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

Науковий нарис

2026

УДК 351.74:343.9.02:004.056(477)(075.8)
Л 84

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

Автори:

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: науковий нарис. _____, 2026. 87 с.

Науковий нарис присвячено інноваційним методикам і сучасним практикам діяльності поліції у сфері протидії організованій кіберзлочинності. Розкрито сучасний стан, тенденції та специфіку функціонування організованої кіберзлочинності, нормативно-правові засади й передовий міжнародний досвід протидії кіберзагрозам, а також практичні можливості розвідки на основі відкритих джерел (OSINT) і цифрової криміналістики, систем штучного інтелекту та предиктивної аналітики, алгоритми виявлення, збору, аналізу й процесуального закріплення цифрових слідів (доказів).

Нарис розрахований на здобувачів усіх рівнів вищої освіти закладів вищої освіти зі специфічними умовами навчання, які здійснюють підготовку фахівців для підрозділів кримінальної поліції, а також на практичних працівників.

УДК 351.74:343.9.02:004.056(477)(075.8)

© Донецький державний університет внутрішніх справ, 2026

ЗМІСТ

ПЕРЕДМОВА **5**

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ **7**

РОЗДІЛ 1. ОРГАНІЗОВАНА КІБЕРЗЛОЧИННІСТЬ: СУЧАСНИЙ СТАН, ТЕНДЕНЦІЇ ТА СПЕЦИФІКА **9**

1.1. Поняття організованої кіберзлочинності **9**
1.2. Сучасний ландшафт загроз і ключові тенденції **11**
1.3. Мережева й сервісна модель («кіберзлочинність як послуга») **13**
1.4. Транснаціональність, фінансова інфраструктура та конвергенція з традиційною організованою злочинністю **16**
1.5. Атрибуція, стратегічне оцінювання та особливості для України **22**

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ТА МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ **30**

2.1. Конституційні засади та система нормативно-правових актів **30**
2.2. Міжнародні та європейські стандарти **30**
2.3. Національне законодавство України **34**
2.4. Особливості правового регулювання в умовах воєнного стану **37**

РОЗДІЛ 3. OSINT ТА ЦИФРОВА КРИМІНАЛІСТИКА В ДІЯЛЬНОСТІ ПОЛІЦІЇ **39**

3.1. Інформаційно-аналітична модель роботи (Intelligence-Led Policing) **39**
3.2. Класифікація відкритих джерел і критична оцінка інформації **41**
3.3. Інструментарій OSINT **42**
3.4. Цифрова криміналістика та її взаємодія з OSINT **46**
3.5. OSINT у документуванні воєнних злочинів **50**

РОЗДІЛ 4. ШТУЧНИЙ ІНТЕЛЕКТ І ПРЕДИКТИВНА АНАЛІТИКА **53**

4.1. Базові технології штучного інтелекту в правоохоронній діяльності **53**
4.2. Аналітичні платформи та технології великих даних **54**
4.3. Предиктивна аналітика: моделі, застосування та інструментарій **58**
4.4. Правові й етичні межі застосування штучного інтелекту **60**

РОЗДІЛ 5. ЦИФРОВІ СЛІДИ: ВИЯВЛЕННЯ, ЗБІР, АНАЛІЗ І ПРОЦЕСУАЛЬНЕ ЗАКРІПЛЕННЯ **65**

5.1. Поняття цифрового сліду і цифрового доказу **65**
5.2. Класифікація слідів і принцип волатильності **66**
5.3. Міжнародні стандарти та принципи роботи з цифровими доказами **71**
ВИСНОВКИ **73**
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **74**

ПЕРЕДМОВА

Цифрова трансформація суспільних відносин зумовила не лише зміну способів життєдіяльності та професійної взаємодії, а й якісну трансформацію способів учинення кримінальних правопорушень. Сьогодні кримінальні угруповання діють у кіберпросторі так само організовано, як колись у фізичному просторі – із розподілом ролей, власною «економікою», інфраструктурою та ринком послуг. Особливої гостроти ця проблема набула для України в умовах воєнного стану, коли кіберпростір став середовищем не лише корисливої злочинності, а й ворожих операцій проти держави, критичної інфраструктури та громадян.

Протидіяти таким загрозам звичними методами вже недостатньо. Сучасний працівник поліції має вміти працювати з цифровими слідами, шукати й перевіряти інформацію у відкритих джерелах, розуміти можливості штучного інтелекту та аналітичних платформ – і водночас чітко усвідомлювати правові й етичні межі застосування цих інструментів.

Актуальність теми зумовлена якісною трансформацією організованої злочинності під впливом цифрових технологій, поширенням моделі «кіберзлочинність як послуга», транснаціональним розподілом інфраструктури, учасників і фінансових потоків, а також потребою адаптації національної правоохоронної практики до європейських стандартів у межах євроінтеграційного курсу України. Окремі аспекти цієї проблематики висвітлено в працях О. Є. Користіна, С. В. Демедюка, Д. В. Ланде, К. Ю. Ісмайлова, О. В. Манжая, О. О. Торбаса, М. І. Пашковського, Г. І. Піщенко, Ю. О. Шопіної та інших дослідників [7; 26; 28; 29; 57; 113; 114]. Водночас комплексного осмислення інноваційних методик протидії саме організованим формам кіберзлочинності, яке поєднувало б кримінологічний, нормативно-правовий, інформаційно-аналітичний і процесуальний виміри, у вітчизняній науці висвітлено недостатньо.

Мета наукового нарису полягає в науковому обґрунтуванні та систематизації інноваційних методик і сучасних практик діяльності поліції у сфері протидії організованій кіберзлочинності з урахуванням міжнародного досвіду та умов правового режиму воєнного стану. Об’єктом дослідження є суспільні відносини, що виникають у процесі протидії організованій кіберзлочинності, предметом – інноваційні методики, інформаційно-аналітичні технології та процесуальні механізми діяльності Національної поліції України в цій сфері.

Методологічну основу дослідження становлять загальнонаукові та спеціальні методи пізнання:

- діалектичний – для розкриття закономірностей розвитку організованої кіберзлочинності;

- системно-структурний і функціональний – для аналізу мережевої та сервісної моделей злочинної діяльності;

- формально-юридичний і порівняльно-правовий – для дослідження національних, міжнародних і європейських нормативно-правових актів;

- якісний аналіз документів і порівняння кейсів – для узагальнення аналітичних звітів Європолу, ENISA, UNODC, FATF та офіційних повідомлень про міжнародні правоохоронні операції;

- моделювання – для побудови схем життєвого циклу кіберзлочинної операції, рівнів атрибуції та алгоритмів роботи з цифровими слідами.

Емпіричну базу дослідження становлять

- відкриті аналітичні звіти Європолу (IOCTA 2026), ENISA (Threat Landscape 2025, версія 1.3), UNODC і FATF за 2024–2026 рр.;

- офіційні повідомлення Європолу та Євроюсту про правоохоронні операції 2025–2026 рр.

До табл. 1.4.1 відібрано операції, щодо яких є офіційне повідомлення правоохоронної інституції з описом об'єкта втручання та зафіксованого результату. Одиницею аналізу є окрема операція або її окрема фаза, а не звіт загалом. Для зіставлення операцій використано відкриті офіційні повідомлення, на які є посилання в табл. 1.4.1. Кейси порівняно за функцією ураженого вузла, зафіксованим результатом втручання та межами його інтерпретації. Відкриті повідомлення нерівномірні за повнотою і переважно відображають безпосередні результати операцій. Тому кейси ілюструють можливі способи впливу на мережу, а їхній довгостроковий ефект потребує окремого оцінювання.

Наукова новизна нарису полягає в обґрунтуванні інтегрованої моделі протидії організованій кіберзлочинності, яка поєднує карту мережі (ролі, ресурси, залежності та юрисдикції), перевірку версій (альтернативні пояснення, походження й незалежність джерел) і процесуальну оцінку даних (законний спосіб отримання та фіксації, процесуальне джерело, можливість перевірки). На відміну від моделі Intelligence-Led Policing (підрозділ 3.1), яка визначає роль аналітики в плануванні правоохоронної діяльності загалом, запропонована модель конкретизує етапи, відповідальних і умови переходу між етапами саме для проваджень щодо організованих кіберзлочинних мереж. На відміну від Протоколу Берклі (підрозділ 3.5), зосередженого на стандартах роботи з відкритими цифровими даними, вона охоплює також закриті дані, транскордонні механізми їх отримання та рішення щодо втручання. Авторськими є також систематизація аналітичних рівнів атрибуції з переліком альтернативних пояснень, вимірів стратегічного оцінювання кіберзлочинної загрози та розмежування орієнтуючого й доказового значення результатів OSINT, цифрової криміналістики та систем штучного інтелекту. Видання ґрунтується на результатах попередніх досліджень авторів [1; 4; 5; 6; 19; 20; 21; 22; 23; 24; 25; 27; 56; 58].

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Офіс Генпрокурора	Офіс Генерального прокурора
ДСР	Департамент стратегічних розслідувань Національної поліції України
ДСТУ	Державний стандарт України
ЄРДР	Єдиний реєстр досудових розслідувань
ЄС	Європейський Союз
ІПНП	Інформаційний портал Національної поліції України
КМУ	Кабінет Міністрів України
КПК	Кримінальний процесуальний кодекс України
МВС	Міністерство внутрішніх справ України
НПА	Нормативно-правовий акт
НПУ	Національна поліція України
НСРД	Негласні слідчі (розшукові) дії
ОРД	Оперативно-розшукова діяльність
ШІ	Штучний інтелект
C2	Командно-контрольний сервер (Command-and-Control)
CaaS	Кіберзлочинність як послуга (Cybercrime-as-a-Service)
DDoS	Розподілена атака на відмову в обслуговуванні (Distributed Denial of Service)
DL	Глибинне навчання (Deep Learning)
EDR	Системи виявлення та реагування на кінцевих точках (Endpoint Detection and Response)

ENISA	Агентство Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity)
Europol	Агентство Європейського Союзу з питань співробітництва у сфері правоохоронної діяльності (European Union Agency for Law Enforcement Cooperation).
FATF	Група з розробки фінансових заходів боротьби з відмиванням коштів (Financial Action Task Force)
ILP	Поліцейська діяльність на основі аналітики (Intelligence-Led Policing)
INTERPOL	Міжнародна організація кримінальної поліції (International Criminal Police Organization)
IOCTA	Оцінка загроз організованої злочинності в інтернеті (Internet Organised Crime Threat Assessment)
ISO/IEC	Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія
ML	Машинне навчання (Machine Learning)
NIS 2	Директива ЄС щодо високого спільного рівня кібербезпеки
NLP	Обробка природної мови (Natural Language Processing)
OSINT	Розвідка на основі відкритих джерел (Open Source Intelligence)
TTPs	Тактики, техніки та процедури (Tactics, Techniques and Procedures)
UNODC	Управління ООН з наркотиків і злочинності (United Nations Office on Drugs and Crime)
VPN	Віртуальна приватна мережа (Virtual Private Network)

РОЗДІЛ 1.
ОРГАНІЗОВАНА КІБЕРЗЛОЧИННІСТЬ: СУЧАСНИЙ СТАН, ТЕНДЕНЦІЇ ТА СПЕЦИФІКА

1.1. Поняття організованої кіберзлочинності

Цифровізація державного управління, економіки, фінансових послуг і повсякденного життя зумовила не лише зміну форм суспільної взаємодії, а й трансформацію структури самої злочинності. Інформаційно-комунікаційні технології створили середовище, у якому злочин можна підготувати, скоординувати й учинити дистанційно, а його наслідки – одночасно проявити в кількох державах. За таких умов кіберзлочинність уже не можна розглядати лише як окремі технічно складні напади на комп'ютерні системи. Її найнебезпечніший сегмент утворюють стійкі кримінальні мережі, що поєднують спеціалізовані знання, цифрову інфраструктуру, фінансові ресурси, анонімні комунікації та розподілену систему виконавців. Саме ця сукупність властивостей дозволяє розглядати організовану кіберзлочинність як особливу форму сучасної організованої злочинності: вона існує переважно у цифровому середовищі, але породжує цілком реальні майнові, економічні, безпекові й соціальні наслідки [29; 114].

Законодавче визначення кіберзлочину. Закон України «Про основні засади забезпечення кібербезпеки України» визначає кіберзлочин 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 [52]. Зверніть увагу: сам факт використання інформаційних технологій ще не робить злочин «організованим». Для цього потрібні додаткові ознаки, про які йдеться далі.

Системоутворювальними ознаками, що трансформують сукупність окремих кіберзлочинів в організовану злочинну діяльність, є стійкість взаємодії, координація дій, функціональний розподіл ролей, спільність кримінальної мети, повторюваність операцій, наявність ресурсної або сервісної бази, а часто – спеціально створеної чи пристосованої цифрової інфраструктури [27; 29].

Повторюваність операцій, спільна інфраструктура та сталі зв'язки між виконавцями дають підстави перевірити версію про організований характер діяльності. Для кримінально-правової оцінки окремо встановлюють ознаки відповідної форми співучасті, передбачені частиною третьою або частиною четвертою статті 28 КК України [17].

Принципово важливо, що цифрова взаємодія дозволяє підтримувати організованість *без постійної фізичної присутності* учасників в одному місці. Тому

традиційні «просторові» критерії (спільні зустрічі, територія дії) для оцінки такої діяльності виявляються недостатніми.

У кримінологічному вимірі організовану кіберзлочинність доцільно розуміти не як окремий перелік складів злочинів, а як *спосіб організації* кримінальної діяльності у цифровому середовищі. Вона охоплює дві великі групи посягань.

Таблиця 1.1.1. Кіберзалежні та кіберпідсилені злочини

Ознака	*Кіберзалежні злочини*	*Кіберпідсилені злочини*
Сутність	існування без комп'ютерних систем фактично неможливе	традиційні посягання, масштаб яких посилюють цифрові технології
Типові приклади	несанкціоноване втручання в роботу систем, створення й поширення шкідливого програмного забезпечення, DDoS-атаки	шахрайство, вимагання, легалізація (відмивання) доходів, незаконний обіг даних
Роль технології	технологія є самою суттю злочину	технологія є засобом масштабування та приховування

Цей поділ (таблиця 1.1.1.) важливий тому, що сучасні організовані мережі дедалі частіше поєднують *обидва* сегменти: технічне проникнення або компрометація облікових даних стають лише першою ланкою подальшого шахрайства, вимагання, викрадення інформації чи відмивання коштів.

Наукові дослідження послідовно вказують на високу латентність, професіоналізацію, транснаціональність і тісний зв'язок кіберзлочинності з організованими формами злочинності [27; 29; 57]. Сучасний етап відрізняється тим, що ці ознаки вже не існують окремо: технології забезпечують масштабованість, а розподіл ролей і спеціалізовані сервіси – організаційну стійкість. У цьому сенсі організована кіберзлочинність дедалі більше нагадує *нелегальний ринок*, де доступ до технічних ресурсів, викрадених даних, серверів, засобів анонімізації та фінансових послуг купується окремо, а кінцевий злочинний результат «збирається» з кількох незалежних сервісів.

Ця модель суттєво відрізняється від звичного уявлення про організовану групу як 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 справжніх даних співучасників, але

системно виконувати визначену функцію, отримувати винагороду й усвідомлювати кримінальний характер спільної діяльності.

Водночас надання технічної чи іншої послуги учасникам кіберзлочинного середовища саме по собі не встановлює обізнаності постачальника, спільного умислу чи його участі у відповідній формі співучасті. Ці ознаки підлягають самостійному встановленню на підставі сукупності доказів щодо змісту взаємодії, усвідомлення її кримінального характеру та узгодженості дій [17].

1.2. Сучасний ландшафт загроз і ключові тенденції

Поточний стан кіберзлочинності визначається не стільки появою принципово нових видів посягань, скільки *безперервною модифікацією* способів їх реалізації, масштабуванням уже відомих моделей і швидкою адаптацією злочинців до нових технологій захисту. Аналітичні матеріали європейських інституцій свідчать про збереження високої інтенсивності атак на доступність сервісів, значний вплив програм-вимагачів, поширеність фішингу, експлуатації вразливостей і викрадення облікових даних [79; 90]. Наступний випуск – ENISA Threat Landscape 2026 – ґрунтується на 8257 інцидентах, зареєстрованих з 01.01.2025 по 31.12.2025 [80]; показники двох випусків стосуються різних періодів і наводяться з їх зазначенням.

ПРАКТИЧНИЙ КЕЙС: Threat Landscape 2025

Агентство Європейського Союзу з кібербезпеки (ENISA) у щорічному звіті Threat Landscape 2025 проаналізувало 4875 інцидентів за період з 01.07.2024 по 30.06.2025. За результатами аналізу:

- DDoS-атаки становили 77 % зафіксованих інцидентів;

- програми-вимагачі (ransomware) визначено найвпливовішою загрозою;

- фішинг та експлуатація вразливостей – провідними шляхами первинного проникнення.

Ці показники не тотожні структурі організованої кіберзлочинності, але описують середовище, у якому організовані актори формують і масштабують свої операції.

Джерело: ENISA. ENISA Threat Landscape 2025.

Високу частку DDoS-активності потрібно інтерпретувати обережно. Значна частина таких атак має хактивістський або ідеологічно мотивований характер і не завжди пов’язана з класичною корисливою організованою злочинністю. Водночас організаційні моделі, що забезпечують масове залучення користувачів, використання бот-мереж, оренду потужностей і проксі-інфраструктуру, демонструють важливу закономірність: кібероперація може бути технічно централізованою, але організаційно розподіленою. Для правоохоронної оцінки це означає необхідність відокремлювати *мотив* (навіщо) від *способу організації* (як) і

встановлювати, чи існує стійке ядро, яке координує учасників і підтримує інфраструктуру.

Програми-вимагачі залишаються показовою формою організованої кіберзлочинності, бо поєднують одразу кілька елементів:

- технічне проникнення, викрадення даних;
- порушення доступності систем;
- психологічний тиск і фінансове вимагання.

Сучасні операції дедалі частіше будуються на *багатоступеневому вимаганні*: злочинці не лише шифрують інформацію, а й погрожують оприлюднити її, звернутися до клієнтів чи партнерів потерпілої організації, скористатися репутаційними та регуляторними ризиками.

ENISA фіксує розвиток агресивних тактик тиску, повторне використання конструкторів програм-вимагачів і поширення засобів, спрямованих на обхід систем виявлення та реагування на кінцевих точках (Endpoint Detection and Response, EDR) [79]. Програма-вимагач є технічним засобом. Операція з її використанням може охоплювати викрадення даних, шифрування та подальший тиск на потерпілих. У моделі ransomware-as-a-service окремі функції розподіляються між оператором сервісу та його партнерами.

Паралельно зберігає значення масове викрадення облікових даних. Екосистема програм-викрадачів даних формує ресурсну базу для подальших атак: викрадені логіни, файли cookie, токени сесій і дані браузера використовуються самими виконавцями або продаються іншим учасникам ринку. Звідси – ще одна важлива властивість: один епізод компрометації здатний породжувати кілька наступних кримінальних сценаріїв. Первинна крадіжка даних, несанкціонований доступ, шахрайство, вимагання й відмивання коштів можуть бути розподіленими в часі та виконуватися різними суб'єктами, але залишатися ланками одного ланцюга [90].

Фішинг і соціальна інженерія також пройшли шлях від примітивних масових розсилок до індустріалізованих сервісів.

ПРАКТИЧНИЙ КЕЙС: Tycoon 2FA – «фішинг як послуга»

У березні 2026 року міжнародна операція за підтримки Європолу порушила роботу платформи Tycoon 2FA – сервісу «фішинг як послуга» (phishing-as-a-service), який надавав підписникам готовий інструментарій для перехоплення активних сесій автентифікації й обходу багатофакторного захисту. Кейс демонструє: злочинний ринок пропонує вже не просто шаблон фішингової сторінки, а технологічно завершений сервіс, доступний навіть користувачам із низькою технічною підготовкою.

Джерело: Europol. Global Phishing-as-a-Service Platform Taken Down… 2026.

Загальна картина сучасної кіберзлочинності визначається не однією домінуючою технологією, а *взаємодією* кількох сегментів: викрадення доступів,

експлуатація вразливостей, malware-інфраструктура, соціальна інженерія, фінансове шахрайство, сервіси анонімізації та механізми відмивання цифрових активів. Саме взаємозалежність цих сегментів робить організовану кіберзлочинність стійкою.

Окремо слід сказати про роль автоматизації та штучного інтелекту. Скрипти, боти, автоматизовані системи перевірки облікових даних і масове сканування вразливостей дозволяють одній групі одночасно працювати з великою кількістю цілей.

UNODC підкреслює, що автоматизація стала важливим чинником переходу кіберзлочинності від ізольованих дій до масштабних операцій, а інтеграція штучного інтелекту додатково підвищує їх швидкість і адаптивність [124]. При цьому штучний інтелект доцільно розглядати передусім як *мультиплікатор* уже відомих загроз: генеративні моделі полегшують створення переконливих фішингових повідомлень різними мовами, персоналізацію соціальної інженерії та створення синтетичного аудіо- й відеоконтенту. Європол в IOCTA 2026 прямо пов'язує сучасну еволюцію кіберзлочинності з поєднанням шифрування, проксі-сервісів і штучного інтелекту (encryption, proxies and AI): ШІ підвищує масштаб і правдоподібність атак, проксі ускладнюють ідентифікацію джерела, а шифрування захищає комунікацію злочинців [90].

