кримінальних епізодів до системного виявлення та нейтралізації організаційного ядра злочинної мережі, її цифрової інфраструктури, кримінальних сервісів, інформаційних ресурсів, фінансових механізмів і транскордонних зв'язків.

Застосування такої моделі передбачає одночасне дослідження складу учасників, їхніх ролей, компетенцій і способів координації; доменів, серверів, IP-адрес, бот-мереж, програмних засобів та інших технічних ресурсів; тактик, методів і повторюваних сценаріїв кримінальної діяльності; цифрових ідентифікаторів, облікових записів і масивів викрадених даних; джерел кримінальних доходів, платіжних інструментів та маршрутів руху коштів; юрисдикцій, у яких перебувають учасники, потерпілі, інформація й інфраструктура; часової послідовності операцій і швидкості відновлення мережі після правоохоронного втручання.

Практичною метою інтегрованої моделі є встановлення критичних вузлів злочинної екосистеми, припинення функціонування яких здатне порушити не одну кримінальну операцію, а діяльність значної кількості взаємопов'язаних суб'єктів. Тому результативність правоохоронних заходів має визначатися не тільки кількістю проведених обшуків, вилучених пристроїв, затриманих осіб або повідомлень про підозру, а й реальним зниженням спроможностей злочинної мережі, руйнуванням її внутрішніх зв'язків, обмеженням доступу до інфраструктури та фінансових ресурсів, зниженням доступності кримінальних сервісів і тривалістю відновлення протиправної діяльності.

Ефективна реалізація зазначеної моделі потребує поєднання реактивного та проактивного компонентів діяльності поліції. Реактивний компонент забезпечує реагування на вже вчинене кримінальне правопорушення, встановлення його обставин, виявлення потерпілих і причетних осіб, збереження цифрової інформації та притягнення винних до відповідальності. Проактивний компонент передбачає системне оцінювання кіберзагроз, виявлення кримінальних сервісів, спільних індикаторів, повторюваних способів дій, інфраструктурних зв'язків і фінансових маршрутів до їх використання у нових кримінальних епізодах. Це дозволяє перейти від реагування на наслідки до завчасного визначення джерел загрози та концентрації ресурсів поліції на найбільш значущих елементах кримінальної мережі.

Аналіз нормативно-правового забезпечення підтвердив, що в Україні сформовано розгалужену систему правового регулювання у сфері забезпечення кібербезпеки, протидії кіберзлочинності, реагування на кіберінциденти й кібератаки, захисту інформаційних та інформаційно-комунікаційних систем, а також об'єктів критичної інфраструктури. Водночас наявність значної кількості нормативно-правових актів не завжди забезпечує узгодженість практики їх застосування. Подальшого вирішення потребують питання розмежування компетенції суб'єктів, оперативного міжвідомчого обміну інформацією, отримання комп'ютерних даних із транскордонних інформаційних систем, правових меж автоматизованої аналітики та єдиних стандартів поводження із цифровими доказами.

Удосконалення нормативного й організаційного забезпечення має бути спрямоване на узгодження повноважень суб'єктів національної системи

кібербезпеки, розроблення типових процедур взаємодії підрозділів стратегічних розслідувань, кіберполіції, слідчих підрозділів і кримінальних аналітиків, удосконалення механізмів термінового збереження комп'ютерних даних, визначення правових засад застосування штучного інтелекту, стандартизацію документування цифрових слідів та адаптацію європейських механізмів отримання електронних доказів до потреб національної правоохоронної практики.

Транснаціональний характер організованої кіберзлочинності зумовлює необхідність розглядати міжнародне співробітництво як невід'ємний складник кожного складного кримінального провадження. Цифрові дані можуть зберігатися за межами України, контролюватися іноземними постачальниками послуг і видалятися через нетривалий строк. Тому іноземна юрисдикція, місце зберігання даних, постачальник відповідної послуги та доступний механізм збереження інформації мають установлюватися вже на початковому етапі розслідування.

У практичній діяльності необхідно комплексно використовувати можливості Конвенції про кіберзлочинність, цілодобової контактної мережі 24/7, міжнародної правової допомоги, каналів Європолу та Інтерполу, платформи SIRIUS і спільних слідчих груп. Водночас інформація, отримана через оперативні або аналітичні міжнародні канали, повинна чітко відмежовуватися від доказів. Для її використання у кримінальному провадженні необхідно забезпечити отримання первинних даних у встановленому порядку, належне процесуальне закріплення та можливість перевірки джерела їх походження.

