МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КРИМІНАЛЬНИЙ АНАЛІЗ І КІБЕРБЕЗПЕКА: ОБ'ЄДНАННЯ ЗУСИЛЬ ДЛЯ НОВИХ ВИКЛИКІВ

Матеріали
науково-практичної конференції

22 травня 2026 року

Одеса
2026

УДК 343.9(477)

Матеріали подано в авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, галузевої термінології, інших відомостей.

Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів: збірник тез науково-практичної конференції (22 травня 2026 р.). Одеса : ОДУВС, 2026. 372 с.

Збірник містить тези доповідей учасників Міжнародної науково-практичної конференції «Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів» , яка відбулася 22 травня 2026 року в Одеському державному університеті внутрішніх справ.

УДК 343.9(477)

Шановні учасники конференції!

Щиро вітаю вас з нагоди відкриття науково-практичної конференції «Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів».

Сьогодні ми зібралися для обговорення надзвичайно важливих питань, які мають стратегічне значення для безпеки держави, розвитку правоохоронної системи та захисту інформаційного простору України. В умовах воєнного стану, стрімкої цифровізації суспільства та постійного зростання кіберзагроз питання кримінального аналізу й кібербезпеки набувають особливої актуальності.

Сучасні виклики вимагають від нас не лише оперативного реагування, а й системного підходу до виявлення, аналізу та попередження загроз. Кіберзлочинність стає дедалі більш організованою, технологічною та транснаціональною, а тому ефективна протидія їй неможлива без поєднання наукового потенціалу, практичного досвіду та сучасних аналітичних інструментів.

Особливого значення сьогодні набувають розвиток кримінального аналізу, впровадження технологій OSINT, використання можливостей штучного інтелекту, Великі дані та цифрової аналітики. Саме ці напрями формують нові підходи до забезпечення кіберстійкості держави, захисту критичної інфраструктури та підвищення ефективності правоохоронної діяльності.

Переконаний, що наша конференція стане важливою платформою для професійного діалогу, обміну досвідом, науковими напрацюваннями та практичними рішеннями. Лише спільними зусиллями науки, освіти, державних інституцій і фахівців-практиків ми зможемо сформувати ефективні механізми реагування на новітні загрози та виклики.

Одеський державний університет внутрішніх справ пишається тим, що є майданчиком для професійного діалогу між наукою, освітою та практикою. Ми впевнені, що результати вашої роботи матимуть практичне значення та сприятимуть підвищенню рівня безпеки в нашій країні.

Бажаю всім учасникам конференції плідної роботи, змістовних дискусій, нових професійних контактів, успішної реалізації ідей та вагомих результатів, які матимуть практичне значення для зміцнення безпеки нашої держави.

ДАВИДЕНКО В'ячеслав Віталійович

ректор Одеського державного університету внутрішніх справ
кандидат юридичних наук, доцент, полковник поліції

СЕКЦІЯ 1.
ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ

ГЕОІНФОРМАЦІЙНИЙ АНАЛІЗ ЗЛОЧИННОСТІ

Антонюк Віолетта Олександрівна
здобувачка вищої освіти
Інститут права та безпеки
Одеський державний університет внутрішніх справ
Науковий керівник: ***Грезіна Олена Миколаївна***
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

Геоінформаційний аналіз злочинності — це сучасний інструмент правоохоронної діяльності, який використовує геоінформаційні системи (ГІС) для візуалізації, аналізу та просторового моделювання злочинів [1;2;3]. Він дає змогу відображати правопорушення на карті, виявляти приховані закономірності та «гарячі точки» злочинності (hot spots), що є критично важливим для розуміння динаміки злочинності та її географічних особливостей [2]. Застосування crime mapping дозволяє не лише фіксувати місця злочинів, а й аналізувати зв'язки з демографічними, інфраструктурними та соціально-економічними характеристиками території.

У сучасному кримінальному аналізі використовується цілий ряд спеціалізованих ГІС-методів, які можна поділити на три ключові групи. Аналіз «гарячих точок» використовує методи (наприклад, ядрове оцінювання щільності, Кет), щоб візуалізувати місця найвищої концентрації злочинів. Це дозволяє визначити зони, де необхідно посилити патрулювання або вжити профілактичних заходів. Аналіз просторово-часових закономірностей, який досліджує, як і чи швидко злочини можуть повторюватися поблизу вже існуючих інцидентів. Це допомагає прогнозувати періоди підвищеного ризику для швидкого реагування. Моделювання ризику та факторів середовища, що вивчає вплив характеристик місцевості

на рівень злочинності. Аналізуються об'єкти, що можуть створювати криміногенне середовище, як-от зупинки громадського транспорту, школи, заклади нічного відпочинку чи продуктові магазини [1]. Експерти наголошують, що найбільш потужною аналітика стає саме при комбінуванні цих методів, що дає комплексну картину ризиків для прийняття стратегічних і тактичних рішень. Для реалізації цих завдань існує спеціалізоване програмне забезпечення, яке використовують правоохоронні органи світу. ArcGIS від Esri —галузевий стандарт, який надає повний набір інструментів для управління даними, аналізу шаблонів і створення карт. QGIS — популярна безкоштовна альтернатива з відкритим кодом, що має спеціалізовані інструменти для роботи в полі через мобільний додаток QField. CrimeStat — це безкоштовна програма, яка спеціалізується саме на просторовій статистиці для аналізу місць скоєння злочинів.