1.3. Мережева й сервісна модель («кіберзлочинність як послуга»)

Однією з найстійкіших тенденцій є перехід від жорстко ієрархічних структур до *мережевих і модульних* моделей. У такій системі організатор не обов'язково керує кожним виконавцем безпосередньо, а окремі учасники вступають 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 та особи, які забезпечують виведення коштів, можуть діяти автономно – але їхні послуги інтегруються в єдиний механізм одержання незаконного доходу. Через це традиційне встановлення «організаційної структури» ускладнюється: межі між учасником групи, постачальником послуги та клієнтом злочинного сервісу стають рухомими.

Мережева модель має ще одну важливу властивість – вона зменшує залежність злочинної діяльності від окремої особи чи технічного ресурсу:

- якщо один виконавець вибуває, його функцію передають іншому;
- якщо сервер вилучено, інфраструктуру розгортають на новій платформі;
- якщо домен заблоковано, використовують інші доменні імена, IP-адреси чи канали.

Це явище називають **оперативною регенерацією**: мережа відновлюється під новою назвою, з частково зміненим складом, але з тими самими контактами, навичками, фінансовими каналами й клієнтською базою.

Функціональна спеціалізація закономірно породжує модель **«кіберзлочинність як послуга»** (Cybercrime-as-a-Service, CaaS), у якій окремі елементи операції купуються або орендуються як самостійний продукт. Європол в 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 для уникнення виявлення [89; 90]. Такий ринок дозволяє *відокремити технічну компетентність від кримінальної ініціативи*: той, хто планує шахрайство чи вимагання, може взагалі не вміти писати шкідливий код – потрібні компоненти доступні як сервіс.

Таблиця 1.3.1. Типові ролі (сервіси) у моделі «кіберзлочинність як послуга»

Роль / сервіс	*Що робить учасник*	*Кримінальний «продукт»*
Розробник шкідливого ПЗ	створює й супроводжує malware	готовий інструмент атаки
Брокер первинного доступу	отримує доступ до систем і перепродає його	доступ до зламаної мережі
Оператор програми-вимагача	розгортає атаку, веде «перемовини»	шифрування/вимагання
Адміністратор інфраструктури	утримує сервери, домени, проксі	операційна життєздатність мережі
Фахівець із соціальної інженерії	створює фішинг, веде «легенду»	компрометація людини
Продавець викрадених даних	агрегує й реалізує масиви даних	бази даних, акаунти, реквізити
Посередник із виведення коштів	«відмиває» й переміщує дохід	легалізовані кошти

Сервісна модель має чотири принципові наслідки:

1) По-перше, вона *знижує бар'єр входження* до кіберзлочинності.

2) По-друге, створює *конкуренцію* між постачальниками незаконних послуг, що підвищує їхню технічну якість і «зручність».

3) По-третє, забезпечує *масштабування*: один постачальник інфраструктури може одночасно обслуговувати безліч незалежних кампаній.

4) По-четверте, *ускладнює доказування* спільного умислу й ролі конкретного суб'єкта, особливо коли взаємодія відбувається через псевдоніми, автоматизовані платформи та короткочасні контакти.

Особливе місце в цій структурі посідають **брокери первинного доступу** – посередники, які спеціалізуються на отриманні доступу до інформаційних систем і його продажу. Їхня діяльність показує, що кримінальний продукт може існувати ще до того, як визначено кінцевий вид атаки: скомпрометований доступ до мережі однієї організації може купити і група операторів ransomware, і шахрайська мережа. Для практики це означає, що розслідування фінального інциденту має охоплювати й попередні ланки: спосіб компрометації, канал продажу, зв'язки продавця з іншими клієнтами та повторюваність інфраструктури. Схожу «забезпечувальну» роль виконують абузостійкий (bulletproof) хостинг, проксі- та VPN-інфраструктури, сервіси масової реєстрації доменів і орендовані сервери – вони не завжди вчиняють атаку безпосередньо, але підтримують життєздатність багатьох злочинних клієнтів одночасно. Саме тому нейтралізація такого допоміжного вузла може дати значно ширший ефект, ніж припинення одного епізоду [89; 91].

Стійкість мереж значною мірою забезпечує **децентралізація інфраструктури**: командно-контрольні (C2) сервери, резервні домени, файлові сховища, облікові записи й криптовалютні адреси розподіляються між різними постачальниками та юрисдикціями. Через це навіть успішне вилучення одного сервера не гарантує припинення операції.

ПРАКТИЧНИЙ КЕЙС: Operation Endgame (2025)

Саме тому сучасні міжнародні операції спрямовують не на один об'єкт, а на одночасне порушення багатьох складових інфраструктури. Упродовж 19-22 травня 2025 року в межах операції Endgame правоохоронці вилучили криптовалюту на суму 3,5 млн євро, припинили роботу близько 300 серверів і нейтралізували 650 доменів. За даними Європолу, станом на 23 травня 2025 року загальна вартість криптовалюти, вилученої від початку операції, перевищила 21,2 млн євро.

Джерело: Europol. Operation ENDGAME Strikes Again… 2025.

Після масштабного втручання мережі часто вдаються до **ребрендингу** – змінюють назву, бренд, комунікаційні канали чи склад учасників. Це не «маркетинг», а спосіб зберегти людський капітал, довіру й клієнтські зв'язки у підпільному середовищі. Тому виявлення наступності між формально різними групами потребує аналізу повторюваних технічних рішень, мовних і поведінкових ознак, інфраструктурних зв'язків, фінансових адрес і контактів – інакше оцінка ризику штучно «обнуляється» щоразу, коли зникає стара назва.

Щоб бачити картину цілісно, організовану кіберзлочинність доцільно розглядати як **життєвий цикл** кримінальної операції. На кожному етапі можуть діяти різні особи й використовуватися різні сервіси, тому одна операція фактично поєднує кілька «мікроринків» незаконних послуг – і припинення одного епізоду не обов'язково руйнує всю структуру.

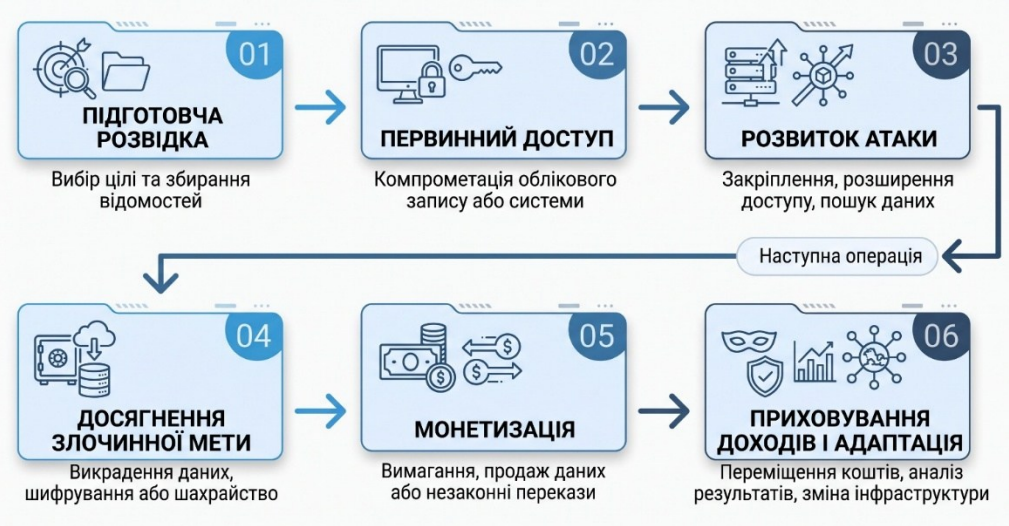

Рис. 1.3.1. Життєвий цикл кіберзлочинної операції

Примітка. *Схема відображає узагальнену модель: у конкретній операції окремі етапи можуть поєднуватися, бути відсутніми або виконуватися різними учасниками.*

Завершення операції може підвищувати організаційну спроможність мережі та створювати ресурси для наступного епізоду. Саме здатність до навчання відрізняє стійке кримінальне підприємство від випадкового правопорушення – накопичений досвід, репутація й технічні напрацювання стають ресурсом для наступних атак.

Окремий системний сегмент – **ринок викрадених даних і цифрових ідентичностей**. Облікові записи, бази клієнтів, платіжні реквізити, файли cookie, токени автентифікації та персональні документи мають самостійну товарну вартість незалежно від того, як їх здобули. Наслідки витоку не завершуються моментом компрометації: дані перепродаються, агрегуються, доповнюються інформацією з інших джерел і роками використовуються в нових шахрайських чи соціально-інженерних сценаріях. Компрометація одного акаунта може відкривати доступ до інших сервісів через повторне використання паролів, федеративну автентифікацію (federated login) або збережені сесії – тобто створювати *каскадний ефект* і кілька хвиль вторинної віктимізації однієї потерпілої особи [5].

1.4. Транснаціональність, фінансова інфраструктура та конвергенція з традиційною організованою злочинністю

Транснаціональність є поширеною характеристикою організованої кіберзлочинності, зумовленою можливістю розподілу учасників, цифрової інфраструктури, потерпілих і фінансових операцій між різними державами. Організатор може перебувати в одній державі, виконавець – в іншій, серверна

інфраструктура – у третій, потерпілий – у четвертій, а переміщення злочинних доходів здійснюватися через сервіси ще кількох юрисдикцій. Унаслідок цього відомості про правопорушення та його цифрові сліди розподіляються між різними правовими й технологічними середовищами, що ускладнює встановлення обставин події та її документування. Водночас транснаціональність не є обов'язковою ознакою кожної організованої кіберзлочинної операції: окремі мережі можуть діяти переважно в межах однієї держави [15; 126].

Умовний розподіл складових кіберзлочинної операції між різними юрисдикціями наведено на схемі 1.4.1.

Для злочинних мереж юрисдикційна фрагментація може створювати додаткові можливості приховування діяльності. Відмінності в законодавстві, строках зберігання даних, процедурах доступу до інформації та швидкості міжнародного співробітництва ускладнюють своєчасне отримання відомостей. Встановлення IP-адреси або місця розміщення сервера саме по собі не гарантує доступу до необхідних даних, особливо якщо вони зберігаються в іноземного постачальника послуг і можуть бути видалені до надходження належного запиту. Тому істотне значення мають своєчасне збереження цифрових слідів, визначення місць зберігання даних та координація дій компетентних органів.



Рис. 1.4.1. Умовна модель транснаціонального розподілу складових кіберзлочинної операції

Примітка. Позначення держав є умовними. Окремі складові можуть перебувати в одній юрисдикції. Схема відображає можливі функціональні зв'язки, а не обов'язкову послідовність дій.

Розподілений характер діяльності потребує аналізу не лише територіального розміщення учасників, а й зв'язків між ними, інфраструктурних залежностей та функціональних ролей. Учасники можуть не зустрічатися особисто й знати одне одного лише за псевдонімами. Їхню взаємодію можуть підтримувати репутація на нелегальних майданчиках, повторювані угоди, спільне використання цифрових ресурсів та економічна взаємозалежність. Проте користування одним сервісом або участь в одному онлайн-середовищі самі по собі не доводять належності осіб до спільної злочинної групи.

Для корисливо орієнтованих мереж економічний компонент має системоутворювальне значення. Підготовка й реалізація операцій потребують серверної інфраструктури, доменних імен, програмного забезпечення, засобів приховування мережевих з'єднань, доступу до скомпрометованих систем та оплати послуг виконавців. Важливими складовими діяльності є отримання й розподіл злочинних доходів, їх переміщення, приховування походження та, в окремих випадках, легалізація. Для мереж із переважно ідеологічною або політичною мотивацією фінансування може забезпечувати операційну діяльність без безпосереднього отримання доходу від кожної атаки.

ПРАВОВИЙ АСПЕКТ: Використання віртуальних активів

Віртуальні активи можуть використовуватися для транскордонного переміщення вартості, зокрема в межах злочинних операцій. Однак саме їх використання не свідчить про злочинний характер діяльності. Застосування інструментів конфіденційності також не є достатньою підставою для висновку про причетність особи до кримінального правопорушення.

У багатьох публічних блокчейнах історія транзакцій доступна для аналізу, що дає змогу досліджувати переміщення активів між адресами. Водночас простеження транзакцій необхідно відрізняти від встановлення особи: блокчейн-адреса сама по собі не розкриває, хто її контролював у конкретний період. Для такого висновку потрібні додаткові відомості, зокрема дані постачальників послуг, результати дослідження пристроїв і комунікацій.

Аналіз може ускладнюватися використанням міжмережевих операцій, сервісів змішування транзакцій, численних проміжних адрес та рахунків фінансових посередників – так званих «грошових мулів» (*money mules*). Оцінювання підозрілої діяльності має враховувати походження активів, структуру й часові параметри транзакцій, зв'язки між учасниками та альтернативні пояснення виявлених ознак. Аналітичні індикатори ризику не слід автоматично прирівнювати до доказів вини.

FATF у цільовому оновленні 2025 року наголосила на необхідності посилення реалізації заходів протидії відмиванню коштів і фінансуванню тероризму у сфері віртуальних активів [94]. У наступному оновленні, оприлюдненому в липні 2026 року, організація продовжила оцінювання прогресу та прогалин у виконанні відповідних стандартів [93].

ПРАКТИЧНИЙ КЕЙС: Сервіс AudiA6

Спеціалізацію фінансових послуг у кіберзлочинному середовищі ілюструє діяльність сервісу AudiA6. За повідомленням Євроюсту від 11 червня 2026 року, міжнародне розслідування, підтримане Євроюстом та Європолом, призвело до припинення роботи вебсайту, через який, за версією слідства, у 2022-2025 роках могло бути відмито понад 336 млн євро у криптовалюті. Сервіс використовували учасники кіберзлочинних операцій, зокрема пов'язаних із програмами-вимагачами, для виведення цифрових активів і приховування руху злочинних доходів. Під час розслідування виявлено понад 6000 записів ідентифікації клієнтів – KYC (Know Your Customer), пов'язаних із рахунками фінансових посередників.

Цей кейс ілюструє можливість існування спеціалізованого фінансового сервісу, який обслуговує різних учасників злочинного середовища. Встановлення способів переміщення активів, рахунків посередників і зв'язків між користувачами такого сервісу може мати значення для аналізу кількох розслідувань. Водночас відомості про ймовірний обсяг відмивання необхідно подавати як позицію слідства, а не як встановлений судом факт.

Для кримінального аналітика фінансові потоки є джерелом відомостей про взаємодію учасників, розподіл доходів і способи забезпечення діяльності. Навіть за зміни окремих адрес і рахунків повторювані механізми переміщення коштів, використання тих самих посередників або сервісів можуть допомагати встановлювати зв'язки між епізодами. Такі висновки потребують зіставлення фінансових даних із комунікаційними, технічними та часовими характеристиками операцій.

Ще однією тенденцією є конвергенція – зближення та взаємопроникнення кіберзлочинності й інших форм організованої злочинної діяльності. Цифрові технології використовуються не лише для атак на інформаційні системи, а й для організації шахрайства, незаконного обігу товарів, експлуатації людей, переміщення доходів та координації учасників. У звіті UNODC *Inflection Point* розглядається взаємозв'язок шахрайських центрів, підпільних фінансових механізмів та незаконних онлайн-майданчиків у Південно-Східній Азії, а також міжнародні наслідки розвитку таких мереж [125; 126].

Конвергенція відбувається у двох напрямах. З одного боку, мережі, які здійснюють традиційні види злочинної діяльності, використовують викрадені ідентифікаційні дані, скомпрометовані облікові записи та цифрові сервіси. З іншого

боку, кіберзлочинні мережі можуть залучати фінансових посередників, фізичну логістику, підроблені документи та інші ресурси поза цифровим середовищем. Тому аналіз таких мереж має охоплювати взаємодію цифрових і фізичних ресурсів, не припускаючи, що кожна операція обов'язково завершується переведенням доходу в готівку або матеріальні активи.

Таблиця 1.4.1. Приклади міжнародних операцій проти кіберзлочинних мереж та їхньої інфраструктури

Операція або об'єкт втручання	*Об'єкт впливу*	*Основний результат та аналітичне значення*	*Межі висновку*
Operation Endgame, травень 2025 року	Шкідливе програмне забезпечення та інфраструктура забезпечення початкового доступу	Фаза 19–22 травня 2025 року: виведено з експлуатації близько 300 серверів, нейтралізовано 650 доменів і вилучено криптовалюту вартістю 3,5 млн євро. Накопичений результат операції станом на 23.05.2025: загальна вартість вилученої від початку операції криптовалюти перевищила 21,2 млн євро	Повідомлення фіксує безпосередні результати; тривалість порушення роботи шкідливого ПЗ і перехід учасників на інші сервіси в ньому не оцінюються
Втручання проти Tycoon 2FA, 2026 рік	Інфраструктура платформи «фішинг як послуга»	Припинено роботу 330 доменів, які забезпечували функціонування фішингових сторінок і панелей керування. Кейс ілюструє вплив на сервіс забезпечення компрометації облікових записів	З повідомлення не встановлюється, як довго сервіс не працював, чи перейшли користувачі на інші платформи та якою є доведена роль кожного учасника
Припинення роботи	Сервіс, підозрюваний у	За версією слідства, у 2022-2025 роках через	Обсяг відмивання – позиція слідства,

AudiA6, 2026 рік	відмиванні криптовалютних доходів	сервіс могло бути відмито понад 336 млн євро. Кейс ілюструє значення фінансових посередників для кіберзлочинних операцій	а не встановлений судом факт
Operation Eastwood, липень 2025 року	Мережа NoName057(16) та інфраструктура DDoS-атак	Порушено роботу понад 100 серверів і значної частини центральної інфраструктури. Кейс ілюструє значення каналів координації, адміністрування та масового залучення учасників	Зафіксовано порушення роботи інфраструктури; відновлення активності мережі після операції потребує окремого оцінювання
Дії проти шахрайських кол-центрів в Україні, грудень 2025 року	Мережа кол-центрів у Дніпрі, Івано-Франківську та Києві, що вчиняла шахрайство щодо потерпілих у державах ЄС, зокрема з використанням програм віддаленого доступу до банківських рахунків	9 грудня 2025 року Офіс Генерального прокурора та Національна поліція України в межах спільної слідчої групи, створеної за підтримки Євроюсту, провели 72 обшуки й затримали 12 осіб. За даними слідства, встановлено понад 400 потерпілих, а збитки перевищують 10 млн євро. Кейс ілюструє роль українських органів як виконавців процесуальних дій у транскордонному розслідуванні	Кількість потерпілих і розмір збитків – оцінка слідства; повідомлення про підозру та затримання не встановлюють вини осіб

Джерело: узагальнено авторами за офіційними повідомленнями Євроюсту та Європолу [81; 82; 87; 88; 91; 92].

1.5. Атрибуція, стратегічне оцінювання та особливості для України

Виявлення організованої кіберзлочинної діяльності ускладнюється латентністю окремих епізодів. Потерпілі можуть тривалий час не помічати компрометації, не повідомляти про інцидент через репутаційні ризики або не усвідомлювати, що окремі події є частиною ширшої кампанії. Цифрові сліди можуть зберігатися в інформаційних системах різних суб'єктів, обмін даними між якими є обмеженим або несвоєчасним.

У таких умовах орган, який розслідує окремий епізод, може отримувати лише частину відомостей про мережу. Водночас і самі учасники не обов'язково знають усю її структуру: розподіл ролей та обмеження доступу до інформації можуть застосовуватися для приховування організаторів. Зменшення інформаційної фрагментації потребує зіставлення даних із різних джерел, міжнародної координації та належного збереження цифрових слідів. Міжвідомча й державно-приватна взаємодія має здійснюватися з дотриманням установлених правових підстав доступу до інформації та вимог її захисту.

Окремою проблемою є атрибуція – обґрунтоване встановлення зв'язку між спостережуваною кібердіяльністю, використаними ресурсами, певною мережею та конкретними особами. IP-адреса, доменне ім'я, блокчейн-адреса або ім'я користувача можуть бути важливими орієнтирами для аналізу, але їх не можна автоматично ототожнювати з конкретною фізичною особою. Інфраструктура може бути орендованою, скомпрометованою або спільною для багатьох користувачів; програмний код – повторно використаним; обліковий запис – переданим іншій особі або захопленим без відома власника [19].

Доцільно розрізняти чотири аналітичні рівні атрибуції: *технічний, інфраструктурний, організаційний і персональний.* Вони можуть досліджуватися паралельно й не утворюють обов'язкової послідовності.

Таблиця 1.5.1. Аналітичні рівні атрибуції

Рівень	*Що встановлює*	*Приклад*	*Альтернативне пояснення / що перевірити*
Технічний	Характеристики застосованих засобів і способів дій, можливі технічні зв'язки між епізодами	Збіг конфігурації шкідливого програмного забезпечення та особливостей його застосування	Той самий інструмент могли придбати чи завантажити різні суб'єкти; перевірити унікальність конфігурації, час і спосіб застосування

Рівень	*Що встановлює*	*Приклад*	*Альтернативне пояснення / що перевірити*
Інфраструктурний	Зв’язки між доменами, серверами, сертифікатами та іншими ресурсами	Використання спільної інфраструктури командування та керування – C2 (*Command and Control*)	Спільний провайдер хостингу, DNS або інший спільний сервіс; перевірити, чи ресурс не обслуговує багатьох незалежних клієнтів
Організаційний	Обґрунтовану належність епізодів до певної мережі або спільної координації	Сукупність технічних, фінансових і комунікаційних даних указує на координацію кількох кампаній однією мережею	Паралельні кампанії різних мереж, що користуються тими самими сервісами; перевірити незалежність джерел, які вказують на координацію
Персональний	Особу учасника, її роль і конкретні дії у визначений період	Встановлення особи, яка керувала обліковим записом під час підготовки або реалізації операції	Спільний, переданий або скомпрометований обліковий запис; перевірити зв’язок особи з конкретною дією та часом (пристрій, сеанс доступу, інші незалежні дані)

Примітка. Авторська систематизація. Наведені рівні не є обов’язковими послідовними етапами.