Розвідка на основі відкритих джерел і цифрова криміналістика мають застосовуватися як взаємопов'язані складові єдиного інформаційно-аналітичного циклу. OSINT забезпечує виявлення цифрових ідентифікаторів, облікових записів, електронних адрес, номерів телефонів, доменів, мережевої інфраструктури, публічних комунікацій та інших відомостей, які визначають напрями подальшого дослідження. Цифрова криміналістика забезпечує пошук, збереження, відновлення й аналіз артефактів, локалізованих на електронних пристроях, серверах, у хмарних середовищах та інформаційних системах.

Результати OSINT повинні визначати об'єкти цифрового криміналістичного дослідження, а виявлені цифрові артефакти – формувати нові пошукові ознаки для відкритої розвідки. Такий циклічний характер роботи забезпечує послідовне уточнення інформаційної моделі події та дає змогу перейти від накопичення розрізнених цифрових відомостей до відтворення структури й механізму кримінальної діяльності. При цьому якість OSINT-дослідження визначається не кількістю використаних сервісів або обсягом зібраної інформації, а правильністю формулювання інформаційної потреби, системністю пошуку, надійністю джерел, верифікацією результатів і повнотою документування виконаних дій.

Кримінальний аналіз у межах запропонованої моделі виконує системоутворювальну функцію. Його призначення полягає у перетворенні різнорідних і фрагментарних даних на перевірене знання про структуру, спроможності, поведінку та вразливі елементи злочинної мережі. Для цього інформація з кримінальних проваджень та оперативно-розшукової діяльності має інтегруватися з результатами OSINT, цифрової криміналістики, фінансового і блокчейн-аналізу, відомостями про кіберінциденти та інформацією міжнародних партнерів.

Результатом кримінального аналізу повинен бути не опис уже відомих обставин, а встановлення функціональної структури мережі, ролей її учасників, повторно використовуваної інфраструктури, способів монетизації кримінальної діяльності, критичних вузлів і найбільш імовірних напрямів подальшої активності. Кримінальний аналіз має супроводжувати весь цикл протидії – від первинного виявлення ознак організованої кіберзлочинної діяльності до оцінювання довгострокових результатів проведеної операції.

Системи штучного інтелекту та аналітичні платформи розширюють можливості поліції щодо опрацювання значних масивів структурованих і неструктурованих даних, виявлення прихованих зв’язків, кластеризації цифрових об’єктів, установлення аномалій, аналізу повторюваних моделей поведінки, автоматизованої кореляції індикаторів кіберзагроз і відстеження руху віртуальних активів. Їх використання може скоротити час первинного опрацювання інформації, підвищити обґрунтованість аналітичних версій та сприяти виявленню закономірностей, які складно встановити шляхом ручного аналізу.

Водночас результати роботи систем штучного інтелекту не можуть визнаватися безумовно достовірними або використовуватися як самостійна підстава для прийняття процесуальних рішень. Вони мають статус орієнтуючої інформації, яка підлягає перевірці уповноваженим працівником і підтвердженню первинними даними, отриманими у законний спосіб. Застосування штучного інтелекту має ґрунтуватися на принципах законності, пропорційності, пояснюваності, недискримінації, захисту персональних даних та обов’язкового людського контролю. Необхідними гарантіями є документування параметрів застосованої системи, ведення журналів автоматизованої обробки, перевірка точності результатів, періодичний аудит алгоритмів і можливість відтворення логіки сформованого висновку.

Виявлення цифрової інформації не є тотожним отриманню цифрового доказу. Цифровий слід набуває доказового значення лише за умови його одержання у визначеному законом порядку, належної фіксації, збереження, перевірки, дослідження та долучення до матеріалів кримінального провадження. Технічна достовірність цифрового об’єкта не усуває наслідків порушення процесуального порядку його отримання, так само як формальне дотримання процесуальної форми не може компенсувати технічно некоректне копіювання або дослідження даних.

Робота із цифровими слідами має здійснюватися як послідовний процес, що охоплює визначення потенційних джерел цифрової інформації, оцінювання нестійкості даних, фіксацію початкового стану пристроїв, залучення спеціаліста, вибір належної процесуальної форми, криміналістичне копіювання, обчислення геш-значень, пакування та зберігання носіїв, дослідження робочої копії, аналітичну інтерпретацію і процесуальне закріплення отриманих результатів. Пріоритетність дій має визначатися з урахуванням конкретної ситуації, стану пристрою, наявності шифрування або віддаленого доступу та ризику безповоротної втрати інформації.