Робота зі створення карт злочинності — це не просто нанесення точок на мапу, а цілісний аналітичний процес, в якому можна виокремити такі ключові етапи: збір та підготовка, що включає в собі отримання даних про злочини (координати, адреси) та геопросторових даних (мапи вулиць, межі дільниць). Геокодування , а саме перетворення текстових адрес у географічні координати (широта/довгота) для нанесення на карту [3]. Важливо для точності майбутнього аналізу. Візуалізація - створення точкових мап, хороплетів (райони з кольоровим градієнтом) або теплових карт (kriging). Аналіз та моделювання – використання статистичних методів для виявлення «гарячих точок», оцінки ризиків кореляції тощо, що часто слугує базою для прогнозної поліцейської діяльності (predictive policing). Інтерпретація - перетворення отриманих даних у конкретні висновки та практичні рекомендації для патрулювання та профілактики, представлені у вигляді зрозумілих звітів чи дашбордів [2;3].

Геоінформаційний аналіз злочинності (crime mapping) є не просто допоміжним інструментом картографування, а фундаментальним методологічним підходом до розуміння просторової природи правопорушень [1;3]. Інтеграція ГІС у кримінальний аналіз дозволяє перейти від пасивної реєстрації інцидентів до активної, прогностичної моделі роботи поліції. Як показують матеріали посібників та практичних кейсів, використання методів виявлення

«гарячих точок», аналізу просторово-часових закономірностей та моделювання факторів середовища забезпечує підвищення ефективності розподілу patrol resources та швидкості реагування, обґрунтованість стратегічних рішень у сфері профілактики злочинності, прозорість діяльності правоохоронних органів перед громадськістю [3]. Водночас успішність його застосування безпосередньо залежить від подолання існуючих викликів — насамперед, забезпечення високої якості первинних даних, дотримання вимог конфіденційності та підвищення кваліфікації аналітиків [2;4].

Список використаних джерел:

1. Калякін С. В., Міхтєєв Д. Д. Сучасні інформаційні технології в діяльності поліції: ГІС, аналіз злочинності та predictive policing. 2025. URL: dspace.univd.edu.ua

2. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с. URL: dspace.lvduvs.edu.ua

3. Gorr W. L., Kurland K. S. GIS Tutorial for Crime Analysis. Redlands, Calif. : ESRI Press, 2012. 272 p. URL: cartographicperspectives.org

4. Kannan M., Singh M. Geographical Information System and Crime Mapping. Taylor & Francis Group, 2020. URL: Taylor & Francis

ТРАНСФОРМАЦІЯ СИСТЕМИ КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ: ІНСТИТУЦІЙНИЙ РОЗВИТОК, МІЖНАРОДНА ІНТЕГРАЦІЯ ТА ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Бутко Роман Юрійович
начальник Департаменту кримінального аналізу Національної поліції України, полковник поліції

Сучасний етап розвитку правоохоронної системи України характеризується суттєвим посиленням ролі кримінального аналізу як ключового інструменту забезпечення оперативно-розшукової діяльності, стратегічного планування та протидії злочинності в умовах гібридних загроз і воєнного стану. Важливим фактором цього процесу

є системна взаємодія закладів вищої освіти системи МВС України з практичними підрозділами Національна поліція України, що дозволяє формувати нове покоління аналітиків, здатних працювати в умовах високої динаміки криміногенного середовища.

Кримінальний аналіз в Україні поступово інтегрується у міжнародний професійний простір. Представники аналітичних підрозділів беруть активну участь у заходах Міжнародної асоціації кримінальних аналітиків у США та європейських професійних форумах, що сприяє обміну методологіями, стандартизації підходів та адаптації кращих практик до національних умов. Така інтеграція забезпечує не лише підвищення професійного рівня, але й формує визнання української школи кримінального аналізу на міжнародному рівні.

За останнє десятиліття у співпраці з закладами вищої освіти системи МВС України сформовано розгалужену мережу фахівців кримінального аналізу, які функціонують на всіх рівнях Національна поліція України — від територіальних підрозділів до центрального апарату. Сьогодні аналітична служба налічує сотні підготовлених фахівців, що забезпечують безперервний цикл аналітичного супроводу оперативної діяльності. Паралельно відбувається інституційна трансформація служби, зокрема створення відділів оперативного моніторингу та підрозділів воєнної аналітики, що відповідає сучасним викликам національної безпеки.