Під час технічного аналізу використовують поняття TTPs – *tactics, techniques and procedures*, тобто тактики, техніки та процедури. Збіг TTPs може бути підставою для висунення аналітичної гіпотези, але не є самостійним підтвердженням тотожності виконавців або належності епізодів до однієї мережі.

Аналітичний висновок про ймовірний зв’язок між епізодами необхідно відрізняти від доказування участі конкретної особи у кримінальному правопорушенні. Методологічною помилкою є перехід від технічного збігу

безпосередньо до твердження про особу виконавця без перевірки проміжних зв'язків.

Сукупність узгоджених ознак може підвищувати обґрунтованість атрибуції за умови перевірки їхньої достовірності, незалежності та альтернативних пояснень. Кілька ознак, що походять від одного джерела або зумовлені використанням спільного сервісу, не слід трактувати як кілька незалежних підтверджень. Наприклад, однакові сервери імен можуть пояснюватися користуванням одним постачальником послуг, а схожий код – придбанням того самого програмного засобу різними користувачами.

В аналітичних матеріалах необхідно розмежовувати встановлені факти, припущення та відомості, які потребують додаткової перевірки. Для кожного суттєвого висновку доцільно зазначати джерела, обмеження даних і ступінь упевненості, обґрунтований наявними матеріалами.

Протидія організованій кіберзлочинності потребує не лише реагування на інциденти, а й системного формування аналітичного уявлення про структуру мереж, їхні ресурси, способи діяльності та можливі наслідки. Кількість зареєстрованих правопорушень є важливим показником, але залежить від рівня виявлення, повідомлення про події та особливостей їх кваліфікації. Тому стратегічне оцінювання має поєднувати статистичні дані з аналізом спроможностей мережі, імовірності нових епізодів і потенційної шкоди [6; 22].

Таблиця 1.5.2. Виміри стратегічного оцінювання кіберзлочинної загрози

Вимір	*Ключове питання*
Суб'єктний	Хто організовує, координує та забезпечує діяльність мережі?
Інфраструктурний	Які цифрові ресурси використовуються та від яких сервісів залежить діяльність?
Операційний	Якими є способи дій, тактики, техніки та процедури?
Фінансовий	Як фінансується діяльність, формується дохід і переміщуються активи?
Географічний	У яких юрисдикціях перебувають учасники, потерпілі, інфраструктура та дані?
Часовий	Як змінюється активність і як швидко мережа відновлюється після втручання?
Наслідки та потенційна шкода	Яких збитків і порушень функціонування можуть зазнати населення, організації або критична інфраструктура?

Вимір	*Ключове питання*
Імовірність і масштаб реалізації	Наскільки ймовірні нові епізоди та яким може бути їхнє охоплення?

Примітка. Представлена авторська систематизація напрямів аналізу. Таблиця не є стандартизованою шкалою оцінювання загрози.

Висновки за кожним із наведених вимірів мають спиратися на визначені джерела даних. Якщо застосовується бальне оцінювання, необхідно окремо встановити критерії, правила присвоєння балів і спосіб урахування невизначеності.

Міжнародні операції проти інфраструктури початкового доступу, фішингових платформ і фінансових сервісів ілюструють значення впливу на ресурси, якими користуються різні учасники злочинного середовища. Для Національної поліції України це означає доцільність виявлення вузлів, втручання щодо яких може обмежити діяльність кількох мереж або запобігти новим епізодам. Водночас припинення роботи окремого сервісу не слід автоматично ототожнювати з остаточним припиненням діяльності його користувачів: необхідно оцінювати можливість відновлення інфраструктури та переходу на альтернативні ресурси.

Організована кіберзлочинна діяльність, спрямована проти України або пов’язана з її цифровим середовищем, розвивається в умовах повномасштабної збройної агресії Російської Федерації. У кіберпросторі діють корисливо орієнтовані злочинні мережі, хактивістські об’єднання, державні та пов’язані з державами суб’єкти. Однакові способи дій – фішинг, застосування шкідливого програмного забезпечення, експлуатація вразливостей, компрометація облікових записів або DDoS-атаки і т.д. – можуть використовуватися з різною мотивацією.

У звіті *ENISA Threat Landscape 2025* описано випадки використання пов’язаними з державами суб’єктами кіберзлочинних методів та їхніх зв’язків із діяльністю програм-вимагачів [79]. Це зумовлює необхідність обережного оцінювання технічних збігів: походження програмного засобу або його попереднє використання певною групою саме по собі не визначає особу, мотивацію чи державну належність суб’єкта нового епізоду.

ПРАКТИЧНИЙ КЕЙС. Operation Eastwood проти NoName057(16)

У липні 2025 року міжнародна операція Eastwood, координована Європолом та Євроюстом, була спрямована проти проросійської кіберзлочинної мережі NoName057(16). За повідомленням Європолу, мережа здійснювала DDoS-атаки проти України та держав, які її підтримують. Унаслідок операції порушено роботу понад 100 серверів і значної частини центральної інфраструктури. Офіційне повідомлення також описує залучення прихильників через ідеологічну мотивацію, ігрові механізми та винагороди.

Для кримінального аналізу цей кейс ілюструє необхідність дослідження не лише безпосередніх учасників атак, а й адміністраторів інфраструктури, каналів координації, механізмів залучення та стимулювання участі [87]. Розмежування цих ролей допомагає визначати функціонально значущі складові мережі. Водночас встановлення конкретних дій кожної особи потребує окремої перевірки.

Воєнний контекст створює додаткові можливості для соціальної інженерії. Гуманітарні виплати, волонтерські збори, військова тематика, державні послуги та мобілізаційні процеси можуть використовуватися як приводи для фішингу й шахрайства. Під час аналізу таких епізодів доцільно зіставляти зміст повідомлень, способи поширення, платіжні реквізити, технічну інфраструктуру та часові характеристики активності. Самої схожості тематики недостатньо для висновку про спільних організаторів.

Воєнний контекст не дає підстав автоматично ототожнювати всі ворожі кібероперації з організованою кіберзлочинністю. Для аналітичного розмежування слід ураховувати склад учасників, мотивацію, механізми координації, фінансування та кінцеву мету. Правову оцінку конкретних діянь необхідно здійснювати окремо, відповідно до встановлених обставин і застосовних норм права. Так само груповий характер атаки або використання певного інструменту самі по собі не доводять державного походження операції.

Аналіз організованої кіберзлочинності потребує поєднання дослідження окремих інцидентів із реконструкцією зв’язків між учасниками, інфраструктурою та фінансовими операціями. Реактивний компонент охоплює встановлення обставин уже вчинених правопорушень, потерпілих і причетних осіб та збереження доказів. Проактивний компонент передбачає виявлення повторюваних моделей, спільних ресурсів і фінансових каналів для оцінювання загроз та запобігання новим епізодам. Кримінальний аналіз забезпечує формування обґрунтованих висновків із розрізнених відомостей за умови перевірки джерел, альтернативних пояснень і меж достовірності результатів [4; 7; 22].

Розглянуті в цьому розділі положення – мережеву організацію, рівні атрибуції, виміри стратегічного оцінювання та межі висновків з міжнародних кейсів – доцільно звести в єдину модель, що визначає послідовність роботи, розподіл функцій і умови переходу між етапами (табл. 1.5.3). Модель поєднує карту мережі, перевірку версій і процесуальну оцінку даних. Вона розмежовує функції аналітика (формування й перевірка версій, оцінювання достовірності джерел), дізнавача, слідчого або прокурора (визначення процесуальної підстави та форми отримання даних, ухвалення процесуальних рішень) і спеціаліста (технічне отримання, фіксація та дослідження даних).

Таблиця 1.5.3. Інтегрована модель протидії організованій кіберзлочинності

Етап	*Хто відповідає*	*Ключова умова або критерій виконання*	*Результат*
1. Первинна оцінка події та початок досудового розслідування	Слідчий або прокурор, дізнавач – у межах повноважень щодо дізнання. За потреби залучається аналітик.	Надійшла заява чи повідомлення про кримінальне правопорушення або самостійно виявлено обставини, що можуть свідчити про його вчинення.	Розпочато досудове розслідування в порядку ст. 214 КПК України або, за наявності відповідних умов, п. 1 ч. 1 ст. 615 КПК України. Визначено дані, що потребують першочергового збереження.
2. Побудова карти ролей, ресурсів і юрисдикцій	Аналітик, за потреби — з технічною допомогою спеціаліста.	Описано відомі вузли та їхні ймовірні функції. Визначено можливих володільців даних і юрисдикції. Позначено прогалини.	Карта мережі із зазначенням підтверджених і ймовірних зв’язків, джерел та юрисдикцій.
3. Перевірка версій та джерел	Аналітик.	Для ключових версій розглянуто альтернативні пояснення. Оцінено походження, надійність і незалежність джерел. Зафіксовано невизначеність.	Аналітичний висновок із розмежуванням підтверджених відомостей, робочих версій і неперевірених припущень та із зазначенням рівня впевненості в ключових висновках.

Етап	*Хто відповідає*	*Ключова умова або критерій виконання*	*Результат*
4. Отримання та процесуальна фіксація даних	Слідчий, прокурор або дізнавач у межах повноважень. Спеціаліст надає технічну допомогу в порядку, передбаченому КПК.	Визначено правову підставу й порядок отримання даних. За потреби одержано необхідний дозвіл або застосовано належний механізм міжнародного співробітництва.	Отримано дані та задокументовано їх походження, спосіб отримання і заходи зі збереження цілісності.
5. Вибір заходів та оцінювання їхніх наслідків	Уповноважені особи ухвалюють рішення в межах компетенції. Керівник підрозділу координує дії, аналітик оцінює результати.	Обґрунтовано вибір заходу з урахуванням правових підстав і можливих наслідків. Визначено показники оцінювання.	Задокументовано рішення, вжиті заходи та їхні наслідки. За наявності даних оцінено тривалість порушення функціонування мережі й ознаки відновлення її активності.

Примітка. Авторська модель. Якщо відомості суперечливі або альтернативне пояснення не виключено, робота повертається до етапу 3; нові дані, отримані на етапах 4–5, оновлюють карту мережі (етап 2). За наявності правової підстави невідкладне збереження даних може здійснюватися паралельно з побудовою карти мережі та перевіркою версій: модель не вимагає завершити етап 3 перед діями щодо збереження даних.

Проведемо ілюстрацію моделі на матеріалах операції проти Tycoon 2FA. За повідомленням Європолу, під час операції проти Tycoon 2FA припинено роботу 330 доменів, які забезпечували функціонування фішингових сторінок і панелей керування [88]. Ці відомості слугують вихідною точкою для побудови карти мережі. На такій карті Tycoon 2FA можна позначити як інфраструктурний вузол, що надавав користувачам сервісу засоби для компрометації облікових записів.

Карта мережі допомагає сформулювати версії щодо того, хто користувався цією інфраструктурою, яку роль виконували окремі учасники та наскільки їхня діяльність залежала від сервісу. Для перевірки цих версій потрібні додаткові відомості, зокрема дані постачальників послуг і результати дослідження вилученої

інфраструктури. Такі матеріали отримують і фіксують у встановленому законом порядку.

Щоб оцінити наслідки операції, потрібні дані про подальшу активність мережі. За ними можна було б з’ясувати, як довго тривало порушення роботи сервісу, чи відновилася його діяльність і чи перейшли його користувачі на інші платформи. Саме ці відомості дали б змогу оцінити тривалість ефекту від припинення роботи доменів.

РОЗДІЛ 2.
НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ТА МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ

2.1. Конституційні засади та система нормативно-правових актів

Під нормативно-правовим забезпеченням розуміють сукупність законодавчих та інших актів, що регулюють певну діяльність. Ефективність правоохоронної діяльності прямо корелює з якістю правового регулювання – особливо в умовах трансформації держави й суспільства [13]. Усі нормативно-правові акти у сфері протидії кіберзагрозам доцільно впорядкувати за юридичною силою. Нормативно-правову основу протидії кіберзагрозам становлять:

1. Конституція України, яка має найвищу юридичну силу.
2. Чинні міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України.
3. Закони України, підзаконні нормативно-правові акти, зокрема нормативні укази Президента України, постанови Кабінету Міністрів України та накази уповноважених органів державної влади.

Важливо, що регулювання протидії кіберзагрозам охоплює й супутні напрями: захист прав і свобод людини у сфері інформаційної безпеки, адміністративно- та кримінально-правове забезпечення протидії кіберзлочинності.

Відповідно до ст. 17 Конституції України, забезпечення економічної та інформаційної безпеки належить до найважливіших функцій держави та є справою всього Українського народу; забезпечення державної безпеки покладається на відповідні військові формування та правоохоронні органи. Водночас Конституція гарантує й права, що безпосередньо стосуються інформаційної сфери: за ст. 31–32 кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, а також невтручання в особисте й сімейне життя. Втручання можливе лише у визначених законом випадках і, як правило, за рішенням суду [16].

Гарантії таємниці комунікацій і невтручання в особисте життя не є абсолютними. За ст. 31 Конституції винятки може встановити лише суд – з метою запобігти злочину чи з'ясувати істину під час розслідування, якщо інакше одержати інформацію неможливо. А ст. 64 Конституції допускає окремі обмеження прав і свобод в умовах воєнного або надзвичайного стану – обов'язково із зазначенням строку дії таких обмежень. Отже, будь-яке втручання має спиратися на закон і бути пропорційним; «воєнний стан» не є підставою обходити процесуальні гарантії.

2.2. Міжнародні та європейські стандарти

Міжнародні та європейські документи утворюють платформу для єдиних підходів держав до забезпечення кібербезпеки. Для України вони мають додаткове значення в контексті євроінтеграції та гармонізації законодавства. Відправною точкою співпраці є Угода про асоціацію між Україною та ЄС [59]: ст. 22 передбачає співробітництво Сторін у боротьбі зі злочинністю та її попередженні, причому серед напрямів прямо названо кіберзлочинність (поряд із торгівлею людьми, незаконним обігом наркотиків і зброї, економічними злочинами, корупцією, підробкою документів).

Таблиця 2.2.1. Ключові міжнародні та європейські документи

Документ	*Значення для України*	*Що встановлює*
Конвенція про кіберзлочинність (Будапештська)	ратифікована у 2005 р.	криміналізує комп'ютерні правопорушення, закладає засади міжнародної співпраці
Додатковий протокол до Конвенції	ратифікований у 2006 р.	передбачає криміналізацію окремих діянь расистського та ксенофобного характеру, вчинених через комп'ютерні системи
Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних	ратифікована у 2010 р.	заходи безпеки та санкції для захисту персональних даних
Директива (ЄС) 2022/2555 (NIS 2)	acquis ЄС (орієнтир для гармонізації)	вимоги до національних стратегій і високого спільного рівня кібербезпеки
Угода про асоціацію Україна – ЄС (ст. 22)	набрала чинності в повному обсязі 1 вересня 2017 р.	співпраця в боротьбі зі злочинністю, зокрема кіберзлочинністю

Документ	*Значення для України*	*Що встановлює*
Другий додатковий протокол до Конвенції про кіберзлочинність (CETS № 224)	підписаний 30.11.2022; станом на вересень 2026 не ратифікований (за даними Договірного бюро Ради Європи) [71]	розширене співробітництво й розкриття електронних доказів: реєстраційні дані доменних імен, дані про абонентів і трафік, механізми для надзвичайних ситуацій, гарантії та захист персональних даних; набирає чинності першого дня місяця після спливу трьох місяців від дати, коли п’ять Сторін Конвенції висловили згоду на його обов’язковість, і застосовується між Сторонами, для яких він набрав чинності
Конвенція ООН проти кіберзлочинності (2024)	станом на вересень 2026 р. не набрала чинності; Україну в переліку підписантів не зазначено (за даними депозитарію ООН) [123]	ухвалена Генеральною Асамблеєю ООН 24.12.2024, відкрита для підписання 25.10.2025; глобальна рамка криміналізації, процесуальних повноважень і співробітництва щодо електронних доказів; набирає чинності на 90-й день після здачі на зберігання 40-го документа про ратифікацію, прийняття, затвердження або приєднання
Пакет ЄС щодо електронних доказів: Регламент (ЄС) 2023/1543, Директива (ЄС) 2023/1544	для України не є механізмом отримання даних; орієнтир гармонізації	європейські накази про надання та збереження електронних доказів, адресовані постачальникам послуг; обов’язок постачальників визначати адресата в ЄС; Регламент застосовується з 18.08.2026 у державах – членах ЄС (крім Данії)

Конвенція про кіберзлочинність (ратифікована у 2005 р.) [15] у розділі II визначає заходи матеріального кримінального права й поділяє склади кримінальних правопорушень на чотири групи:

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

2) пов’язані з комп’ютерами;

3) пов’язані зі змістом;

4) пов’язані з порушенням авторських і суміжних прав.

Її **Додатковий протокол до Конвенції про кіберзлочинність** від 28 січня 2003 року передбачає криміналізацію визначених у ньому діянь расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Отже, Додатковий протокол не створює автономного правового режиму, а розширює предметну сферу матеріально-правових положень Конвенції, що необхідно враховувати під час кримінально-правової кваліфікації відповідних діянь.

Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ратифікована у 2010 р.) зобов'язує вживати заходів безпеки проти випадкового чи несанкціонованого знищення, втрати, доступу, зміни або поширення персональних даних, а також установлювати санкції та засоби правового захисту за порушення відповідних норм [14].

Директива NIS 2 (Директива (ЄС) 2022/2555) вимагає, щоб кожна держава-член ухвалила національну стратегію кібербезпеки, яка визначає цілі й пріоритети, управлінську систему, механізми оцінювання ризиків, інструменти реагування на інциденти та відновлення, а також заходи підвищення обізнаності громадян. Директива охоплює й такі напрями, як кібербезпека ланцюгів постачання продуктів і послуг ІКТ, скоординоване оприлюднення інформації про вразливості, підтримання доступності, цілісності та конфіденційності «публічного ядра» відкритого інтернету, розвиток освіти й навичок, підтримка кіберстійкості та кібергігієни малих і середніх підприємств, сприяння активному кіберзахисту [75]. Для України цей документ є важливим орієнтиром гармонізації, хоча національна стратегія має враховувати й внутрішню безпекову ситуацію, загострену збройною агресією РФ.

Європейська правова рамка не обмежується переліченими документами. Питання застосування штучного інтелекту регулює Регламент (ЄС) 2024/1689 (Artificial Intelligence Act) – його положення, зокрема щодо заборони прогнозування злочинної поведінки виключно на основі профілювання, детально розглянуто в Розділі 4. А транскордонний доступ до електронних доказів охоплює Другий додатковий протокол до Конвенції про кіберзлочинність (CETS № 224) – призначення його положень пояснено в підрозділі 5.2 [119]. На рівні ООН ухвалено Конвенцію проти кіберзлочинності, яка станом на вересень 2026 не набрала чинності [123], а в ЄС з 18.08.2026 застосовується Регламент (ЄС) 2023/1543 про європейські накази щодо надання та збереження електронних доказів [116] (див. табл. 2.2.1).

Міжнародні та європейські документи виконують подвійну роль: вони встановлюють спільні стандарти протидії кіберзлочинності, і слугують орієнтиром для гармонізації українського законодавства. Для практика це означає, що національні норми потрібно тлумачити в контексті відповідних міжнародних зобов'язань України.

2.3. Національне законодавство України

На виконання конституційних засад і міжнародних зобов'язань в Україні сформовано розгалужену систему національних актів. Її ядро становлять закони.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» (№ 80/94-ВР) регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [46].

Закон України «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII) є базовим: він визначає правові й організаційні основи захисту життєво важливих інтересів людини, суспільства та держави в кіберпросторі, цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження суб'єктів і засади координації їхньої діяльності [52].

Закон України «Про захист персональних даних» (№ 2297-VI) регулює обробку й захист персональних даних та спрямований на захист прав людини, зокрема права на невтручання в особисте життя [47].

Окремі аспекти обробки й захисту інформації регулюють також закони «Про інформацію» (ст. 11 – про конфіденційну інформацію про особу, яку не можна збирати, зберігати, використовувати й поширювати без згоди, крім визначених законом випадків), «Про електронні комунікації» (ст. 119 – про обов'язок постачальників забезпечувати схоронність даних щодо кінцевого користувача) та «Про доступ до публічної інформації» (ст. 10-1 – про умови оприлюднення публічної інформації, що містить персональні дані, у формі відкритих даних) [36; 37; 48].

Оскільки подальші розділи присвячені роботі з відкритими джерелами та цифровими доказами, доцільно окремо розглянути підстави обробки персональних даних [47].

Підстави обробки персональних даних: за Законом України «Про захист персональних даних», персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Стаття 11 визначає вичерпний перелік підстав для їх обробки:
- згода суб'єкта персональних даних;
- дозвіл на обробку, наданий володільцю відповідно до закону виключно для здійснення його повноважень;
- укладення та виконання правочину, стороною/вигодонабувачем якого є суб'єкт даних;
- захист життєво важливих інтересів суб'єкта даних;
- виконання обов'язку володільця, передбаченого законом;
- захист законних інтересів володільця або третьої особи (крім випадків переважання прав суб'єкта даних).