Наскрізними умовами належного поводження із цифровими доказами є забезпечення їх автентичності, цілісності, відтворюваності та належного походження. З цією метою необхідно створювати криміналістичні копії, обчислювати й документувати геш-значення, досліджувати робочі копії замість оригінальних носіїв, забезпечувати безперервність ланцюга зберігання та фіксувати кожне передання цифрового об’єкта. Особливу загрозу для допустимості доказів становлять вихід за межі судового дозволу, копіювання комп’ютерних даних без участі спеціаліста, подолання систем логічного захисту без належної процесуальної підстави, відсутність контрольних цифрових значень і розрив ланцюга зберігання.

Між орієнтуючою інформацією та доказом має існувати чіткий і документований процесуальний перехід. Результати OSINT, кримінального аналізу, блокчейн-аналітики та застосування систем штучного інтелекту можуть використовуватися для формування версій, визначення напрямів розслідування і планування процесуальних дій, але не повинні підміняти доказування. Трансформація виявленої інформації у доказову базу передбачає її аналітичне оцінювання, перевірку за незалежними джерелами, встановлення первинного джерела, визначення належної процесуальної форми отримання, фіксацію, збереження, криміналістичне дослідження та подальше оцінювання належності, допустимості й достовірності.

Практична реалізація інтегрованої моделі потребує узгоджених дій на стратегічному, оперативному й тактичному рівнях. На стратегічному рівні необхідно забезпечити системне оцінювання організованих кіберзагроз, визначення пріоритетних злочинних мереж, сервісів та інфраструктурних вузлів, планування ресурсів і розвиток міжнародного співробітництва. Оперативний рівень має охоплювати інтеграцію інформації, формування міждисциплінарних груп, установлення зв’язків між окремими кримінальними епізодами та планування комплексних заходів. На тактичному рівні необхідним є застосування стандартизованих алгоритмів роботи із цифровими даними та доказами.

Доцільним є запровадження у підрозділах Національної поліції України типових алгоритмів, контрольних переліків і шаблонів процесуальних документів для проведення OSINT-досліджень, первинного реагування на кіберінциденти, огляду цифрових пристроїв, проведення обшуку, копіювання комп’ютерних даних, роботи з хмарними сервісами, отримання інформації від

постачальників послуг, аналізу віртуальних активів та використання міжнародних механізмів збереження даних. Такі інструменти мають не замінювати професійне рішення працівника, а мінімізувати ризик пропуску критично важливих технічних і процесуальних дій.

Необхідною умовою ефективності запропонованої моделі є системна професійна підготовка працівників поліції. Її зміст повинен охоплювати методологію OSINT, цифрову криміналістику, кримінальний, фінансовий і блокчейн-аналіз, правила поводження із цифровими доказами, міжнародні механізми отримання інформації, принципи відповідального використання штучного інтелекту, захист персональних даних і дотримання прав людини. Підготовка має бути практико-орієнтованою та відтворювати повний цикл діяльності – від отримання первинної інформації та формулювання аналітичного завдання до встановлення структури злочинної мережі, збереження цифрових слідів і процесуального закріплення доказів.

Таким чином, основним результатом проведеного дослідження є формування інтегрованої моделі протидії організованій кіберзлочинності, у межах якої:

- стратегічне оцінювання загроз визначає пріоритети правоохоронної діяльності;
- кримінальний аналіз забезпечує встановлення структури та критичних вузлів злочинної мережі;
- OSINT і цифрова криміналістика використовуються для виявлення, перевірки та дослідження цифрової інформації;
- аналітичні платформи й системи штучного інтелекту розширюють можливості опрацювання значних масивів даних;
- процесуальні алгоритми забезпечують трансформацію отриманих відомостей у допустимі докази;
- міжнародне співробітництво створює можливості для доступу до транскордонної інформації та скоординованого впливу на злочинну інфраструктуру.

Інноваційні технології у цій моделі не замінюють працівника поліції та не усувають необхідності професійної оцінки. Їх призначення полягає у розширенні можливостей людини щодо пошуку, систематизації, зіставлення, перевірки й аналізу інформації. Остаточне рішення щодо значення отриманих результатів, напряму подальших дій та належної процесуальної форми їх реалізації повинно залишатися за уповноваженою особою.