Для працівника поліції це означає: збирання й використання персональних даних (зокрема з відкритих джерел) має спиратися на конкретну законну підставу, а не на саму лише технічну можливість їх отримати.

Крім законів, сферу протидії кіберзагрозам регулює значний масив підзаконних актів.

Таблиця 2.3.1. Основні підзаконні нормативно-правові акти (за функцією)

Група	**Акт**
Стратегічні документи	Стратегія кібербезпеки України (Указ Президента № 447/2021) [53]; Стратегія інформаційної безпеки (Указ Президента № 685/2021) [54]
Інституційні засади	Положення про Національний координаційний центр кібербезпеки (Указ Президента № 242/2016) [49]; Положення про організаційно-технічну модель кіберзахисту (постанова КМУ № 1426, 2021) [40]
Реагування та взаємодія	Національний план реагування на кіберінциденти, кібератаки та кіберзагрози (постанова КМУ № 1533, 2025) [39]; Порядок взаємодії суб'єктів національної системи реагування з правоохоронними та іншими органами (постанова КМУ № 1471, 2025) [42]
Контроль і оцінювання	Порядок державного контролю за додержанням вимог у сфері кіберзахисту (постанова КМУ № 1668, 2025) [43]; Порядок оцінювання стану кіберзахисту систем та об'єктів критичної інфраструктури (постанова КМУ № 1799, 2025) [45]
Критична інфраструктура та обмін	Порядок ведення Реєстру об'єктів критичної інфраструктури (постанова КМУ № 415, 2023) [41]; Порядок міжвідомчого обміну в Національній системі конфіденційного зв'язку (постанова КМУ № 303, 2015) [44]

Підзаконна база стрімко оновлюється: лише наприкінці 2025 року ухвалено одразу кілька ключових актів (постанови КМУ № 1533, 1471, 1668, 1799). Це означає, що працівник поліції має періодично звірятися з чинними редакціями, адже нормативне регулювання цієї сфери змінюється швидше, ніж багатьох інших.

Нормативні акти, наведені в табл. 2.3.1, визначають не лише повноваження суб'єктів, а й послідовність їхніх дій. Закон № 2163-VIII у редакції Закону № 4336-IX від 27.03.2025 [32; 52] оновив перелік і повноваження суб'єктів забезпечення кібербезпеки, засади кіберзахисту державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, а також національну систему реагування на кіберінциденти. Національний план реагування (постанова КМУ № 1533) і Порядок взаємодії суб'єктів національної системи реагування з правоохоронними та іншими органами (постанова КМУ № 1471) [39; 42] пов'язують технічне реагування на кіберінцидент із передаванням відомостей правоохоронним органам. Для практичного застосування цей зв'язок доцільно подати у вигляді матриці (табл. 2.3.2).

Таблиця 2.3.2. Від події до процесуального рішення: розподіл дій суб'єктів

Подія	***Хто реагує***	***Які матеріали передаються***	**На якій підставі**	**Наступне рішення**
Кіберінцидент в інформаційній системі (зокрема на об'єкті критичної інформаційної інфраструктури)	Власник (оператор) системи; CERT-UA та інші суб'єкти національної системи реагування	Повідомлення про інцидент, індикатори компрометації, журнали подій	Закон № 2163-VIII (у ред. Закону № 4336-IX); постанови КМУ № 1533, № 1471	Локалізація та усунення наслідків; оцінка наявності ознак кримінального правопорушення
Під час реагування виявлено обставини, що можуть свідчити про вчинення кримінального правопорушення	Суб'єкт реагування; Національна поліція (кіберполіція) або інший правоохоронний орган за підслідністю	Відомості про інцидент, збережені дані, контакти володільців інформації	Постанова КМУ № 1471; ст. 214 КПК України	Внесення відомостей до ЄРДР у порядку ст. 214 КПК України
Заява потерпілого про кіберзлочин	Орган Національної поліції	Заява, наявні цифрові матеріали (повідомлення, реквізити, знімки екрана) із зазначенням їх походження	Ст. 214 КПК України	Внесення відомостей до ЄРДР; вжиття заходів для збереження даних за наявності належної правової підстави; планування процесуальних дій

Подія	*Хто реагує*	*Які матеріали передаються*	На якій підставі	Наступне рішення
Потрібні дані, що зберігаються в іноземного постачальника послуг	Слідчий, прокурор; контактний пункт мережі 24/7	Запит про термінове збереження; надалі – запит у межах належного механізму міжнародного співробітництва	Ст. 29, 35 Конвенції про кіберзлочинність; розділ IX КПК України	Отримання даних у процесуальній формі, придатній для використання в доказуванні

Примітка. Авторська систематизація. Матриця відображає типову послідовність дій і не замінює вимог відповідних нормативно-правових актів.

Реагування на кіберінцидент і досудове розслідування мають різні цілі: перше спрямоване на відновлення функціонування систем, друге – на встановлення обставин кримінального правопорушення. Тому за наявності обставин, що можуть свідчити про вчинення кримінального правопорушення, суб'єкти реагування мають ураховувати потребу збереження даних, що можуть стати джерелом доказів, а рішення про початок досудового розслідування ухвалюють у порядку ст. 214 КПК України [18].

2.4. Особливості правового регулювання в умовах воєнного стану

Збройна агресія РФ загострила проблему кібербезпеки, сформувавши нові – зовнішні – загрози військово-політичного характеру. Це вплинуло і на правове регулювання.

По-перше, як зазначено вище, ст. 64 Конституції допускає окремі обмеження прав і свобод в умовах воєнного стану – обов'язково зі строком дії [16].

По-друге, законодавець оперативно вніс зміни, орієнтовані на швидкість реагування та посилення відповідальності:

- Закон України № 2137-IX (від 15.03.2022) вніс зміни до Кримінального процесуального кодексу України та Закону «Про електронні комунікації» задля підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам [35]. Ці зміни особливо важливі з огляду на *фактор часу*: дані про з'єднання зберігаються обмежений строк, і зволікання може призвести до їх втрати;

- Закон України № 2149-IX (від 24.03.2022) вніс зміни до Кримінального кодексу України щодо посилення боротьби з кіберзлочинністю в умовах воєнного стану [34].

До воєнного «пакета» належать і закони, спрямовані на протидію ворожому інформаційному впливу, зокрема щодо заборони виготовлення та поширення

інформаційної продукції, що пропагує дії держави-агресора (закони № 2109-IX та № 2110-IX) [31; 33].

По-третє, значну частину оновлень становлять підзаконні акти реагування, ухвалені у 2025 році (постанови КМУ № 1533, 1471, 1668, 1799) [39; 42; 43; 45], що свідчить про активну розбудову національної системи реагування на кіберінциденти.

Окремо слід ураховувати спеціальний порядок досудового розслідування в умовах воєнного стану, передбачений ст. 615 КПК України. Його застосовують лише за наявності умов, визначених цією статтею, зокрема коли виконання відповідних процесуальних дій у порядку та строки, встановлені КПК, є об'єктивно неможливим. Цей порядок не скасовує загальних засад кримінального провадження і не є підставою для обходу процесуальних гарантій під час отримання цифрових даних [18].

Оцінювання практичних наслідків розглянутих законодавчих змін потребує окремого дослідження. Дані про зареєстровані кримінальні правопорушення самі по собі не вимірюють ефекту правових змін: їхня динаміка залежить також від рівня виявлення, повідомлення про події та практики кваліфікації. Для обґрунтованого висновку потрібні зіставні дані за визначені періоди до і після змін із розбивкою за статтями КК України, рядками та показниками звітності. За відсутності таких даних доцільно говорити не про результативність змін, а про напрями подальшого вдосконалення – посилення міжнародної взаємодії та впровадження сучасних аналітичних інструментів, яким присвячено наступні розділи.

РОЗДІЛ 3. OSINT ТА ЦИФРОВА КРИМІНАЛІСТИКА В ДІЯЛЬНОСТІ ПОЛІЦІЇ

3.1. Інформаційно-аналітична модель роботи (Intelligence-Led Policing)

Практично будь-яка діяльність людини сьогодні пов’язана з використанням цифрових технологій, а отже, залишає інформаційні відображення у цифровому середовищі. Значна частина цих даних формується *автоматично*, без активної участі користувача (авторизації в системах, синхронізація з хмарою, службові журнали), що підвищує їх криміналістичну цінність. Через це цифрові дані перетворилися на один із найважливіших об’єктів дослідження та інформаційно-аналітичного забезпечення поліції.

Традиційно робота поліції ґрунтувалася на матеріальних слідах, показаннях і речових доказах. Цифровізація змінила не лише способи вчинення правопорушень, а й характер інформації, що використовується під час їх розслідування: якщо раніше цифрові дані були допоміжними, то сьогодні вони нерідко становлять *основу* доказової бази. Відповідно, сучасна діяльність поліції дедалі більше орієнтується на **інформаційно-аналітичну модель**: ключову роль відіграють не лише реагування на вже вчинене, а й своєчасне виявлення інформаційних ознак протиправної діяльності, аналіз цифрових взаємозв’язків і прийняття рішень на основі комплексного аналізу. Такий підхід відповідає міжнародній концепції **Intelligence-Led Policing (ILP)**, за якою інформація та її аналітичне опрацювання є основою планування роботи правоохоронних органів [4; 7].

У межах цієї моделі цінність становить не накопичення максимального обсягу даних, а перетворення різнорідних масивів на *перевірене знання*, придатне для управлінських і процесуальних рішень. Досягається це поєднанням двох взаємопов’язаних напрямів роботи з цифровою інформацією.

Таблиця 3.1.1. OSINT і цифрова криміналістика: розмежування функцій

Ознака	*OSINT (відкрита розвідка)*	*Цифрова криміналістика*
Об’єкт	інформація у відкритих джерелах	цифрові дані на носіях, у системах, мережах, хмарі
Мета	пошук, збір, перевірка, аналітичне опрацювання	виявлення, вилучення, дослідження, процесуальне закріплення
Режим доступу	законно доступна відкрита інформація	доступ у порядку, визначеному КПК (часто за судовим рішенням)

Ознака	*OSINT (відкрита розвідка)*	*Цифрова криміналістика*
Типовий результат	орієнтуюча інформація, пошукові гіпотези, зв’язки; первинний матеріал із відкритого джерела за належної фіксації може використовуватися в доказуванні	задокументовані результати технічного дослідження; доказове використання залежить від способу отримання, процесуального джерела та оцінки у провадженні

Ці напрями не конкурують, а утворюють єдину систему. Результати OSINT (наприклад, встановлені акаунти, електронні адреси, доменні імена чи криптовалютні гаманці) визначають подальші напрями пошуку, а підтвердження причетності конкретної особи потребує вже методів цифрової криміналістики. У свою чергу, дослідження мобільного телефону чи комп’ютера дає нові цифрові ідентифікатори, які стають вихідними даними для наступного OSINT-дослідження [21; 113].



Рис. 3.1.1. Циклічність роботи з цифровою інформацією

Особливого значення ці інструменти набули в Україні в умовах повномасштабної збройної агресії РФ: документування воєнних злочинів, встановлення причетних осіб, аналіз інформаційних операцій і взаємодія з міжнародними партнерами суттєво розширили сферу практичного застосування OSINT та цифрової криміналістики.

3.2. Класифікація відкритих джерел і критична оцінка інформації

Обсяг інформації у відкритому доступі безперервно зростає: державні реєстри, електронні сервіси, соціальні мережі, геоінформаційні платформи створюють нові можливості для поліції. Якщо кілька десятиліть тому багато відомостей можна було отримати лише за офіційним запитом, то сьогодні значний їх обсяг доступний із законних відкритих джерел.

Проте **відкритість інформації не означає її автоматичної придатності** для правоохоронної діяльності. Відкриті джерела дуже неоднорідні за достовірністю, актуальністю й повнотою. Частина відомостей формується користувачами без будь-якої перевірки, а інформаційний простір активно використовується для дезінформації та маніпуляцій. Тому одним із ключових є **принцип критичної оцінки джерела**: значення має не лише зміст інформації, а й розуміння її походження, способу формування, часу оприлюднення, можливих мотивів автора та ризиків викривлення. Відкриті джерела не обмежуються вебсайтами й соцмережами. Їх доцільно систематизувати за функціональним призначенням і характером інформації [10; 28; 113].

Таблиця 3.2.1. Категорії відкритих джерел у діяльності поліції

Категорія	*Що містить*	*Особливість*
Офіційні державні ресурси	державні реєстри, портали органів влади, судові рішення, відкриті дані, публічні закупівлі	високий рівень достовірності; цінна орієнтуюча інформація
Ресурси соціальних медіа	публікації, фото й відео, контакти, участь у спільнотах, геопозначки	найінформативніші, але потребують найретельнішої перевірки (можливі приховування й фальсифікації)
Інформаційно-медійні ресурси	ЗМІ, інформаційні агентства, пресрелізи, аналітичні платформи	дають змогу відстежувати події в часі; ризик неперевірених чи викривлених відомостей
Геоінформаційні та картографічні	супутникові знімки, цифрові карти, панорами, моніторинг руху	геолокація, документування змін обстановки (зокрема воєнних злочинів)

Категорія	*Що містить*	*Особливість*
Технічні відкриті джерела	домени, IP-адреси, DNS-записи, цифрові сертифікати, історичні записи	розслідування фішингу, malware-інфраструктури, встановлення інфраструктури угруповань
Ресурси віртуальних активів / блокчейн	публічні транзакції, криптовалютні адреси	простеження руху активів; протидія відмиванню та фінансуванню злочинності

Робота з відкритими джерелами не звільняє від дотримання законодавства про захист персональних даних (див. Розділ 2). Збирання й використання персональних даних, навіть загальнодоступних, має спиратися на законну підставу, бути пропорційним меті й не порушувати прав людини. Загальнодоступність відомостей не робить будь-які дії з ними автоматично правомірними.

3.3. Інструментарій OSINT

Професійне OSINT-дослідження ґрунтується не на кількості сервісів, а на *обґрунтованій послідовності* їх застосування (див. рис. 3.3.1). Вибір інструмента визначається характером вихідних даних, типом об'єкта й поставленим завданням:

1. Пошукові системи й оператори розширеного пошуку. Результативний пошук передбачає не просто введення ключових слів, а формування стратегії: точні словосполучення, альтернативне написання імен, оператори (обмеження за доменом, типом файлу, фрагментом URL, точною фразою). Різні системи по-різному індексують і ранжують результати, тому відсутність відомостей в одній із них не є доказом їх відсутності.

2. Ретроспективний аналіз. Інформацію нерідко змінюють або видаляють, але попередні версії можуть зберігатися. Класичний засіб – Wayback Machine, що дає доступ до архівних копій вебсторінок за різні періоди. Цей засіб і подібні корисні для дослідження історії шахрайських чи фішингових ресурсів. Проте слід зауважити, що архівна копія може бути неповною, тож відсутність елемента в архіві не доводить, що його не було на сайті.



Рис. 3.3.1. Логіка OSINT-дослідження

3. Пошук за цифровими ідентифікаторами. Вихідними даними часто є окрема ознака – псевдонім, електронна адреса, номер телефону тощо. Користувачі нерідко застосовують однакові псевдоніми на різних платформах, що дозволяє будувати початкову «карту» цифрової присутності. Але збіг псевдоніма (як і згадка e-mail чи номера) – це лише *пошукова ознака*: вона потребує перевірки за сукупністю інших характеристик (фото, контакти, час активності, мовні особливості, зв'язки і т.д.).

4. Дослідження особи та її оточення. Спеціалізовані платформи, як-от Big Data People (Artellence), поєднують фотопошук (пошук імовірних відповідностей за зображенням із зазначенням джерел), побудову графів зв'язків, семантичний аналіз тексту (методами обробки природної мови) і просторово-часовий аналіз активності. Це дає змогу перейти від окремої особи до її інформаційного оточення. Проте візуалізований зв'язок – аналітична ознака, а не самодостатнє підтвердження відносин. Для висновку, отриманого з біометричного пошуку чи комерційної платформи, фіксують межі даних, на яких ґрунтується результат, і підставу подальшої перевірки.

5. Відкриті державні та корпоративні дані. Для переходу від особи до пов'язаних компаній, судових і виконавчих проваджень, закупівель і санкцій застосовують українські аналітичні системи. YouControl агрегує дані з понад 180 державних реєстрів та офіційних джерел і дає змогу досліджувати структуру власності, керівництва, зв'язки суб'єктів та історичну динаміку змін [128]. Opendatabot забезпечує швидкий перехід від первинного ідентифікатора (назва, код ЄДРПОУ, ПІБ, ФОП) до структурованих відкритих даних і має API до низки

реєстрів [112]. Слід зауважити, що агрегатор *не замінює першоджерело* – ключові обставини перевіряють за офіційними даними. Для агрегаторів і комерційних платформ у матеріалах перевірки зазначають походження даних, категорію доступу, дату актуальності відомостей і можливість їх незалежної перевірки.

6. Технічна інфраструктура. Доменне ім'я, IP-адреса, DNS-записи й сертифікати можуть бути вихідними точками. Первинні відомості дають WHOIS/RDAP і аналіз DNS; SecurityTrails дозволяє працювати з історією DNS і піддоменами; urlscan.io показує технічні взаємодії сторінки (звернення до зовнішніх доменів, завантаження сценаріїв); VirusTotal зіставляє URL, домени, IP-адреси та файли. Проте зауважимо, що спільна IP-адреса чи інший технічний збіг самі по собі не підтверджують спільне адміністрування. Перед надсиланням матеріалів до urlscan.io чи VirusTotal перевіряють режим видимості результатів (публічний чи приватний), оскільки надіслані дані можуть стати доступними іншим користувачам сервісу; для службових матеріалів використовують засоби, схвалені в підрозділі.

7. Верифікація цифрового контенту. Фото й відео можуть містити цінні відомості, але їх легко модифікувати чи згенерувати. Перевірка охоплює:

- зворотний пошук зображень (Google Lens, TinEye тощо) для виявлення попередніх публікацій і копій;
- аналіз метаданих (наприклад, ExifTool);
- візуальний аналіз і геолокацію (зіставлення орієнтирів із картами, супутниковими знімками, панорамами);
- роботу з відео через виділення ключових кадрів (InVID-WeVerify);
- перевірку часу (тіні, погода, сезон і т.д.).

Водночас слід ураховувати два методологічні застереження: перша знайдена копія не завжди є першоджерелом, а відсутність метаданих не є ознакою маніпуляції (соцмережі часто видаляють їх під час завантаження).

Таблиця 3.3.1. Інструменти OSINT за завданнями

Завдання	*Приклади інструментів*	*Ключове застереження*
Розширений пошук у вебі	оператори пошукових систем	системи індексують по-різному – зіставляйте результати
Ретроспектива вебсторінок	Wayback Machine	архівна копія може бути неповною
Пошук за ідентифікаторами	пошук за username / email / номером	збіг ≠ належність одній особі

Завдання	*Приклади інструментів*	*Ключове застереження*
Особа та оточення	Big Data People (Artellence)	зв’язок – аналітична ознака, потребує перевірки
Відкриті державні/корпоративні дані	YouControl, Opendatabot	агрегатор не замінює першоджерело
Технічна інфраструктура	WHOIS/RDAP, SecurityTrails, urlscan.io, VirusTotal	технічний збіг ≠ спільне адміністрування
Верифікація контенту	Google Lens, TinEye, ExifTool, InVID-WeVerify	найраніша копія ≠ першоджерело; брак метаданих ≠ маніпуляція

Замість розширення переліку сервісів доцільно стандартизувати фіксацію результатів перевірки. Для цього кожне суттєве твердження, отримане з відкритих джерел, оформлюють у вигляді короткої картки перевірки (табл. 3.3.2).

Таблиця 3.3.2. Картка перевірки відкритих даних

Елемент картки	*Що фіксують*	*Приклад: дві публікації з тим самим відео*
Твердження, яке перевіряють	Конкретне твердження, а не тема загалом	Відео зафіксувало певну подію в певному місці та час
Первинне джерело та похідні публікації	Хто першим оприлюднив матеріал; які публікації його відтворюють	Обидві публікації відтворюють те саме відео; первинне джерело встановлюють окремо
Час і спосіб фіксації	Коли, ким і яким засобом збережено матеріал; контрольне (геш-)значення	Збережено сторінки й файл відео з датою, URL і геш-значенням
Незалежні підтвердження	Джерела, що не походять від того самого матеріалу	Супутникові знімки, інші відеозаписи, офіційні дані щодо місця й часу

Елемент картки	*Що фіксують*	*Приклад: дві публікації з тим самим відео*
Альтернативні пояснення	Інші місце, час чи подія, яким може відповідати матеріал; ознаки монтажу чи генерування	Відео могло бути зняте раніше або в іншому місці
Статус висновку	Встановлено / обґрунтована версія / не підтверджено	Встановлено факт поширення відео; відомості про саму подію – версія, що потребує підтвердження

Наведений приклад показує типову помилку: дві публікації, що відтворюють те саме відео, підтверджують поширення відео, а не саму подію. Відомості про подію потребують окремого підтвердження незалежними джерелами.

Радимо ознайомитися з наступними інструментами та підходами OSINT. Базові навігатори та каталоги інструментів:
OSINT Framework – структуроване дерево джерел та утиліт для пошуку за типами даних: https://osintframework.com/;
AsIntCollection – систематизована тематична панель пошукових інструментів та реєстрів: https://start.me/p/b5Aow7/asint_collection.
Методологія та розслідувальні платформи:
Bellingcat – міжнародний колектив дослідників; їхні методичні гайди та відкритий інструментарій Bellingcat Toolkit: https://www.bellingcat.com/;
Berkeley Protocol on Digital Open Source Investigations (OOH) – базовий міжнародний стандарт юридичної фіксації та верифікації відкритих цифрових даних: https://www.ohchr.org/;
OCCRP Aleph – глобальний архів витоків, корпоративних реєстрів та документів для дослідження міжнародної злочинності: https://aleph.occrp.org/.

3.4. Цифрова криміналістика та її взаємодія з OSINT

Якщо OSINT працює з відкритою інформацією, то встановлення фактичних обставин часто потребує дослідження даних на носіях, у пристроях, системах, мережах і хмарі. Специфіку цієї роботи визначає *природа цифрових даних*: вони можуть бути швидко змінені, скопійовані, переміщені чи знищені, а частина існує лише обмежений час (оперативна пам’ять, активні з’єднання, тимчасові файли, хмарні сесії). Тому помилка на початковому етапі здатна не лише знищити відомості, а й змінити початковий стан середовища.

Через це цифрова криміналістика ґрунтується на контрольованій послідовності дій (див. рис. 3.4.1.).



Рис. 3.4.1. Контрольована послідовність роботи з цифровими даними

Ключові засади цієї роботи включають:

1) *Цілісність (незмінність) даних.* Оригінальний носій чітко відмежовують від копії. Для перевірки незмінності застосовують криптографічні геш-функції: унікальне контрольне значення масиву даних порівнюють на різних етапах – якщо воно збіглося, дані не змінювалися.

2) *Спосіб отримання даних.* Спосіб отримання даних визначають за типом джерела, завданням дослідження, правовими межами та технічною доступністю. Для сумісного носія можливе створення побітового образу, що дає змогу досліджувати також видалені об’єкти, залишкові фрагменти й нерозподілений простір; дослідження в такому разі проводять на копії. Для інших джерел застосовують доступний спосіб отримання даних у визначеному обсязі. У документації зазначають метод, його обмеження та можливі зміни стану джерела.

3) *Пріоритетність отримання.* Дані мають різну стійкість: нестійкі (оперативна пам’ять, активні з’єднання, відкриті сесії і т.д.) втрачаються після вимкнення чи від’єднання пристрою, тому їх фіксують першими.

4) *Мобільну криміналістику*. Смартфон – комплексне джерело даних (комунікації, контакти, медіа, геолокація, активність застосунків, підключення до мереж і т.д.). Спосіб отримання визначає обсяг доступних даних.

Таблиця 3.4.1. Способи отримання даних із мобільного пристрою

Спосіб	*Результат*
Логічне отримання	доступ до визначених категорій даних через доступні програмні механізми
Отримання файлової системи	бази даних застосунків, журнали, конфігураційні файли, системні артефакти

Спосіб	*Результат*
Фізичне отримання	копія доступного вмісту пам’яті для поглибленого аналізу (за наявності технічної можливості)

Примітка. Наведені способи є узагальненою класифікацією. Їх доступність і обсяг одержаних даних залежать від моделі пристрою, версії операційної системи, стану блокування, засобу та завдання дослідження [95].

Дослідження мобільного пристрою є однією з найскладніших ділянок цифрової криміналістики: сучасний смартфон поєднує комунікації, контакти, медіа, геолокацію, активність застосунків і дані про підключення до мереж, а виробники постійно посилюють шифрування та механізми захисту. Саме тому для законного вилучення й дослідження таких даних застосовують спеціалізовані програмно-апаратні комплекси, два з яких набули статусу галузевих стандартів: Cellebrite UFED та Magnet AXIOM [65; 67; 108].

Cellebrite UFED (Universal Forensic Extraction Device – універсальний пристрій для криміналістичного вилучення даних) розробляє ізраїльська компанія Cellebrite, заснована 1999 р. у м. Петах-Тіква. Виробник позиціює рішення як «галузевий стандарт законного доступу та збору цифрових даних». UFED підтримує найширший спектр джерел – кнопкові телефони та смартфони на iOS і Android, SIM- та SD-картки, GPS-пристрої й навіть дрони [66; 67].

Залежно від моделі пристрою, версії операційної системи та стану блокування UFED застосовує кілька методів збору даних: логічне вилучення, вилучення файлової системи (full file system, FFS) і фізичне вилучення, а також техніки доступу «після першого розблокування» (After-First-Unlock, AFU) до сучасних пристроїв iOS та Android. Принциповою є вимога «криміналістично коректного збору» – збереження цілісності даних упродовж усього процесу. Роботу побудовано у два етапи: UFED здійснює вилучення, а подальший аналіз, декодування даних застосунків, розшифрування за допомогою ключів пристрою та елементів «в’язки ключів», атаки з відновлення пароля й формування звітів (зокрема у форматах PDF і HTML) виконує модуль Physical Analyzer. Для доступу до заблокованих пристроїв у лінійці виробника представлено рішення UFED Premium, а для роботи з хмарними джерелами – UFED Cloud Analyzer.

У 2024 р. Cellebrite об’єднала й оновила лінійку в межах єдиного пакета Cellebrite Inseyets, який виробник називає «остаточним пакетом цифрової криміналістики». UFED та оновлений аналітичний модуль (Physical Analyzer, версія PA x10) входять до цього пакета й, за заявою компанії, забезпечують доступ до даних, раніше недосяжних. Попри ребрендинг, абревіатура UFED залишається усталеною назвою етапу вилучення [65].

Magnet AXIOM – програмна платформа цифрової криміналістики канадської компанії Magnet Forensics (м. Ватерлоо, провінція Онтаріо). На відміну від UFED,

орієнтованого насамперед на вилучення, AXIOM є передусім аналітичною платформою: вона дає змогу відновлювати, аналізувати та формувати звіти за даними одразу з кількох типів джерел – комп'ютерів, мобільних пристроїв, хмарних сервісів і навіть бортових систем транспортних засобів – у межах єдиної справи. Платформа організовує дані за артефактами (слідами застосунків, пристроїв і хмарних сервісів) та надає інструменти інтелектуального аналізу, побудови зв'язків і єдиної хронології подій, що безпосередньо відповідає розглянутому вище принципу побудови єдиної хронології цифрових подій.

Саме вилучення даних, зокрема із заблокованих пристроїв, в екосистемі Magnet виконують окремі спеціалізовані продукти, а компонент Magnet One пов'язує інструменти між собою через хмару. У 2023 р. Magnet Forensics придбала інвестиційна компанія Thoma Bravo, об'єднавши її з компанією Grayshift – розробником рішення GrayKey [109].

GrayKey (спершу продукт компанії Grayshift, нині – Magnet GrayKey) призначений для законного доступу до заблокованих і зашифрованих пристроїв iOS та Android – від застарілих до найновіших моделей. Серед можливостей – збереження вилучених даних (захист від таймерів автоматичного перезавантаження та від втрати відомостей, що «застарівають» із часом), розшифрування keychain (iOS) і даних keystore (Android). Інструмент має обмежений обіг: він доступний лише правоохоронним і державним органам визначеного кола країн і не постачається приватному сектору. Перелік підтримуваних моделей і версій операційних систем змінюється з оновленнями, тому його звіряють з актуальною документацією виробника [110], а результати незалежного тестування конкретної версії – з матеріалами програми NIST CFTT [70].

Застосування будь-якого з цих комплексів підпорядковане загальній методології. Міжнародним орієнтиром є настанови NIST SP 800-101 (Guidelines on Mobile Device Forensics) [95], які наводять класифікацію методів отримання даних за п'ятьма рівнями (вибір конкретного способу залежить від пристрою, засобу та завдання дослідження):

1) ручне вилучення (зчитування з екрана);
2) логічне вилучення;
3) hex-dump / JTAG (фізичне вилучення пам'яті «на місці»);
4) chip-off (фізичне зняття мікросхеми пам'яті);
5) micro read (мікроскопічне зчитування станів комірок пам'яті).

У міру переходу від першого рівня до п'ятого методи стають технічно складнішими, інвазивнішими, тривалішими й дорожчими, а застосування окремих методів (передусім інвазивних, як-от chip-off) створює ризик, що інші способи отримання стануть недоступними; цей ризик залежить від конкретного методу й пристрою. Саме тому порядок і спосіб вилучення планують заздалегідь, із урахуванням пріоритетності отримання нестійких даних.

Логічне вилучення дає копію логічних об'єктів зберігання (файлів і каталогів у межах файлової системи), тоді як фізичне – образ фізичного носія (мікросхеми

пам’яті), включно з видаленими об’єктами, залишковими фрагментами та нерозподіленим простором. Обсяг фактично доступних даних щоразу залежить від моделі пристрою, версії операційної системи, стану блокування та механізмів захисту. Дослідження, як правило, проводять на криміналістичній копії, а її незмінність підтверджують криптографічними геш-функціями.

Професійне використання таких комплексів передбачає кілька застережень:

По-перше, інструмент залишається лише засобом: технічний результат (виявлений акаунт, номер, з’єднання і т.д.) потребує аналітичної інтерпретації та процесуального закріплення й сам по собі не підтверджує причетності конкретної особи.

По-друге, застосування можливе виключно на законних підставах, із дотриманням вимог щодо судового санкціонування та захисту персональних даних (див. Розділ 2).

По-третє, надійність інструментів потребує перевірки: програми криміналістичного тестування (зокрема NIST CFTT [70]) верифікують коректність роботи таких засобів, а практика засвідчує, що навіть у провідних рішень виявляли вразливості – так, у квітні 2021 р. розробники месенджера Signal оприлюднили опис вразливостей в UFED і Physical Analyzer [111]. Це обґрунтовує вимогу працювати лише з актуальними, валідованими версіями й документувати кожну суттєву дію.

Технічний з’язок між об’єктами ще не визначає його змісту, а виявлення акаунта, номера чи e-mail не підтверджує автоматично їх використання конкретною особою в конкретний час. Обґрунтований висновок формується на сукупності взаємопов’язаних даних із різних незалежних джерел, із чітким розмежуванням установлених фактів, аналітичних висновків і гіпотез.

3.5. OSINT у документуванні воєнних злочинів

Документування воєнних злочинів не належить безпосередньо до протидії організованій кіберзлочинності, проте є суміжною практикою, у якій найповніше сформовано вимоги до роботи з відкритими цифровими даними. З неї доцільно запозичувати критерії встановлення походження матеріалу, оцінювання незалежності джерел і збереження контенту, придатного для подальшої перевірки.

В умовах збройної агресії РФ сфера застосування OSINT і цифрової криміналістики суттєво розширилася: відкриті дані використовують для документування воєнних злочинів, встановлення причетних осіб, аналізу інформаційних операцій і взаємодії з міжнародними партнерами. Супутникові знімки, відкриті картографічні сервіси та верифікований контент із соціальних мереж дають змогу підтверджувати факт руйнування об’єктів цивільної інфраструктури, переміщення техніки чи зміну обстановки на місцевості. Особливість цієї роботи – підвищені вимоги до достовірності й документування,

адже зібрані матеріали можуть бути використані в міжнародних юрисдикційних процесах, де до доказів застосовують найсуворіші стандарти [115].

У практиці документування можна виокремити кілька взаємопов'язаних напрямів. Перший – фіксація самих подій: за допомогою комерційних супутникових знімків (зокрема операторів Maxar Technologies та Planet Labs), відкритих картографічних і панорамних сервісів та верифікованого користувацького контенту встановлюють факт, час і місце ударів по цивільних об'єктах, руйнувань, переміщення військової техніки. Другий – встановлення причетних осіб і підрозділів через зіставлення цифрових ідентифікаторів, елементів форми, маркувань техніки, відкритих профілів і метаданих. Третій – аналіз інформаційних операцій і протидія дезінформації, адже держава-агресор систематично намагається дискредитувати відкриті докази (показовим є спростування російських заперечень щодо подій у Бучі, проведене на основі супутникових знімків та відкритих даних) [76]. Четвертий – взаємодія з міжнародними партнерами та передання верифікованих матеріалів до відповідних механізмів правосуддя.

ПРАКТИЧНИЙ КЕЙС

Міжнародним орієнтиром для розслідувань на основі відкритих цифрових даних є ***Berkeley Protocol on Digital Open Source Investigations*** *(ООН, 2022) – практичний посібник з ефективного використання відкритої цифрової інформації під час розслідування порушень міжнародного кримінального, гуманітарного права та прав людини. Він задає стандарти пошуку, верифікації, збереження й документування цифрових матеріалів так, щоб вони зберігали доказову цінність. Для української практики документування воєнних злочинів цей протокол є базовим методологічним документом.*

Джерело: Berkeley Protocol on Digital Open Source Investigations. United Nations, 2022.

Протокол Берклі установлює мінімальні професійні стандарти роботи з відкритими цифровими даними за п'ятьма напрямами — виявлення (identification), збирання (collection), збереження (preservation), верифікація (verification) та аналіз (analysis), так, щоб матеріали зберігали доказову цінність [62; 63].

Методичний інструментарій документування спирається на техніки, розглянуті в підрозділі 3.3, але з посиленими вимогами. Геолокація (зіставлення орієнтирів із картами, супутниковими знімками та панорамами тощо) і хронолокація (визначення часу за тінями, погодою, сезоном і т.д.) дають змогу прив'язати матеріал до конкретного місця й часу. Для захоплення контенту з наперед вбудованими верифікованими метаданими та захищеним ланцюгом забезпечення збереження застосовують спеціалізовані рішення – зокрема застосунок eyeWitness to Atrocities, створений Міжнародною асоціацією юристів (IBA), матеріали якого, за повідомленням IBA, використовуються в українських

судових провадженнях [122]. Значні масиви верифікованих інцидентів систематизують профільні організації – наприклад, проєкт «Eyes on Russia» Центру інформаційної стійкості та дослідницька спільнота Bellingcat [76]. Водночас діє ключове застереження розділу: найраніша знайдена копія не завжди є першоджерелом, а відсутність метаданих не є доказом маніпуляції, тому кожен елемент перевіряють за сукупністю незалежних ознак.

Підвищені вимоги до документування зумовлені тим, що зібрані матеріали можуть живити конкретні міжнародні провадження. Прокурор Міжнародного кримінального суду (МКС) відкрив розслідування ситуації в Україні 2 березня 2022 р. за зверненнями держав-учасниць, а 17 березня 2023 р. палата МКС видала ордери на арешт у зв'язку з незаконною депортацією та переміщенням українських дітей. Під егідою Агентства Європейського Союзу з питань співробітництва у сфері кримінального правосуддя (Євроюст) 25 березня 2022 р. створено Спільну слідчу групу (JIT, Joint investigation team) за участю України, Литви та Польщі, до якої згодом долучилися інші держави та МКС. 23 лютого 2023 р. запрацювала База даних доказів основних міжнародних злочинів (CICED) для захищеного зберігання й аналізу доказів, а в структурі Євроюсту сформовано Міжнародний центр з переслідування за злочин агресії проти України (ICPA) [83; 97; 120]. Саме тому матеріал, зібраний із порушенням методології, ризикує втратити доказову силу в таких процесах.

Для протидії організованій кіберзлочинності з цієї практики випливають три правила. По-перше, встановлення місця й часу зйомки (геолокація, хронолокація) і висновок про причетність конкретної особи – різні завдання: перше підтверджує обставини події, друге потребує окремих даних, що пов'язують особу з дією (цифрових слідів, показань, висновків експертів). По-друге, походження матеріалу та незалежність джерел встановлюють до того, як матеріал використовують для висновків. По-третє, контент зберігають у спосіб, що дає змогу перевірити його цілісність і обставини фіксації.

РОЗДІЛ 4. ШТУЧНИЙ ІНТЕЛЕКТ І ПРЕДИКТИВНА АНАЛІТИКА

4.1. Базові технології штучного інтелекту в правоохоронній діяльності

Організована кіберзлочинність функціонує як високотехнологічна індустрія, що застосовує автоматизацію, машинне навчання й генеративні моделі для масштабування атак. Відповіддю на це має бути не менш технологічний інструментарій правоохоронних органів. Концепція розвитку штучного інтелекту в Україні (схвалена розпорядженням Кабінету Міністрів України № 1556-р) [55] визначає ШІ як організовану сукупність інформаційних технологій для виконання складних комплексних завдань. У протидії кіберзлочинності практичне значення мають кілька базових технологій.

Таблиця 4.1.1. Базові технології ШІ та їх застосування

Технологія ШІ	*Дія*	*Приклади застосування у протидії кіберзлочинності*
Машинне навчання (ML)	навчається на даних, виявляє закономірності й аномалії	виявлення аномальної поведінки, прогнозування атак
Глибинне навчання (DL)	багаторівневі нейромережі для складних патернів	розпізнавання облич і номерних знаків, аналіз відео
Обробка природної мови (NLP)	аналіз тексту й мовлення	опрацювання перехоплених комунікацій, повідомлень у соцмережах і месенджерах
Комп’ютерний зір	аналіз зображень і відеоматеріалів	ідентифікація об’єктів, аналіз відеоспостереження
Графовий (мережевий) аналіз	моделює зв’язки між особами, подіями, пристроями, потоками	декомпозиція структури угруповання, виявлення критичних вузлів
Великі дані (Big Data)	збирання, зберігання й кореляція великих різнорідних масивів	аналіз у режимі, наближеному до реального часу

Генеративні моделі, які поліція застосовує для опрацювання інформації, можуть також використовуватися в кіберзлочинній діяльності. За їх допомогою зловмисники готують фішингові повідомлення різними мовами, створюють або модифікують шкідливий код, а також синтезують голос і відеозображення для

імітації реальних осіб. Для організованих груп це спрощує масштабування шахрайських кампаній. Ту саму схему можна адаптувати до різних аудиторій, змінюючи мову повідомлень і зміст звернень [124].

У роботі поліції такі матеріали потребують перевірки походження й контексту поширення. Наприклад, під час аналізу голосового повідомлення, надісланого нібито від імені керівника, варто з'ясувати, з якого облікового запису його надіслано, за яких обставин його отримав адресат і чи підтверджується зміст повідомлення незалежними відомостями. За можливості для дослідження використовують первинний файл, перевіряють доступні метадані та зіставляють матеріал з іншими даними про подію.

Для первинного аналізу правоохоронні органи можуть застосовувати інструменти виявлення ознак синтетичного або зміненого контенту. Результат автоматизованої перевірки допомагає визначити, які матеріали потребують поглибленого дослідження. Оскільки такі інструменти можуть помилково позначити справжній матеріал або пропустити синтетичний, фахівець оцінює їхні результати разом із відомостями про походження файлу та іншими матеріалами справи.

4.2. Аналітичні платформи та технології великих даних

Аналітична платформа – це програмно-апаратний комплекс, що інтегрує збирання, нормалізацію, зберігання, аналіз і візуалізацію даних із різних джерел. Принципова відмінність платформ нового покоління – вбудовані модулі ШІ, які автоматизують виявлення закономірностей, аномалій і прихованих зв'язків, недоступних людині в розумні строки. Такі системи здатні аналізувати поведінку користувачів і пристроїв, визначати аномалії в мережевому трафіку, ідентифікувати шкідливе ПЗ, а в окремих випадках й автоматично блокувати загрози, що особливо важливо для захисту об'єктів критичної інфраструктури.

Окремим напрямом є використання великих мовних моделей для автоматизованого реферування великих обсягів документів, попереднього аналізу перехоплених комунікацій, перекладу багатомовних матеріалів, підготовки проєктів аналітичних довідок і узагальнення судової практики. Це автоматизує повсякденні завдання та пришвидшує пошук. Проте прогнози й висновки таких систем мають використовуватися лише як один із факторів під час ухвалення рішення, а не як його єдина підстава.

Оскільки організована кіберзлочинність має мережеву, часто транснаціональну структуру, центральним аналітичним завданням є не фіксація окремих епізодів, а *декомпозиція структури* угруповання. Графовий аналіз у поєднанні з машинним навчанням дозволяє:

- будувати соціальні графи на основі даних про комунікації, транзакції, спільне використання інфраструктури (серверів, доменів, гаманців тощо);

- обчислювати метрики центральності, що вказують на організаторів, координаторів і критичні вузли, нейтралізація яких завдає угрупованню максимальної шкоди;

- виявляти приховані спільноти та посередників між осередками.

Додатково алгоритми зв'язування злочинів автоматизовано виявляють серійність (наприклад, належність розрізнених у часі й просторі епізодів одному угрупованню за збігами тактик, інструментів, інфраструктури і т.д.), а технології атрибуції атак з певним ступенем імовірності пов'язують атаки з відомими угрупованнями. Результати такого аналізу є орієнтуючою інформацією.

Транснаціональний характер організованої кіберзлочинності робить міжнародну взаємодію не допоміжним, а системним елементом протидії: інфраструктура зловмисників, потерпілі та цифрові докази нерідко перебувають у різних юрисдикціях. Тому провідні інституції розгорнули спеціалізовані платформи обміну даними, координації операцій і доступу до електронних доказів – на рівні Європолу, Інтерполу та національних агрегаторів даних про інциденти.

Ядром європейської системи є Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre, EC3), створений при Європолі у 2013 р. Центр зосереджений на кіберзалежних злочинах, протидії сексуальній експлуатації дітей і платіжному шахрайству, працює з «темною мережею», координує аналітичні проєкти та надає державам-членам операційну, стратегічну й експертну підтримку [84].