Принципово важливим є забезпечення нерозривного зв’язку між технологічною результативністю та законністю. Жоден, навіть найбільш точний аналітичний результат не може компенсувати порушення прав людини або встановленого законом порядку отримання доказів. Водночас формальне дотримання процесуальної форми не забезпечить результативності, якщо цифрові дані були втрачені, пошкоджені або технічно неправильно досліджені. Тому правова, організаційна, аналітична, технологічна і криміналістична складові повинні функціонувати як елементи єдиної системи.

Стратегічною метою діяльності поліції має бути не лише розкриття окремого кримінального правопорушення, а системне зниження спроможності організованих кіберзлочинних мереж до відновлення, масштабування та повторного вчинення протиправних діянь. Саме здатність своєчасно виявити злочинну екосистему, установити її організаційне ядро та критичні елементи, юридично правильно зафіксувати цифрові сліди і забезпечити скоординований вплив на технологічні, інформаційні та фінансові основи її функціонування визначатиме реальну ефективність протидії організованій кіберзлочинності в сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вікторчук М. В., Багатко А. С. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 86, ч. 3. С. 257-263. DOI: https://doi.org/10.24144/2307-3322.2024.86.3.39.

2. Грищук В. Р. Електронні (цифрові) дані у кримінальному провадженні: від електронного сліду до доказу. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. Вип. 93, ч. 5. С. 68-73. DOI: https://doi.org/10.24144/2307-3322.2026.93.5.9.

3. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів : ЛьвДУВС, 2022. 204 с.

4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 15.07.2026).

5. ДСТУ EN ISO/IEC 27037:2022. Інформаційні технології. Методи захисту. Настанови щодо ідентифікації, збирання, отримання та збереження цифрових доказів (EN ISO/IEC 27037:2016, IDT; ISO/IEC 27037:2012, IDT). Київ : ДП «УкрНДНЦ», 2022.

6. Зачек О. І., Дмитрик Ю. І., Сеник В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19.

7. Зоря І. С., Марущак А. В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. Матеріали конференції Вінницького національного технічного університету. Вінниця : ВНТУ, 2024. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf (дата звернення: 22.07.2026).

8. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; НДІ вивчення проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2024. 208 с.

9. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 29.08.2026).

10. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 29.08.2026).

11. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139.

12. Коваленко А. В. Електронні докази у кримінальному провадженні: сучасний стан та перспективи використання. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2018. № 4. С. 237-245.

13. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2022. № 4. С. 226-236.

14. 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: 17.07.2026).

15. Лунгол О. Методологічні засади атрибуції суб'єктів гібридної агресії в національному кіберпросторі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* Вип. 2, 2025, с. 74-82, doi:10.28925/2663-4023.2025.30.904

16. Макаліш Б. Д., Мойко О. О., Лучик В. Є. Сучасні виклики кіберзлочинності та роль Національної поліції України у їх подоланні. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 309-322. DOI: https://doi.org/10.28925/2663-4023.2025.31.983.

17. Мовчан А. В., Крутік Ю. Ю., Горбенко Г. М. Інформаційне забезпечення кримінального аналізу. Інформаційно-аналітичне забезпечення діяльності Національної поліції України : монографія / за заг. ред. О. Є. Користіна. Київ : ВД «Дакор», 2024. Розд. 14. С. 133-146.

18. Моргунова Т. І. Використання штучного інтелекту в правоохоронній діяльності. Наукові інновації та передові технології. 2025. № 2 (42). С. 638-652.

19. Муравська Ю., Метельський І., Романів Р. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства*. 2024. № 2 (38). С. 90-97.

20. Офіс Генерального прокурора. Про результати діяльності органів правопорядку щодо стану запобігання та протидії правопорушенням, учиненим у сфері кібербезпеки (кіберзлочини). URL: https://www.gp.gov.ua/ua/posts/pro-rezultati-diyalnosti-organiv-pravoporyadku-shodo-stanu-zapobigannya-ta-protidiyi-pravoporushennyam-yaki-vchineno-u-sferi-kiberbezpeki-kiberzlochini (дата звернення: 14.08.2026).

21. Пашковський М. І. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. Концептуальні основи цифровізації кримінального провадження України : монографія / за ред. Н. В. Глинської. Харків : Право, 2024. С. 233-274.

22. Піщенко Г. І., Шопіна Ю. О. Кібербезпека та кіберзлочинність в Україні: сучасні тенденції. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 4, № 92. С. 193-199. DOI: https://doi.org/10.24144/2307-3322.2025.92.4.26.

23. Постанова Касаційного кримінального суду у складі Верховного Суду від 21.11.2024 у справі, реєстраційний номер судового рішення 123314009. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/123314009 (дата звернення: 15.07.2026).

24. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 15.07.2026).
25. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 07.09.2026).
26. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 11.09.2026).
27. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 13.09.2026).
28. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text (дата звернення: 05.09.2026).
29. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ Генеральної прокуратури України, МВС України, СБУ, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення: 11.08.2026).
30. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 11.08.2026).
31. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу : наказ Адміністрації Держспецзв'язку від 30.08.2023 № 773. URL: https://zakon.rada.gov.ua/rada/show/v0773519-23#Text (дата звернення: 23.07.2026).
32. Про затвердження Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози : постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-п#Text (дата звернення: 03.09.2026).
33. Про затвердження Положення про організаційно-технічну модель кіберзахисту : постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text (дата звернення: 04.09.2026).

34. Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього : постанова Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text (дата звернення: 07.09.2026).

35. Про затвердження Порядку взаємодії суб’єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб’єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб’єктами оперативно-розшукової діяльності : постанова Кабінету Міністрів України від 13.11.2025 № 1471. URL: https://zakon.rada.gov.ua/laws/show/1471-2025-п#Text (дата звернення: 07.09.2026).

36. Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту : постанова Кабінету Міністрів України від 17.12.2025 № 1668. URL: https://zakon.rada.gov.ua/laws/show/1668-2025-п#Text (дата звернення: 07.09.2026).

37. Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури : постанова Кабінету Міністрів України від 31.12.2025 № 1799. URL: https://zakon.rada.gov.ua/laws/show/1799-2025-п#Text (дата звернення: 11.09.2026).

38. Про затвердження Порядку організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв’язку : постанова Кабінету Міністрів України від 14.05.2015 № 303. URL: https://zakon.rada.gov.ua/laws/show/303-2015-п#Text (дата звернення: 18.08.2026).

39. Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту : наказ Адміністрації Держспецзв’язку від 24.06.2022 № 284. URL: https://zakon.rada.gov.ua/laws/show/z0758-22#Text (дата звернення: 15.08.2026).

40. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.08.2026).

41. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 15.08.2026).

42. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 15.08.2026).

43. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 15.08.2026).

44. 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: 14.08.2026).

45. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 17.08.2026).

46. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 19.08.2026).

47. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 15.07.2026).

48. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 15.07.2026).

49. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. Право і безпека. 2024. № 2 (93). С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13.

50. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, від 27.06.2014. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 13.08.2026).

51. Чигрина Г. Л. Допустимість використання штучного інтелекту у правоохоронній діяльності. Актуальні проблеми інноваційної економіки та права. 2024. № 2. С. 6–10. DOI: https://doi.org/10.36887/2524-0455-2024-2-1.

52. Шевчук Т. А., Свистун Я. В. Використання штучного інтелекту у протидії злочинності. Вісник кримінологічної асоціації України. 2021. № 2 (25). С. 128–134.

53. Al Shamsi H. R. S., Safei S. Artificial Intelligence Adoption in Predictive Policing to Predict Crime Mitigation Performance. International Journal of Sustainable Construction Engineering and Technology. 2023. Vol. 14, no. 3. P. 289–298. DOI: https://doi.org/10.30880/ijscet.2023.14.03.025.

54. 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. New York ; Geneva : United Nations, 2022. 166 p. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf (accessed: 11.09.2026).

55. DaViera A. L., Uriostegui M., Gottlieb A., Onyeka O. C. Risk, Race, and Predictive Policing: A Critical Race Theory Analysis of the Strategic Subject List. American Journal of Community Psychology. 2024. Vol. 73, no. 1–2. P. 91–103. DOI: https://doi.org/10.1002/ajcp.12671.

56. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed: 11.09.2026).

57. ENISA. Electronic Evidence: A Basic Guide for First Responders. Heraklion : European Union Agency for Network and Information Security, 2014. URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (accessed: 15.09.2026).

58. ENISA. ENISA Threat Landscape 2025. Athens : European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed: 15.09.2026).

59. Europol. Global Operation Targets NoName057(16) Pro-Russian Cybercrime Network. 16.07.2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network (accessed: 15.09.2026).

60. Europol. Global Phishing-as-a-Service Platform Taken Down in Coordinated Public-Private Action. 04.03.2026. URL: https://www.europol.europa.eu/media-press/newsroom/news/global-phishing-service-platform-taken-down-in-coordinated-public-private-action (accessed: 15.09.2026).