Платформа SIRIUS – спільний проєкт Європолу та Євроюсту, що діє як центр компетенції з транскордонного доступу до електронних доказів у ЄС. Допомагає правоохоронним і судовим органам та постачальникам послуг орієнтуватися у складному правовому полі отримання даних, що зберігаються в онлайн-сервісів, забезпечує обмін знаннями (настанови, навчання, інструменти) та співпрацю публічного й приватного секторів. SIRIUS обслуговує спільноту компетентних органів із понад 50 країн (усі держави ЄС і дедалі більше держав поза ЄС) – понад 8 500 компетентних органів і близько 220 постачальників послуг [85]. Водночас SIRIUS не є правовою підставою отримання даних: платформа надає методичну та інформаційну підтримку під час вибору належної процедури, а самі дані отримують через відповідний правовий механізм [85].

Система аналізу шкідливого програмного забезпечення Європолу (Europol Malware Analysis System/Solution, EMAS) – динамічне автоматизоване середовище для дослідження зразків шкідливого ПЗ. У контрольованій «пісочниці», що імітує комп'ютер-жертву, локальну мережу й частково підключення до інтернету, зразок запускають і спостерігають за його поведінкою, зокрема за спробами звернутися до керувальних (C2) серверів. Кожен зразок зіставляють із базою попередніх: спільні ознаки (наприклад, та сама C2-інфраструктура) виявляють зв'язки між атаками, а результати передають до оперативних систем Європолу (зокрема SIENA) для обміну з державами-членами [96].

Інтерпол забезпечує глобальну взаємодію насамперед через захищену систему поліцейського зв'язку I-24/7, що з'єднує національні центральні бюро країн-членів. У сфері кіберзлочинності діють спеціалізовані сервіси: майданчик обміну знаннями Cybercrime Knowledge Exchange (неполіцейський обмін відомостями про тенденції, профілактику, методики виявлення й розслідування) та централізований операційний хаб Cybercrime Collaborative Platform – Operation для координації глобальних правоохоронних операцій у захищених робочих просторах [72; 127].

У США функцію національного агрегатора даних про інциденти виконує Центр скарг на інтернет-злочини (Internet Crime Complaint Center, IC3) ФБР, створений у 2000 р. IC3 приймає та систематизує скарги громадян і організацій, які можуть передаватися федеральним, штатним, місцевим і міжнародним правоохоронним органам для розслідування, а узагальнені дані оприлюднює в щорічному звіті про інтернет-злочинність. За звітом IC3 за 2024 рік зафіксовано рекордні збитки від інтернет-злочинності – близько 16,6 млрд дол. США [98].

Правовою основою взаємодії є Угода про оперативне та стратегічне співробітництво між Україною та Європолом (підписана у 2016 р.) [86], а також доступ української поліції до системи Інтерполу I-24/7. Користування ресурсами Європолу та Інтерполу в межах угод про співробітництво суттєво розширює аналітичні можливості українських правоохоронців – від перевірки ідентифікаторів до участі у скоординованих транскордонних операціях. За даними звіту Департаменту кіберполіції Національної поліції України, лише у 2024 році українські поліцейські разом з іноземними колегами ініціювали та забезпечили участь у 17 міжнародних поліцейських операціях, що дали змогу нейтралізувати низку потужних хакерських об'єднань [11]. Показовим є приклад координованої Європолом операції 2024 року, що припинила діяльність учасника міжнародного хакерського угруповання, який скомпрометував близько 1,5 тис. акаунтів вебсервісу та розгорнув до 1 млн віртуальних машин для майнінгу криптовалюти.

Водночас обмін даними в усіх цих системах здійснюється виключно на законних підставах, із дотриманням вимог щодо захисту персональних даних і правил відповідних платформ. Міжнародні ресурси не замінюють національну аналітику, а посилюють її, забезпечуючи доступ до ширшого масиву перевірених даних і механізмів спільного реагування.

Національна поліція України вже застосовує системи розпізнавання облич і автоматичного розпізнавання номерних знаків (Automatic Number Plate Recognition, ANPR): відповідні модулі інтегрують у міські комплекси відеоспостереження, а розгортання мережі камер із функцією біометричної ідентифікації охоплює десятки тисяч пристроїв [2; 3]. Ці технології дають змогу встановлювати особу за зображенням, перевіряти транспорт за базами розшуку та автоматизувати виявлення інцидентів.

В умовах збройної агресії РФ Україні надано безоплатний доступ до технології розпізнавання облич американської компанії Clearview AI – її першим

почало використовувати Міністерство оборони у 2022 р. На момент надання доступу база Clearview AI налічувала понад 10 млрд зображень, зібраних із відкритих вебджерел. Технологію застосовують, зокрема, для ідентифікації загиблих (у тому числі за пошкодженими обличчями), встановлення причетних до злочинів осіб і перевірки осіб на блокпостах, виявлення та спростування дезінформації, а також для возз'єднання родин [121]. Це безпосередньо корелює із завданнями документування воєнних злочинів, встановлення причетних осіб і розшуку загиблих та зниклих безвісти.

Водночас Clearview AI є суперечливою технологією. Її базу сформовано шляхом масового автоматизованого збирання (скрапінгу) зображень із відкритих джерел без згоди осіб, що стало підставою для санкцій наглядових органів низки держав: зокрема, у 2024 р. орган із захисту даних Нідерландів наклав на компанію штраф у розмірі 30,5 млн євро (рішення від 16.05.2024, оприлюднене 03.09.2024); за даними нідерландського регулятора, база компанії містила понад 30 млрд фотографій, а в Італії ще у 2022 р. компанію оштрафовано на 20 млн євро [77; 104]. Для української практики це означає, що застосування подібних засобів має спиратися на законну підставу, бути пропорційним меті й узгоджуватися із законодавством про захист персональних даних та правами людини (див. Розділ 2).

Варто також приділити увагу вітчизняним розробкам: «Касандра» та «Безпечне місто». Система «Касандра» Міністерства юстиції України є прикладом із сфери пробації, а не поліцейської діяльності. Вона оцінює ймовірність повторного вчинення правопорушення: співробітник пробації відповідає на перелік запитань, а алгоритм нараховує бали й формує підсумкову оцінку (за шкалою від 0 до 97), автоматизуючи підготовку досудової доповіді про обвинуваченого [60]. За відкритими повідомленнями, йдеться про бальне (актуарне) оцінювання ризику за заздалегідь визначеними запитаннями; без технічної документації немає підстав стверджувати, що система використовує машинне навчання, тому її слід відрізняти від моделей, які самостійно навчаються на даних.

Комплекси «Безпечне місто» поєднують міське відеоспостереження з відеоаналітикою: окрім розпізнавання облич і номерних знаків із перевіркою за базами розшукуваних осіб і викрадених транспортних засобів, вони виявляють скупчення людей, залишені предмети, акти вандалізму та інші позаштатні ситуації, фіксуючи події для оперативного реагування [2].

Спільним застереженням для всіх цих засобів є те, що вони залишаються інструментами підтримки прийняття рішень, а не їх заміною. Результат автоматизованого розпізнавання чи оцінювання (ймовірний збіг облич, бальна оцінка ризику) потребує перевірки людиною за сукупністю незалежних даних, оскільки можливі хибні збіги та упередженість алгоритмів. Технічний збіг сам по собі не є доказом, а обробка біометричних і персональних даних має здійснюватися виключно на законних підставах.

Попри успіхи, впровадження ШІ в кіберполіції стримується системними проблемами:

- нестачею фахівців, які поєднують компетентності в інформаційній безпеці, аналізі даних і кримінальному процесі;
- технічною застарілістю обладнання;
- відсутністю уніфікованих методик;
- обмеженим фінансуванням.

Саме тому підготовка аналітиків у закладах вищої освіти системи МВС розглядається як стратегічний напрям.

4.3. Предиктивна аналітика: моделі, застосування та інструментарій

Предиктивна (прогнозна) аналітика – це сукупність методів статистичного аналізу, машинного навчання та інтелектуального аналізу даних для прогнозування ймовірності настання подій на основі історичних і поточних даних [1]. У поліцейській діяльності виокремлюють три базові моделі прогнозування.

Таблиця 4.3.1. Базові моделі предиктивного прогнозування

Модель	*Об'єкт / питання*	*Чутливість для прав людини*
Просторово-часове	де й коли ймовірні правопорушення (ділянки, об'єкти, час)	нижча (не спрямоване на конкретну особу)
Прогнозування суб'єктів	ризик вчинення чи повторного вчинення правопорушень конкретними особами або групами	найвища (профілювання особи)
Прогнозування віктимізації	потенційні жертви або вразливі об'єкти атак	помірна

Принципову відмінність має **просторово-орієнтоване** прогнозування порівняно з **персонально-орієнтованим**. Помилки першого призводять здебільшого до неоптимального розподілу патрульних ресурсів, а якщо попередні дані залежать від інтенсивності патрулювання, просторове прогнозування також може посилювати нерівномірність поліцейської уваги до окремих територій, тоді як персональне прогнозування спрямовує увагу поліції на конкретних осіб, які за визначенням є невинуватими у «спрогнозованих» щодо них діяннях. Тому воно значно чутливіше з погляду наслідків для прав людини – і саме тому AI Act забороняє прогнозування злочинної поведінки виключно на основі профілювання (див. підрозділ 4.4).

У протидії організованій кіберзлочинності предиктивна аналітика має специфічний зміст:

1) прогнозування кібератак на основі індикаторів компрометації та TTPs відомих угруповань;

2) виявлення аномалій у трафіку й журналах подій ще до настання шкідливих наслідків;

3) аналіз фінансових потоків – кластеризація адрес блокчейну, виявлення схем «міксування» та транзитних ланцюгів;

4) прогнозування розвитку самих угруповань (нові сервіси даркнету, ребрендинг ransomware-груп, міграція учасників).

Зарубіжний досвід застосування предиктивної аналітики засвідчує таке:

- ФБР США використовує ШІ для розпізнавання осіб на відео в реальному часі та прогнозування місця й часу злочину;
- поліція Великої Британії – для аналізу відкритих джерел з метою виявлення загроз національній безпеці;
- у Німеччині аналітичні системи опрацьовують фінансову інформацію, виявляючи ознаки відмивання, корупції та шахрайства.

Таблиця 4.3.2. Приклади зарубіжних систем предиктивного поліціювання

Система / досвід	*Країна*	***Що вимірювали / яке обмеження оцінки***
PredPol	США (Лос-Анджелес та інші міста)	розподіл патрульних ресурсів за прогнозом ділянок; оцінки ефекту ґрунтуються переважно на даних самих департаментів, незалежні оцінювання суперечливі; аудит 2019 р. у Лос-Анджелесі не дав змоги встановити вплив на злочинність [107]
PRECOBS	Німеччина	прогнозування повторних квартирних крадіжок; відповідність вимогам захисту даних не є показником ефективності, вплив на злочинність потребує окремого оцінювання
LASER	США (Лос-Анджелес)	зміна кількості насильницьких злочинів у пілотних районах за даними департаменту; аудит Генерального інспектора (2019) не дав змоги оцінити вплив програми через недоліки обліку даних [107] (див. також рамку «Strategic Subject List»)

Наведені в табл. 4.3.2 приклади описують переважно те, що вимірювали самі поліцейські департаменти, і не завжди підтверджені незалежними оцінюваннями. За систематичним оглядом науковців [106], шість із 161 відібраного дослідження (3,7 %) оцінювали застосування прогнозних моделей у реальній поліцейській

практиці, а 155 досліджень були ретроспективними [106]. Звідси точність прогнозу на історичних даних і вплив поліцейського втручання на злочинність слід оцінювати окремо. Наявних емпіричних доказів поки недостатньо, щоб стверджувати, що предиктивне поліціювання гарантовано знижує злочинність, тому впровадження таких систем має супроводжуватися власним доказовим оцінюванням. Модель SARA (Scanning, Analysis, Response, Assessment), яку нерідко згадують поряд із прогнозними системами, належить до методів проблемно-орієнтованої поліцейської діяльності: вона описує цикл виявлення й аналізу проблеми, реагування та оцінювання результатів і не передбачає окремого прогнозного модуля.

Не менш важливим є аналіз ризиків предиктивного підходу. Якщо алгоритм навчається на історичних даних із соціальними чи етнічними упередженнями, він відтворює й підсилює ці викривлення. Механізм має назву «петля зворотного зв'язку»: прогноз системи зумовлює посилене патрулювання певної території, що збільшує кількість зафіксованих там правопорушень, а нові дані «підтверджують» початковий прогноз. Перевірки програм у Чикаго [69] і Лос-Анджелесі [107] показали, що ризики пов'язані не лише з алгоритмами, а й з якістю та повнотою вхідних даних, порядком їх оновлення і тим, як результати використовують у поліцейській практиці. Звідси випливає, що аудиту має підлягати вся практика застосування системи, а не лише її програмний код.

ПРАКТИЧНИЙ КЕЙС. Strategic Subject List (Чикаго) – межі персонального прогнозування

Система охоплювала базу з майже 400 тис. осіб, яким на основі даних про затримання (а не про обвинувальні вироки) присвоювався бал ризику причетності до збройного насильства за шкалою 0–500 [69]. За результатами регресійного аналізу оприлюднених даних переліку бал ризику прогнозував расову або етнічну належність затриманої особи навіть з урахуванням просторових характеристик району [73]. Квазіекспериментальне оцінювання пілотної версії переліку 2013 р. (426 осіб) не виявило, що особи з переліку рідше за порівняльну групу ставали жертвами вбивств чи стрілянини; водночас їх частіше затримували у справах про стрілянину [118]. Ці висновки стосуються пілотної версії моделі. 1 листопада 2019 р. програму припинено [69]. Аудит Генерального інспектора Поліцейської комісії Лос-Анджелеса щодо подібної програми LASER показав, що серед осіб у базі «хронічних правопорушників», для яких аудиторам були доступні деталізовані розрахунки балів, 44 % мали нуль або одне затримання за насильницькі злочини [107].

4.4. Правові й етичні межі застосування штучного інтелекту

Застосування ШІ правоохоронними органами перебуває у сфері підвищеного правового ризику, бо безпосередньо стосується прав на приватність, захист

персональних даних, справедливий суд і презумпцію невинуватості. Європейським регуляторним орієнтиром для України є Регламент (ЄС) 2024/1689 (AI Act) [117], що запроваджує ризик-орієнтований підхід.

Серед ключових заборон AI Act для поліції можна виділити:

- заборону систем біометричної категоризації за чутливими ознаками та нецільового збирання зображень облич з інтернету чи камер відеоспостереження для створення баз розпізнавання;
- заборону дистанційної біометричної ідентифікації «в реальному часі» у загальнодоступних місцях для правоохоронних цілей, крім вичерпно визначених ст. 5(1)(h) випадків: цільового пошуку жертв викрадення, торгівлі людьми чи сексуальної експлуатації, а також зниклих осіб; відвернення конкретної, суттєвої та безпосередньої загрози життю або фізичній безпеці осіб чи реальної та наявної або реальної й передбачуваної загрози терористичного акту; встановлення місцезнаходження або особи підозрюваного у вчиненні кримінальних правопорушень, перелічених у додатку II до Регламенту, за які передбачено позбавлення волі на максимальний строк не менше чотирьох років. Таке використання за загальним правилом потребує попереднього дозволу судового органу або незалежного адміністративного органу, рішення якого є обов'язковим; у належно обґрунтованій невідкладній ситуації застосування може розпочатися без дозволу, якщо за ним звертаються без зволікання, щонайпізніше протягом 24 годин; у разі відмови застосування негайно припиняють, а дані, результати й вихідні дані, пов'язані з таким застосуванням, видаляють (ст. 5(3)). Таке використання можливе лише тоді, коли держава-член передбачила цю можливість і детальні правила в національному праві (ст. 5(5));
- заборону використовувати системи ШІ для оцінювання або прогнозування ризику вчинення фізичною особою кримінального правопорушення виключно на підставі профілювання цієї особи або оцінювання її особистісних рис і характеристик (ст. 5(1)(d) Регламенту (ЄС) 2024/1689 [117]). Ця заборона не поширюється на використання системи ШІ як допоміжного засобу під час оцінювання людиною можливої причетності особи до кримінальної діяльності, якщо така оцінка вже ґрунтується на об'єктивних і перевірюваних фактах, безпосередньо пов'язаних із цією діяльністю.

Сферу застосування Регламенту визначає його ст. 2: він охоплює, зокрема, постачальників, які вводять в обіг або в експлуатацію системи ШІ чи вводять в обіг моделі ШІ загального призначення в ЄС, незалежно від місця їх заснування; суб'єктів, які впроваджують системи ШІ та засновані або розташовані в ЄС; а також постачальників і суб'єктів впровадження з третіх держав у визначених випадках, коли результат роботи системи використовується в ЄС; Регламент не застосовується до систем, що використовуються виключно для військових цілей, оборони чи національної безпеки. Для України AI Act є орієнтиром гармонізації; правові підстави застосування ШІ Національною поліцією в Україні визначає українське законодавство – КПК, закони «Про Національну поліцію», «Про

оперативно-розшукову діяльність» і «Про захист персональних даних» [18; 47; 50; 51; 117].

Правомірність застосування біометричного розпізнавання доцільно оцінювати не за аналогією з іншими слідчими діями, а за самостійними критеріями: метою використання; законною підставою; необхідністю (чи недосяжна мета менш втручальними засобами); пропорційністю втручання; обсягом і категоріями опрацьовуваних даних; незалежною перевіркою результату людиною за первинними даними; порядком оскарження рішення. У праві ЄС опрацювання персональних даних компетентними органами з метою запобігання, розслідування, виявлення кримінальних правопорушень чи притягнення до відповідальності регулює Директива (ЄС) 2016/680: опрацювання біометричних даних для однозначної ідентифікації особи допускається лише за суворої необхідності, з належними гарантіями та, зокрема, якщо його дозволено правом ЄС чи держави-члена [74].

Регуляторні підходи інших юрисдикцій менш централізовані, але мають спільні риси. У США регулювання фрагментоване (каліфорнійський закон CCPA вимагає прозорості збирання даних; Міністерство юстиції рекомендує оцінювати потенціал упередженості алгоритмів). У Великій Британії застосування таких систем підпорядковане Закону про захист даних 2018 року, настановам Управління комісара з інформації (ICO) і рекомендаціям Національної ради шефів поліції. Спільний знаменник – принцип пропорційності: високоризикові технології спостереження можна впроваджувати лише за доведеної користі, що переважає втручання у права людини, тим більше що надані поліції повноваження вкрай важко відкликати.

Досвід окремих держав окреслює межі допустимого. Китайські системи тотального відеоспостереження й соціального рейтингу критикують за непрозорість алгоритмів і трансформацію технологій безпеки на засіб контролю над суспільством, несумісний із демократичними стандартами. Натомість литовський досвід застосування ШІ для виявлення дезінформації (система щоденно відстежує понад 10 000 матеріалів, а верифікацію здійснюють фахівці) ілюструє збалансовану модель «ШІ виявляє – людина перевіряє».

Національну правову основу застосування інтелектуальних технологій становлять Конвенція про кіберзлочинність, закони «Про основні засади забезпечення кібербезпеки України», «Про Національну поліцію» та «Про оперативно-розшукову діяльність», Стратегія кібербезпеки України й Концепція розвитку ШІ [15; 50; 51; 52; 53; 55]. Водночас спеціального нормативного регулювання застосування ШІ у правоохоронній діяльності бракує; у наукових публікаціях вітчизняні вчені пропонують доповнити статтю 25 Закону «Про Національну поліцію» правом застосовувати засоби ШІ для збору, обробки й аналізу інформації, а статтю 8 Закону «Про оперативно-розшукову діяльність» – правом застосовувати ШІ для роботи з оперативною інформацією, але за умови

одночасного закріплення гарантій (вичерпного переліку цілей, строків зберігання, аудиту алгоритмів, судового контролю тощо).

Етичний вимір концентрується навколо кількох ризиків:

- *алгоритмічної упередженості* (ШІ обробляє історичні дані, що можуть містити упередження);

- *проблеми «чорної скриньки»* (більшість нейромереж не пояснюють своїх рішень, тож ані слідчий, ані суд не можуть встановити, чому алгоритм визначив особу як причетну);

- *конфіденційності* (автоматизований аналіз трафіку чи відеоспостереження без правових підстав створює ризики масового стеження).

Важливо й те, що алгоритмічна справедливість не має суто технічного розв'язання: математично доведено, що різні формальні критерії справедливості не можуть бути задоволені одночасно за відмінних базових показників для різних груп [68; 105]. Тому вибір критерію справедливості є нормативним рішенням, яке має ухвалюватися прозоро й підлягати зовнішньому контролю, а не «зашиватися» розробником у код.

Узагальнюючи, інтеграцію ШІ-інструментів у службову діяльність доцільно будувати за алгоритмом, наведеним на рис. 4.4.1.



Рис. 4.4.1. Алгоритм інтеграції ШІ-інструментів

Документування застосування ШІ-інструмента охоплює версію моделі та дату її оновлення, встановлений поріг збігу, виявлені під час перевірки хибні збіги

та результати перевірки первинних даних, на яких ґрунтується рішення. Рішення за результатами ухвалює уповноважена особа або орган у порядку, визначеному законом.

Дослідження за опитуванням 316 працівників підрозділу огляду місця події поліції Абу-Дабі [61] побудувало регресійну модель, у якій оцінена результативність протидії злочинності пов'язувалася з упровадженням предиктивних технологій, спеціалізованою технічною підготовкою та колаборативним навчанням персоналу. В опитувальній моделі навчання персоналу було пов'язане з оціненою результативністю. Причинний ефект підготовки персоналу потребує перевірки в іншому дизайні дослідження.

РОЗДІЛ 5. ЦИФРОВІ СЛІДИ: ВИЯВЛЕННЯ, ЗБІР, АНАЛІЗ І ПРОЦЕСУАЛЬНЕ ЗАКРІПЛЕННЯ

5.1. Поняття цифрового сліду і цифрового доказу

Цифрові (електронні) сліди можна визначити як комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення [12]. Такі сліди мають три важливі властивості:

- вони містять інформацію про стан і результати роботи комп'ютерної системи;
- не можуть бути безпосередньо сприйняті органами чуття людини;
- завжди потребують інтерпретації за допомогою технічних засобів.

Через стрімку цифровізацію цифрові сліди нерідко стають єдиним можливим відображенням обставин правопорушення в електронному середовищі.

Принципово розмежовувати цифровий слід і доказ у кримінальному провадженні. Цифровий слід – це дані, потенційно пов'язані з подією. У кримінальному провадженні відомості з цифрового середовища можуть використовуватися в доказуванні, якщо їх отримано в порядку, встановленому КПК України, та подано через передбачене ним процесуальне джерело. Комп'ютерні дані за відповідних умов можуть належати до документів у розумінні ст. 99 КПК. Відомості про походження даних, спосіб їх отримання та цілісність потрібні для перевірки результату. Допустимість оцінюють за правилами КПК з урахуванням обставин отримання доказу [12; 18; 28]. Отже, слід розрізняти фактичні дані (відомості про обставини події), процесуальні джерела доказів (ст. 84 КПК: показання, речові докази, документи, висновки експертів) і носій інформації, на якому ці дані зберігаються. Порядок призначення та проведення судових експертиз визначає Інструкція, затверджена наказом Міністерства юстиції України № 53/5 [38].

Таблиця 5.1.1. Цифровий слід і доказ у кримінальному провадженні

Ознака	*Цифровий слід*	*Доказ у кримінальному провадженні*
Що це	дані, потенційно пов'язані з подією	фактичні дані, отримані в передбаченому КПК порядку (ч. 1 ст. 84 КПК)
Носій і форма	будь-який носій чи система, де дані зберігаються (пристрій, сервер, хмарний сервіс)	процесуальне джерело: показання, речові докази, документи (зокрема комп'ютерні дані за ст. 99 КПК), висновки експертів

Ознака	*Цифровий слід*	*Доказ у кримінальному провадженні*
Умова використання	виявлення та фіксація; відомості про походження, спосіб отримання та цілісність потрібні для подальшої перевірки	отримання в порядку КПК; кожний доказ оцінюють щодо належності, допустимості та достовірності, а сукупність доказів – щодо достатності та взаємозв'язку для прийняття відповідного процесуального рішення (ст. 94 КПК)
Значення	орієнтуюча інформація для висунення та перевірки версій	використання в доказуванні; оцінювання здійснюють уповноважені суб'єкти (слідчий, прокурор, слідчий суддя, суд) у межах своїх повноважень

Чинний КПК України не виокремлює електронні докази як самостійне процесуальне джерело. Це створює потребу закріплення дефініцій «електронних даних» та «електронного доказу» для єдності правозастосовної практики. Електронні дані можуть бути скопійовані на інші носії без зміни їхнього змісту. Гешування дає змогу перевіряти їхню цілісність шляхом порівняння геш-значень, обчислених під час первинної фіксації та на подальших етапах роботи. Автентичність установлюють за сукупністю відомостей про джерело, обставини створення й отримання даних, їхні метадані та документований порядок поводження з ними. Сам по собі збіг геш-значень не доводить автентичності даних або достовірності відображених у них подій.

Показовою в цьому контексті є постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29.03.2021 у справі № 554/5090/16-к [30]. Суд виходив з того, що електронний документ може існувати на різних носіях, а примірники, ідентичні за змістом, можуть розглядатися як оригінали. Тому електронна форма матеріалу і сам факт його існування на іншому носії не роблять його недопустимим. Водночас висновок суду не звільняє від перевірки походження матеріалу, способу його отримання та цілісності. Випадки, коли копії комп'ютерних даних, виготовлені із залученням спеціаліста, визнаються оригіналом документа (ч. 4 ст. 99 КПК), розглянуто в підрозділі 5.2.

5.2. Класифікація слідів і принцип волатильності

Цифрові сліди доцільно систематизувати за двома критеріями – місцем локалізації та стійкістю.

Таблиця 5.2.1. Класифікація цифрових слідів за місцем локалізації

Група	*Приклади*	*Особливість*
Локальні	файли та їх фрагменти, артефакти ОС і застосунків, журнали подій, історія браузерів, збережені сеанси месенджерів	містяться на кінцевих пристроях (комп'ютери, смартфони, накопичувачі, IoT)
Мережеві	логи серверів і мережевого обладнання, записи про з'єднання й трафік в операторів, сесії VPN, DNS-запити, метадані маршрутизації пошти	зберігаються обмежений строк
Хмарні	дані у хмарних сховищах, SaaS-сервісах, месенджерах і соцмережах	фізично розміщені на серверах постачальників, здебільшого за межами юрисдикції України
У публічних розподілених реєстрах	записи блокчейнів про криптовалютні транзакції	загальнодоступні й незмінювані, але потребують атрибуції адрес особам чи сервісам

За стійкістю розрізняють волатильні (енергозалежні) дані, що безповоротно зникають після вимкнення живлення, і неволатильні, які зберігаються тривалий час. Самостійну доказову цінність мають метадані – вони нерідко дозволяють установити обставини, які неможливо довести змістом самого файлу (наприклад, час і пристрій створення документа).

Ключове практичне правило випливає з різної стійкості даних: послідовність збирання має відповідати порядку волатильності (настанова IETF RFC 3227) [64] – першими фіксують найменш стійкі дані.

Порядок волатильності (від найменш стійких даних до найстійкіших) схематично можна представити наступним чином:

1. Вміст оперативної пам'яті, активні мережеві з'єднання, запущені процеси, ключі шифрування в пам'яті.
2. Тимчасові дані та поточний стан системи.
3. Дані на дисках і знімних носіях.
4. Віддалені системні журнали аудиту безпеки та резервні копії комп'ютерних систем.

Слідова картина діяльності організованих кіберзлочинних угруповань має особливості, що прямо впливають на алгоритми: розподілена інфраструктура

(орендовані сервери у різних юрисдикціях, bulletproof-хостинг), багаторівнева анонімізація (VPN, Tor, ланцюги проксі), наскрізне шифрування, розрахунки у криптовалютах із міксерами, автоматизоване знищення слідів.

Звідси маємо три практичні наслідки:

1. сліди навіть одного епізоду розпорошені між багатьма володільцями інформації у різних країнах;
2. вирішальне значення має чинник часу, бо дані про з'єднання зберігаються обмежений строк;
3. вилучення окремого пристрою рідко дає повну картину, тому збирання доказів планують як серію скоординованих дій щодо всіх вузлів інфраструктури угруповання.

Розкриємо зазначені положення детальніше. У справах про кіберзлочини практично вся доказова база має цифрову форму, а цифрові дані легко й часто безповоротно втрачаються. Головна особливість таких слідів у тому, що помилка на етапі збирання, як правило, вже не може бути виправлена: якщо дані зникли, їх неможливо «перезняти» вдруге. Тому обидва наведені правила стосуються того самого – чинника часу й незворотності втрати. Перше захищає дані, що зникають у момент вимкнення пристрою; друге – дані, що зникають у постачальника послуг, коли спливає строк їх зберігання.

Правило 1. Оцінювати ризики зміни стану увімкненого пристрою.

Що це означає. Частина даних у комп'ютері існує лише доти, доки він працює. Це так звані волатильні (енергозалежні) дані: вміст оперативної пам'яті (RAM), активні мережеві з'єднання, запущені процеси і, найважливіше, ключі шифрування, які система тримає в пам'яті. Щойно зникає живлення, зникають і вони, причому безповоротно.

Чому вимкнення особливо небезпечне за ознак шифрування? Сучасні засоби повнодискового шифрування (наприклад, BitLocker, VeraCrypt, LUKS) працюють так: поки пристрій увімкнений, а криптоконтейнер змонтований (відкритий), дані доступні у звичайному вигляді, бо ключ розшифрування завантажено в оперативну пам'ять. Але варто вимкнути живлення – ключ зникає з пам'яті, а диск знову перетворюється на суцільний масив зашифрованих даних, відновити доступ до якого без пароля чи ключа здебільшого неможливо. Образно кажучи, увімкнений зашифрований пристрій – це відчинений сейф. Вимкнення живлення рівнозначне зачиненню сейфа, ключ від якого залишився всередині.

Що робити на практиці. Зміна стану пристрою може призвести до втрати нестійких даних або ускладнити доступ до них. Спосіб збереження визначають з урахуванням стану пристрою, ризику втрати даних, безпеки та повноважень. Рішення і спричинені ним зміни документують. Такий підхід охоплює й ситуації, коли фіксація активної системи сама змінює її стан. Рекомендовану послідовність дій на місці наведено в підрозділі 5.3.

Це і є практичне втілення принципу волатильності (настанова IETF RFC 3227): першими фіксують найменш стійкі дані.

Правило 2. Діяти швидко щодо даних, які провайдери зберігають обмежений час.

Багато цінних слідів перебуває не на пристрої підозрюваного, а в постачальників послуг – операторів зв'язку, онлайн-сервісів, хостингів. Дані про з'єднання (журнали, IP-адреси, маршрути трафіку) вони зберігають лише обмежений строк, після чого автоматично видаляють або перезаписують. Тобто доказ може зникнути не через дії злочинця, а через звичайний регламент провайдера – просто тому, що сплив час.

Що таке запит про збереження? Термінове збереження спрямоване на запобігання втраті вже наявних даних: це ще не отримання даних, а їх «заморожування». Підставу, порядок і строк збереження визначають за нормами, застосовними до конкретного випадку. Для одержання даних окремо визначають належну процедуру й звертаються з урахуванням строку, на який дані збережено. Якщо застосовують тимчасовий доступ до речей і документів, керуються ст. 159–166 КПК України; п. 7 ч. 1 ст. 162 КПК визначає відомості, що належать до охоронюваної законом таємниці [18].

Якщо збережені комп'ютерні дані перебувають на території іншої держави – Сторони Конвенції про кіберзлочинність, їх термінове збереження може забезпечуватися за запитом відповідно до статті 29 Конвенції, зокрема за сприяння цілодобової контактної мережі 24/7, передбаченої статтею 35. Згідно з пунктом 7 статті 29, дані зберігають протягом щонайменше 60 днів, щоб запитуюча Сторона могла подати належний запит про їх пошук, доступ, арешт, інше забезпечення збереження або розкриття. Після отримання такого запиту збереження продовжується до ухвалення рішення щодо нього. Цей механізм слід відрізняти від передбаченого пунктом 2 статті 16 внутрішньодержавного збереження даних: воно здійснюється протягом необхідного строку, але не більше 90 днів, із можливістю подальшого поновлення відповідного розпорядження. Збереження даних саме по собі не означає надання доступу до них: їх отримання потребує окремої належної правової процедури [15; 119].

Другий додатковий протокол до Конвенції (CETS № 224) передбачає окремі механізми для різних категорій даних. Стаття 6 стосується запитів щодо реєстраційних даних доменних імен. Стаття 7 передбачає пряме направлення розпорядження постачальнику послуг на території іншої Сторони щодо визначених збережених відомостей про абонента. Стаття 8 передбачає звернення до іншої Сторони для виконання розпорядження про прискорене надання відомостей про абонента або даних про трафік. Статті 9 і 10 передбачають механізми для надзвичайних ситуацій. Статті 13 і 14 установлюють умови, гарантії та вимоги щодо захисту персональних даних. Протокол не встановлює універсального строку

зберігання даних, а положення ст. 16 Конвенції стосуються внутрішньодержавного збереження вже наявних даних [15; 119].

Механізми термінового збереження даних, міжнародної правової допомоги та співпраці через контактні пункти мережі 24/7 слід розрізняти за призначенням. Збереження забезпечує незмінність уже наявних даних, а їх отримання потребує окремого запиту в належній процедурі. Платформа SIRIUS надає практичну інформацію про політики постачальників і методичну підтримку, але не є самостійною правовою підставою для отримання даних [15; 85; 119].

Обидва правила спрямовані на запобігання втраті цифрових даних унаслідок припинення живлення пристрою або спливу строків їх зберігання постачальником послуг. Залучення спеціаліста визначається вимогами відповідної процесуальної процедури та потребою у спеціальних знаннях і навичках. Частина четверта статті 99 КПК України передбачає, що копії інформації, у тому числі комп'ютерних даних, які містяться у визначених цією нормою системах та їх невід'ємних частинах, виготовлені слідчим або прокурором із залученням спеціаліста, визнаються судом як оригінал документа [18]. Це положення не встановлює обов'язкової участі спеціаліста в усіх діях із цифровими даними. Для забезпечення можливості перевірки їх цілісності та походження необхідно належно документувати отримання, копіювання, зберігання й передання матеріалів; гешування застосовують як технічний засіб контролю незмінності даних.

5.3. Міжнародні стандарти та принципи роботи з цифровими доказами

Незалежно від виду слідів робота з цифровими доказами спирається на принципи, вироблені міжнародною практикою. Їх викладено, зокрема, в міжнародних стандартах ISO/IEC 27037:2012 (ідентифікація, збирання, отримання та збереження цифрових доказів) [100], ISO/IEC 27041:2015 (забезпечення придатності й адекватності методів розслідування інцидентів) [101], ISO/IEC 27042:2015 (аналіз та інтерпретація цифрових доказів) [102] і ISO/IEC 27043:2015 (принципи та процеси розслідування інцидентів) [103], а також у настановах INTERPOL для лабораторій цифрової криміналістики [99] і посібнику ENISA для першого реагування [78]. В Україні стандарт ISO/IEC 27037 прийнято як національний стандарт ДСТУ EN ISO/IEC 27037:2022 [9]. Стандарти мають рекомендаційний характер і визначають технічні умови перевірки даних; вимоги до отримання доказів і процесуального оформлення встановлює КПК України [18]. Основними є шість принципів:

- ✓ **законність** – кожна дія ґрунтується на нормі КПК та, за потреби, на судовому рішенні;
- ✓ **цілісність** – із моменту фіксації дані не можуть бути змінені; 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 доступу до носія та його передання від вилучення до суду;

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

✓ **мінімальне втручання** – обрання способу, який найменше змінює стан системи-джерела; якщо зміни неминучі, вони документуються.

Порушення встановленого законом порядку отримання даних оцінюють за правилами КПК щодо допустимості доказів. Можливість перевірити походження, цілісність і спосіб отримання даних ураховують під час оцінювання конкретного доказу. Відхилення від технічної настанови оцінюють за його впливом на перевірність матеріалу та з урахуванням вимог закону [18].

Описаний нижче алгоритм реалізують після внесення відомостей до ЄРДР у порядку ст. 214 КПК України (крім випадків, прямо передбачених законом), а за наявності умов, визначених ст. 615 КПК, – з урахуванням спеціального порядку досудового розслідування в умовах воєнного стану (див. підрозділ 2.4) [18].

Алгоритм виявлення цифрових слідів охоплює чотири етапи:

1. ***Аналіз первинної інформації про кіберінцидент*** (заява потерпілого, повідомлення CERT-UA, банків, результати ОРД, матеріали OSINT, дані іноземних партнерів тощо) – реконструкція механізму події та формування вихідного набору ідентифікаторів (вектор атаки, облікові записи, IP, домени, гаманці, зразки ПЗ, індикатори компрометації і т.д.).

2. ***Побудова карти джерел*** – перелік потенційних носіїв слідів (пристрої, сервери, дані операторів, хмарні сервіси, криптобіржі, публічні блокчейни тощо). Для кожного визначають володільця, юрисдикцію, ймовірний строк зберігання та процесуальну форму доступу. Джерела ранжують за волатильністю й ризиком знищення.

3. ***Невідкладне забезпечення збереження даних*** – вжиття заходів для збереження даних за наявності належної правової підстави; щодо іноземних сервісів – запити про термінове збереження через контактний пункт мережі 24/7 (ст. 29, 35 Конвенції про кіберзлочинність). Загальнодоступний контент фіксується оглядом із технічною фіксацією до можливого видалення. Для відкритої вебсторінки це огляд комп’ютерних даних за ст. 237 КПК з дотриманням вимог до протоколу та додатків до нього (ст. 104–107 КПК). Для закритих даних, що перебувають у володільця, окремо визначають належну підставу їх отримання, зокрема тимчасовий доступ до речей і документів у передбачених КПК випадках.

4. ***Планування скоординованого збирання*** – координація процесуальних дій щодо джерел, пріоритетність і правові підстави яких визначено в конкретному провадженні, синхронізація з міжнародними партнерами, розподіл спеціалістів і техніки, сценарії дій для типових ситуацій.

Особливої алгоритмізації потребує робота з волатильними даними безпосередньо на місці. Далі розглянемо рекомендовану послідовність дій слідчого спільно зі спеціалістом:

1. убезпечити обстановку: відсторонити присутніх від пристроїв, зафіксувати фото- й відеозйомкою стан техніки (екрани, підключені кабелі й накопичувачі, серійні номери);

2. оцінити ризики зміни стану увімкнених пристроїв: зміна стану пристрою може призвести до втрати нестійких даних або ускладнити доступ до них (зокрема за ознак повнодискового шифрування – BitLocker, VeraCrypt, LUKS). Спосіб збереження визначають з урахуванням стану пристрою, ризику втрати даних, безпеки та повноважень; за потреби спеціаліст знімає образ оперативної пам'яті, фіксує активні з'єднання, процеси та змонтовані криптоконтейнери. Рішення і спричинені ним зміни документують;

3. оцінити ризик дистанційної зміни даних і визначити спосіб їх збереження з урахуванням стану пристрою та можливих наслідків втручання (зокрема, чи потрібна ізоляція від мереж – режим польоту, екранувальні пакети Фарадея); зміну стану пристрою задокументувати [95];

4. вимкнені пристрої, як правило, не вмикати – їх досліджують у лабораторних умовах;

5. обрати спосіб копіювання з урахуванням типу джерела: для сумісного носія – побітовий образ із використанням засобів блокування запису; для інших джерел – доступний спосіб отримання даних у визначеному обсязі. Подальше дослідження здійснюють на робочій копії, а оригінал опечатують, якщо його вилучено;

6. обчислити геш-значення за стійким алгоритмом (наприклад, SHA-256) і зафіксувати в протоколі, який саме масив даних зафіксовано (образ носія, окремі файли, експорт), коли і яким засобом обчислено контрольне значення; збіг значень підтверджує незмінність зафіксованого масиву, але сам по собі не доводить автентичності даних;

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

8. започаткувати облік ланцюга зберігання: документують кожне передання носія, а також створення файлів і робочих копій, доступ до них і їх передання (від кого, кому, коли, з якою метою).

ВИСНОВКИ

Вивчення теоретико-правових засад, актуальних тенденцій і сучасних практик діяльності поліції у сфері протидії організованій кіберзлочинності дає змогу сформувати цілісне уявлення про природу цього явища та окреслити пріоритетні напрями підвищення спроможності правоохоронних органів.

1. Організована кіберзлочинність функціонує як мережа з розподілом ролей, ресурсів і залежностей, у якій модель «кіберзлочинність як послуга» відокремлює кримінальну ініціативу від технічної компетентності. Тому об'єктами впливу є не лише виконавці атак, а й брокери первинного доступу, адміністратори платформ, оператори інфраструктури, розробники шкідливого програмного забезпечення та фінансові посередники. Водночас надання послуги учасникам мережі саме по собі не встановлює обізнаності чи спільного умислу. Технічний, інфраструктурний, організаційний і персональний рівні атрибуції не утворюють послідовності, у якій висновок одного рівня автоматично переходить на інший. Відновлення діяльності може супроводжуватися ознаками наступності. Їх оцінюють з урахуванням незалежності джерел та альтернативних пояснень.

2. Запропонована модель поєднує встановлення ролей і залежностей у кіберзлочинній мережі, перевірку альтернативних пояснень та визначення законного способу отримання даних. Вона дає змогу планувати дії з урахуванням того, що вже встановлено, які висновки залишаються версіями і які відомості потрібно отримати для їх перевірки. Модель визначає п'ять етапів – від первинної оцінки події до рішення щодо втручання та оцінювання його наслідків, – відповідальних за кожен етап і умови переходу між ними (табл. 1.5.3); її ілюстрацію наведено на матеріалах операції проти Tycoon 2FA.

3. Результати OSINT і автоматизованої аналітики в цій моделі спрямовують подальшу перевірку. Значення конкретних матеріалів для доказування визначають із урахуванням їхнього походження, порядку отримання та можливості перевірки. Вимоги до отримання доказів та їх допустимості встановлює КПК України. Геш-значення використовують для перевірки цілісності цифрових даних. Походження матеріалу й послідовність дій із ним перевіряють за документами про його отримання, передання та зберігання. Результати систем штучного інтелекту, зокрема біометричного розпізнавання, потребують перевірки людиною за первинними даними; рішення за ними ухвалює уповноважена особа або орган у порядку, визначеному законом.