61. Europol. How Cybercrime Enablers Are Facilitating Crime: Live Expert Session. 13.05.2026. URL: https://www.europol.europa.eu/publications-events/events/how-cybercrime-enablers-are-facilitating-crime (accessed: 15.09.2026).

62. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Luxembourg : Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (accessed: 15.09.2026).

63. Europol. IOCTA 2026 – The Evolving Threat Landscape: How Encryption, Proxies and AI Are Expanding Cybercrime. 28.04.2026. URL: https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape (accessed: 13.09.2026).

64. Europol. Operation ENDGAME Strikes Again: The Ransomware Kill Chain Broken at Its Source. 23.05.2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source (accessed: 15.08.2026).

65. Europol. Ransomware Gangs Cut Off from EUR 336 Million ‘AudiA6’ Crypto Laundering Pipeline. 11.06.2026. URL:

https://www.europol.europa.eu/media-press/newsroom/news/ransomware-gangs-cut-eur-336-million-audia6-crypto-laundering-pipeline (accessed: 01.09.2026).

66. FATF. Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. Paris : Financial Action Task Force, 2025. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html (accessed: 11.09.2026).

67. Hung T.-W., Yen C.-P. Predictive Policing and Algorithmic Fairness. Synthese. 2023. Vol. 201, no. 6. Article 206. DOI: https://doi.org/10.1007/s11229-023-04189-0.

68. INTERPOL. Global Guidelines for Digital Forensics Laboratories. Lyon : INTERPOL Global Complex for Innovation, 2019. URL: https://www.interpol.int (accessed: 12.09.2026).

69. ISO/IEC 27037:2012. Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva : ISO, 2012.

70. ISO/IEC 27042:2015. Information Technology. Security Techniques. Guidelines for the Analysis and Interpretation of Digital Evidence. Geneva : ISO, 2015.

71. ISO/IEC 27043:2015. Information Technology. Security Techniques. Incident Investigation Principles and Processes. Geneva : ISO, 2015.

72. Lee Y., Bradford B., Posch K. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. Justice Evaluation Journal. 2024. Vol. 7, no. 2. P. 127–160. DOI: https://doi.org/10.1080/24751979.2024.2371781.

73. Opendatabot. Сервіс моніторингу відкритих державних даних. URL: https://opendatabot.ua/open/about (дата звернення: 03.09.2026).

74. OSINT Open Source Intelligence. Інструменти та методи : навчальний посібник / О. Є. Користін, С. В. Демедюк, К. Ю. Ісмайлов, Д. В. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 7БЦ, 2025. 460 с.

75. OSINT Open Source Intelligence. Теорія та методологія : монографія / О. Є. Користін, С. В. Демедюк, О. І. Барановський, Д. В. Ланде та ін. Київ : 7БЦ, 2025. 304 с.

76. Pashniev D. V., Shmatkov D. I., Kolomiitsev S. O., Manzhai O. V., Nosov V. V., Luchyk V. Ye., Serdiuk O. O. AI and OSINT Tools and Methods for Tracing Missing, Deported or Forcibly Displaced Children: Guidelines for the Use of Open Source Intelligence and New Technologies, Including Facial Recognition. Kharkiv : Ministry of Internal Affairs of Ukraine ; Kharkiv National University of Internal Affairs, 2024. 80 p.

77. Raji I., Sholademi D. B. Predictive Policing: The Role of AI in Crime Prevention. International Journal of Computer Applications Technology and Research. 2024. Vol. 13, issue 10. P. 66–78. DOI: https://doi.org/10.7753/IJCATR1310.1006.

78. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L

2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed: 07.09.2026).

79. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224). Strasbourg : Council of Europe, 2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol (accessed: 23.08.2026).

80. UNODC. Emerging Threats: The Intersection of Criminal and Technological Innovation in the Use of Automation and AI. Vienna : United Nations Office on Drugs and Crime, 2025. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf (accessed: 26.08.2026).

81. UNODC. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Vienna : United Nations Office on Drugs and Crime, 2024. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (accessed: 17.08.2026).

82. YouControl. Аналітична система для комплаєнсу, аналізу ринків, ділової розвідки та розслідувань. URL: https://youcontrol.com.ua/about_us/ (дата звернення: 10.09.2026).

Науково-практичне видання

ЛУНГОЛ Ольга Миколаївна

ГАБОРЕЦЬ Ольга Андріївна

ІННОВАЦІЙНІ МЕТОДИКИ ТА СУЧАСНІ ПРАКТИКИ В ДІЯЛЬНОСТІ ПОЛІЦІЇ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ

Науково-практичні рекомендації