Розглянуті міжнародні операції ілюструють вплив на інфраструктурні та фінансові вузли кіберзлочинних мереж. Відкриті джерела переважно висвітлюють безпосередні результати таких втручань. Для оцінювання довгострокового ефекту потрібні зіставні дані про тривалість порушення роботи сервісів, повторну активність і результати подальших проваджень. Для проваджень, де дані зберігаються за кордоном, юрисдикцію, постачальника послуги та доступний

механізм збереження й отримання даних доцільно встановлювати на початковому етапі.

4. Емпіричну базу дослідження становлять відкриті офіційні повідомлення та аналітичні звіти, які нерівномірні за повнотою й переважно відображають безпосередні результати операцій. Модель обґрунтовано аналітично та проілюстровано окремими кейсами; її емпірична перевірка на матеріалах кримінальних проваджень не проводилася. Наведені в нарисі дані про ефективність предиктивних систем ґрунтуються переважно на оцінках самих поліцейських органів і потребують незалежного підтвердження.

Перспективними напрямами подальших наукових досліджень є емпірична перевірка запропонованої моделі на матеріалах кримінальних проваджень, розроблення методики кількісного оцінювання спроможностей організованих кіберзлочинних мереж і тривалості їх відновлення після правоохоронного втручання, обґрунтування пропозицій щодо законодавчого закріплення понять «електронні дані» та «електронний доказ» у КПК України, а також формування правових гарантій і процедур незалежного аудиту систем штучного інтелекту, що застосовуються в правоохоронній діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Багаутдінова М., Лунгол О. М. Прогнозування злочинності за допомогою методу нечіткої кластеризації С-середніх. Актуальні питання діяльності підрозділів кримінальної поліції : матеріали Всеукр. наук.-практ. конф. (Кропивницький, 14 квітня 2023 р.). Кропивницький : ДонДУВС, 2023. С. 268–270.

2. Безпечне місто: використання інтелектуальних технологій для громадської безпеки // УНІАН. URL: https://www.unian.ua/science/10088759-bezpechne-misto-vikoristannya-intelektualnih-tehnologiy-dlya-gromadskoji-bezpeki.html (дата звернення: 01.10.2026).

3. В Україні запрацює 50-тисячна мережа камер стеження з функцією розпізнавання облич // ThePage. URL: https://thepage.ua/ua/news/v-ukrayini-zapracyuyut-50-tis-kamer-stezhennya-z-funkciyeyu-rozpiznavannya-oblich-sho-vidomo (дата звернення: 02.10.2026).

4. Габорець О. А., Лунгол О. М. Кримінальний аналіз у діяльності правоохоронних органів: міжнародний досвід. Національні інтереси України. 2026. № 4 (21). С. 1177–1194. URL: https://surl.li/qqaocv (дата звернення: 12.10.2026).

5. Габорець О. А., Лунгол О. М. Соціальна інженерія як феномен інформаційного впливу в цифровому середовищі. Національні інтереси України. 2025. № 11 (16). С. 95–104. URL: https://surl.li/wldsho (дата звернення: 12.10.2026).

6. Габорець О., Лунгол О., Волобоєв А. Стратегічний кримінальний аналіз як інструмент прогнозування та запобігання злочинності. Центральноукраїнський вісник права та публічного управління. 2026. № 2. С. 47–54. URL: https://cuj.dnuvs.ukr.education/index.php/cuj/article/view/175 (дата звернення: 12.10.2026).

7. Гончарук О. М., Ісмайлов К. Ю. Кримінальний аналіз у системі правоохоронних органів України: поняття, мета й завдання. Правовий часопис Донбасу. 2023. № 2 (83). С. 3–9.

8. 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).

9. ДСТУ EN ISO/IEC 27037:2022. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, отримання та збереження цифрових доказів. Київ : ДП «УкрНДНЦ», 2022.

10. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. Аналітично-порівняльне правознавство. 2025. № 6, т. 2.

11. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : офіційний вебсайт / Департамент кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/ (дата звернення: 11.10.2026).

12. Коваленко А. В. Електронні сліди у кримінальному провадженні: поняття, властивості та види.

13. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України : навч. посіб. Львів : ЛьвДУВС, 2022. 416 с.

14. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108) від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 13.08.2026).

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

16. 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).

17. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 05.09.2026).

18. 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: 05.09.2026).

19. Лунгол О. М. Методологічні засади атрибуції суб'єктів гібридної агресії в національному кіберпросторі. Кібербезпека: освіта, наука, техніка. 2025. Вип. 2 (30). С. 74–82. DOI: 10.28925/2663-4023.2025.30.904.

20. Лунгол О. М., Габорець О. А. Інтегративний підхід у професійній підготовці фахівців для підрозділів кримінальної поліції. Перспективи та інновації науки. 2025. № 11 (57). С. 823–831. URL: https://surl.li/yozxgo (дата звернення: 12.10.2026).

21. Лунгол О. М., Габорець О. А. OSINT-технології в правоохоронній діяльності : навч. посіб. (мультимедійне видання). Кропивницький : Book Creator, 2023. 107 с.

22. Лунгол О. М., Габорець О. А., Тулінов В. С. Концептуальні основи розвитку кримінального аналізу як інструменту протидії злочинності в умовах воєнного стану. Актуальні питання у сучасній науці. 2026. № 5 (47). С. 2442–2455. URL: https://drive.google.com/file/d/1Q9ed3rdm3dsWbndb-8SeDVGvb2EqL14F/view (дата звернення: 12.10.2026).

23. Лунгол О. М., Габорець О. А., Тулінов В. С. Лінгвістичні аспекти ідентифікації маніпулятивного контенту в мережі Інтернет методами OSINT-аналізу. Вісник науки та освіти. 2026. № 3 (45). С. 1053–1066. URL: https://surl.lu/rembfl (дата звернення: 12.10.2026).

24. Лунгол О. М., Габорець О. А., Тулінов В. С., Суюсанов Л. І. Цифровий профайлінг та психологічна портретистика в сучасній оперативно-розшуковій діяльності: теоретико-прикладний аспект. Успіхи і досягнення у науці. 2026. № 3 (25). С. 291–301. URL: https://surl.li/deoxfr (дата звернення: 12.10.2026).

25. Макаринська А., Лунгол О. Modern digital technologies in criminal analysis. Актуальні питання діяльності підрозділів кримінальної поліції : матеріали Всеукр.

наук.-практ. конф. (Кропивницький, 14 квітня 2023 р.). Кропивницький : ДонДУВС, 2023. С. 357–360.

26. Манжай О. В. Поліцейська діяльність у кіберсфері : підручник / МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2024. 188 с.

27. Організація розкриття шахрайств, учинених в кіберпросторі : монографія / А. В. Шевчишен, М. Ю. Романов, А. О. Волобоєв, О. М. Лунгол, О. А. Габорець, С. В. Головкін ; за заг. ред. С. С. Вітвіцького. Київ : Алерта, 2023. 200 с.

28. 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.

29. 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: 10.24144/2307-3322.2025.92.4.26.

30. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29.03.2021 у справі № 554/5090/16-к (провадження № 51-1878кмо20). Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/96074938 (дата звернення: 21.09.2026).

31. Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора : Закон України від 03.03.2022 № 2109-IX. URL: https://zakon.rada.gov.ua/laws/show/2109-20#Text (дата звернення: 15.08.2026).

32. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 21.09.2026).

33. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції : Закон України від 03.03.2022 № 2110-IX. URL: https://zakon.rada.gov.ua/laws/show/2110-20#Text (дата звернення: 15.08.2026).

34. Про внесення змін до Кримінального кодексу України щодо підвищення боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 15.08.2026).

35. 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).

36. 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).

37. 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).

38. Про затвердження Інструкції про призначення та проведення судових експертиз та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз : наказ Міністерства юстиції України від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 05.09.2026).

39. 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).

40. 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).

41. Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text (дата звернення: 04.09.2026).

42. Про затвердження Порядку взаємодії суб’єктів національної системи реагування на кіберінциденти : 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).

43. 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).

44. Про затвердження Порядку міжвідомчого обміну 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: 04.09.2026).

45. Про затвердження Порядку оцінювання стану кіберзахисту систем та об’єктів критичної 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).

46. 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).

47. 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).

48. 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).

49. 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).

50. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 05.09.2026).

51. 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: 05.09.2026).

52. 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).

53. Про рішення Ради національної безпеки і оборони України від 14.05.2021 «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).

54. Про рішення Ради національної безпеки і оборони України від 15.10.2021 «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).

55. 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: 22.08.2026).

56. Розуменко О., Лунгол О. Аналіз розвідданих та розслідування злочинів. Актуальні питання діяльності підрозділів кримінальної поліції : матеріали Всеукр. наук.-практ. конф. (Кропивницький, 14 квітня 2023 р.). Кропивницький : ДонДУВС, 2023. С. 380–382.

57. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с. DOI: 10.32837/11300.27740.

58. Тулінов В. С., Габорець О. А., Лунгол О. М. Виявлення психологічних тригерів інформаційного простору засобами цифрової розвідки. Наукові інновації та передові технології. 2026. № 5 (57). С. 3091–3101. URL: https://surl.li/zckdfb (дата звернення: 12.10.2026).

59. 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).

60. Штучний інтелект допоможе уникнути повторних злочинів: Мін’юст запускає «Касандру» // Укрінформ. 13.09.2020. URL: https://www.ukrinform.ua/rubric-technology/3098629-stucnij-intelekt-dopomoze-uniknuti-povtornih-zlociniv-minust-zapuskae-kasandru.html (дата звернення: 11.10.2026).

61. 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. URL: https://journal.uthm.edu.my/index.php/IJSCET/article/view/15323 (дата звернення: 21.09.2026).

62. Berkeley Protocol on Digital Open Source Investigations : project webpage / Human Rights Center, UC Berkeley School of Law. URL: https://humanrights.berkeley.edu/projects/berkeley-protocol-on-digital-open-source-investigations/ (дата звернення: 11.10.2026).

63. 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 (OHCHR) ; Human Rights Center, UC Berkeley School of Law, 2022. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf (дата звернення: 11.09.2026).

64. Brezinski D., Killalea T. Guidelines for Evidence Collection and Archiving : RFC 3227. IETF, 2002. URL: https://www.rfc-editor.org/rfc/rfc3227 (дата звернення: 21.08.2026).

65. Cellebrite Inseyets : FAQ / Cellebrite DI Ltd. 2024. URL: https://media.cellebrite.com/wp-content/uploads/2024/10/Cellebrite-Inseyets-FAQ.pdf (дата звернення: 11.10.2026).

66. Cellebrite Press Kit / Cellebrite DI Ltd. 2020. URL: https://cellebrite.com/wp-content/uploads/2020/09/Cellebrite-Press-Kit.pdf (дата звернення: 21.08.2026).

67. Cellebrite UFED. The Industry Standard for Lawfully Accessing and Collecting Digital Data : official webpage / Cellebrite DI Ltd. URL: https://cellebrite.com/en/ufed/ (дата звернення: 11.10.2026).

68. Chouldechova A. Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments. Big Data. 2017. Vol. 5, No. 2. P. 153–163. DOI: 10.1089/big.2016.0047.

69. City of Chicago Office of Inspector General. Advisory Concerning the Chicago Police Department’s Predictive Risk Models. Chicago, 2020. URL: https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf (дата звернення: 21.11.2026).

70. Computer Forensics Tool Testing Program (CFTT) : official webpage / National Institute of Standards and Technology. URL: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt (дата звернення: 21.09.2026).

71. Council of Europe Treaty Office. Chart of Signatures and Ratifications of Treaty 224: Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence. URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (дата звернення: 20.08.2026).

72. Cybercrime Collaboration Services (Cybercrime Knowledge Exchange; Cybercrime Collaborative Platform – Operation) : official webpage / INTERPOL. URL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services (дата звернення: 11.10.2026).

73. 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. 2023.

74. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Official Journal of the EU. 2016. L 119. P. 89–131. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj (дата звернення: 21.09.2026).

75. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive). Official Journal of the EU. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 11.09.2026).

76. Disinformation & Denial: Russia's Attempts to Discredit Open Source Evidence of Bucha : report / Centre for Information Resilience, Eyes on Russia. URL: https://www.info-res.org/eyes-on-russia/reports/disinformation-denial-russias-attempts-to-discredit-open-source-evidence-of-bucha/ (дата звернення: 11.10.2026).

77. Dutch Supervisory Authority Imposes a Fine on Clearview Because of Illegal Data Collection for Facial Recognition : news / European Data Protection Board. 2024. URL: https://www.edpb.europa.eu/news/dutch-supervisory-authority-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for_en (дата звернення: 21.08.2026).

78. ENISA. Electronic Evidence — A Basic Guide for First Responders. Heraklion : ENISA, 2015. URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (дата звернення: 21.08.2026).

79. ENISA. ENISA Threat Landscape 2025. Version 1.3, 22.09.2026. Athens : European Union Agency for Cybersecurity, 2026. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення: 24.09.2026).

80. ENISA. ENISA Threat Landscape 2026. Athens : European Union Agency for Cybersecurity, 2026. DOI: 10.2824/0806036. URL: https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf (дата звернення: 24.09.2026).

81. Eurojust. Cryptocurrency Money Laundering Site Shut Down Thanks to Coordinated Investigation. 11.06.2026. URL: https://www.eurojust.europa.eu/news/cryptocurrency-money-laundering-site-shut-down-thanks-coordinated-investigation (дата звернення: 01.10.2026).

82. Eurojust. Fraudulent Call Centres in Ukraine Rolled Up : press release. 16.12.2025. URL: https://www.eurojust.europa.eu/news/fraudulent-call-centres-ukraine-rolled (дата звернення: 13.08.2026).

83. Eurojust: One Year of Judicial Support for Ukraine (Joint Investigation Team; Core International Crimes Evidence Database, CICED; International Centre for the Prosecution of the Crime of Aggression, ICPA) // eucrim — The European Criminal Law Associations' Forum. 2023. URL: https://eucrim.eu/news/eurojust-one-year-of-judicial-support-for-ukraine/ (дата звернення: 11.10.2026).

84. European Cybercrime Centre (EC3) : official webpage / Europol. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення: 11.10.2026).

85. Europol and Eurojust Launch Phase 3 of the SIRIUS Project to Enhance Cross-Border Access to Electronic Evidence : news / Eurojust. 15.01.2025. URL: https://www.eurojust.europa.eu/news/europol-and-eurojust-launch-phase-3-sirius-project-enhance-cross-border-access-electronic-evidence (дата звернення: 11.10.2026).

86. Europol and Ukraine Sign Agreement to Tackle Cross-Border Crime : news / Europol. URL: https://www.europol.europa.eu/newsroom/news/europol-and-ukraine-sign-agreement-to-tackle-cross-border-crime (дата звернення: 11.10.2026).

87. 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 (дата звернення: 15.09.2026).

88. 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 (дата звернення: 15.09.2026).

89. 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 (дата звернення: 15.09.2026).

90. 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 (дата звернення: 13.09.2026).

91. 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 (дата звернення: 15.08.2026).

92. 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 (дата звернення: 01.09.2026).

93. FATF. Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs. Paris : Financial Action Task Force, 2026. URL:

https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html (дата звернення: 01.10.2026).

94. 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 (дата звернення: 11.09.2026).

95. Guidelines on Mobile Device Forensics : NIST Special Publication 800-101. Revision 1 / R. Ayers, S. Brothers, W. Jansen. Gaithersburg, MD : National Institute of Standards and Technology, 2014. 85 p. DOI: 10.6028/NIST.SP.800-101r1. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-101r1.pdf (дата звернення: 02.10.2026).

96. How Europol Analyzes Malware (Europol Malware Analysis System, EMAS) // Help Net Security. 02.12.2015. URL: https://www.helpnetsecurity.com/2015/12/02/how-europol-analyzes-malware/ (дата звернення: 01.10.2026).

97. ICC Judges Issue Two Arrest Warrants in the Context of the Situation in Ukraine, 17 March 2023 / Coalition for the International Criminal Court. URL: https://coalitionfortheicc.org/node/3447 (дата звернення: 04.10.2026).

98. Internet Crime Complaint Center (IC3): Annual Reports; 2024 Internet Crime Report / Federal Bureau of Investigation. URL: https://www.ic3.gov/AnnualReport/Reports (дата звернення: 05.10.2026).

99. INTERPOL. Global Guidelines for Digital Forensics Laboratories. Lyon : INTERPOL, 2019. URL: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf (дата звернення: 22.09.2026).

100. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva : ISO, 2012.

101. ISO/IEC 27041:2015. Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method. Geneva : ISO, 2015. URL: https://www.iso.org/standard/44405.html (дата звернення: 21.07.2026).

102. ISO/IEC 27042:2015. Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. Geneva : ISO, 2015. URL: https://www.iso.org/standard/44406.html (дата звернення: 21.07.2026).

103. ISO/IEC 27043:2015. Information technology — Security techniques — Incident investigation principles and processes. Geneva : ISO, 2015. URL: https://www.iso.org/standard/44407.html (дата звернення: 21.07.2026).

104. Italy Slaps Facial Recognition Firm Clearview AI with €20 Million Fine // Engadget. 2022. URL: https://www.engadget.com/italy-slaps-facial-recognition-firm-clearview-ai-with-20-million-euro-fine-212500675.html (дата звернення: 11.10.2026).

105. Kleinberg J., Mullainathan S., Raghavan M. Inherent Trade-Offs in the Fair Determination of Risk Scores. 8th Innovations in Theoretical Computer Science Conference (ITCS 2017). Wadern : Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. Art. 43. P. 43:1–43:23. DOI: 10.4230/LIPIcs.ITCS.2017.43.

106. 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: 10.1080/24751979.2024.2371781.

107. Los Angeles Police Commission. Office of the Inspector General. Review of Selected Los Angeles Police Department Data-Driven Policing Strategies. Los Angeles, 2019. URL: https://www.oig.lacity.org/_files/ugd/b2dd23_21f6fe20f1b84c179abf440d4c049219.pdf (дата звернення: 20.09.2026).

108. Magnet Axiom : official webpage / Magnet Forensics. URL: https://www.magnetforensics.com/products/magnet-axiom/ (дата звернення: 03.10.2026).

109. Magnet Forensics Inc. Enters Into Definitive Agreement to be Acquired by Thoma Bravo : press release / Thoma Bravo. 20.01.2023. URL: https://www.thomabravo.com/press-releases/magnet-forensics-inc.-enters-into-definitive-agreement-to-be-acquired-by-thoma-bravo (дата звернення: 02.10.2026).

110. Magnet GrayKey : official webpage / Magnet Forensics. URL: https://www.magnetforensics.com/products/magnet-graykey/ (дата звернення: 01.10.2026).

111. Marlinspike M. Exploiting Vulnerabilities in Cellebrite UFED and Physical Analyzer from an App’s Perspective : blog / Signal. 21.04.2021. URL: https://signal.org/blog/cellebrite-vulnerabilities/ (дата звернення: 20.09.2026).

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

113. OSINT Open Source Intelligence. Інструменти та методи : навч. посіб. / 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.

114. 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.

115. Pashniev D. V., Shmatkov D. I., Kolomiitsev S. O. et al. AI and OSINT Tools and Methods for Tracing Missing, Deported or Forcibly Displaced Children. Kharkiv : MIA of Ukraine ; KhNUIA, 2024. 80 p.

116. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. Official Journal of the EU. 2023. L 191. P. 118–180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj (дата звернення: 20.08.2026).

117. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act). Official Journal of the EU. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 07.09.2026).

118. Saunders J., Hunt P., Hollywood J. S. Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot. Journal of Experimental Criminology. 2016. Vol. 12, No. 3. P. 347–371. DOI: 10.1007/s11292-016-9272-0.

119. 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 (дата звернення: 23.08.2026).

120. Statement of ICC Prosecutor Karim A. A. Khan QC on the Situation in Ukraine: Receipt of Referrals from States Parties and Opening of an Investigation, 2 March 2022 / International Criminal Court. URL: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-qc-situation-ukraine-receipt-referrals-39-states (дата звернення: 02.10.2026).

121. Ukraine Has Started Using Clearview AI's Facial Recognition During War // CNBC (Reuters). 13.03.2022. URL: https://www.cnbc.com/2022/03/13/ukraine-has-started-using-clearview-ais-facial-recognition-during-war.html (дата звернення: 03.10.2026).

122. Ukrainian Court Cases Rely on Footage Captured with the IBA-Founded eyeWitness to Atrocities App / International Bar Association. URL: https://www.ibanet.org/Ukrainian-court-cases-rely-footage-captured-IBA-founded-eyeWitness-to-Atrocities-app (дата звернення: 01.10.2026).

123. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (New York, 24.12.2024) : status / United Nations Treaty Collection, Chapter XVIII, 16. URL: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18 (дата звернення: 21.09.2026).

124. 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.pdf (дата звернення: 26.08.2026).

125. UNODC. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. Vienna : United Nations Office on Drugs and Crime, 2025. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf (дата звернення: 01.10.2026).

126. UNODC. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia.

Vienna : United Nations Office on Drugs and Crime, 2024. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (дата звернення: 17.08.2026).

127. What is INTERPOL? (I-24/7 Global Police Communications System) : official webpage / INTERPOL. URL: https://www.interpol.int/en/Who-we-are/What-is-INTERPOL (дата звернення: 03.10.2026).

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

Наукове видання

ЛУНГОЛ Ольга Миколаївна

ГАБОРЕЦЬ Ольга Андріївна

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

Науковий нарис