Окремої уваги потребує впровадження цілодобового режиму аналітичного супроводу та розвиток системи ситуаційного аналізу в структурі Департаменту кримінального аналізу. У межах функціонування ситуаційного центру МВС України забезпечується координація аналітичних підрозділів, взаємодія з іншими правоохоронними органами та аналітична підтримка оперативних заходів у форматі 24/7. Важливим елементом є розробка типових алгоритмів реагування, що дозволяють забезпечити безперервний цикл від виявлення критичної інформації до її практичного використання в розкритті злочинів.

Суттєвим напрямом розвитку є цифровізація аналітичної діяльності, зокрема впровадження технологій відеоаналітики та систем обробки великих масивів відеоданих. Використання ліцензованих програмно-апаратних рішень дозволяє здійснювати ефективну обробку терабайтів відеоінформації, що значно підвищує

оперативність розслідувань. Окремим інноваційним кроком є створення інтегрованих систем доступу до мереж публічного відеоспостереження та формування національного реєстру камер системи «Безпечна країна», що розширює аналітичні можливості правоохоронних органів.

Паралельно з технічними інноваціями активно розвивається освітньо-методологічна база кримінального аналізу. Створення аналітичного навчального порталу на базі платформи MOODLE забезпечує накопичення, систематизацію та передачу знань, отриманих у практичній діяльності. Наразі платформа містить понад 130 навчальних курсів у 26 категоріях, що дозволяє поєднувати теоретичну підготовку з практичними кейсами та здійснювати регулярне тестування рівня компетентностей аналітиків.

Значним досягненням є також розвиток власних програмних рішень, зокрема системи оперативно-відомчого аналізу, яка забезпечує автоматизовану візуалізацію маршрутів руху об'єктів, облік відеокамер та інтеграцію аналітичних даних. Подібні інструменти формують нову архітектуру кримінального аналізу, орієнтовану на швидкість обробки інформації, міжвідомчу взаємодію та технологічну автономність.

Таким чином, сучасний етап розвитку кримінального аналізу в Україні характеризується комплексною трансформацією, що охоплює інституційний, освітній, міжнародний та технологічний виміри. Системна інтеграція з освітнім середовищем, розвиток цифрових інструментів та активна міжнародна співпраця формують підґрунтя для подальшого підвищення ефективності діяльності Національна поліція України у сфері протидії злочинності та забезпечення національної безпеки.

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Гайна Сергій Вікторович
курсант 202 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України
Науковий керівник: ***Калугін Володимир Юрійович***
професор кафедри кримінального аналізу
та інформаційних технологій, к.ю.н., доцент

Роль кримінального аналізу у протидії організованій злочинності в сучасних умовах набуває особливої актуальності у зв'язку з трансформацією форм і методів злочинної діяльності, її високим рівнем латентності, транснаціональним характером та активним використанням інформаційно-комунікаційних технологій. Організована злочинність становить складне соціально-правове явище, що характеризується стійкістю злочинних угруповань, ієрархічною структурою, розподілом ролей між учасниками та здатністю адаптуватися до змін у правовому полі та діяльності правоохоронних органів. У цих умовах традиційні методи протидії злочинності часто виявляються недостатньо ефективними, що обумовлює необхідність впровадження інноваційних підходів, серед яких ключове місце займає кримінальний аналіз. [1, с. 21].

Кримінальний аналіз являє собою комплексну діяльність, спрямовану на збір, обробку, оцінку та інтерпретацію інформації з метою прийняття управлінських та оперативних рішень, і є невід'ємною складовою сучасної правоохоронної діяльності, що забезпечує підвищення ефективності боротьби зі злочинністю шляхом використання аналітичних методів та інформаційних технологій [1, с. 34].

У свою чергу, кримінальний аналіз дозволяє прогнозувати розвиток злочинної діяльності та визначати пріоритетні напрями оперативно-розшукової роботи [2, с. 52].

Однією з ключових функцій кримінального аналізу є виявлення та документування зв'язків між учасниками організованих злочинних груп. Завдяки застосуванню сучасних аналітичних

методів, зокрема аналізу соціальних мереж, можливо встановити структуру злочинного угруповання, визначити його лідерів, координаторів та виконавців, а також виявити приховані зв'язки між окремими елементами кримінального середовища. Це, у свою чергу, створює передумови для більш точного планування оперативно-розшукових заходів та ефективного документування злочинної діяльності.

Сьогодні значно ускладнюється криміногенна ситуація, що зумовлює необхідність використання більш сучасних та ефективних аналітичних інструментів. Зокрема, важливу роль відіграє аналіз великих масивів даних, отриманих із різних джерел, включаючи відкриті джерела інформації (OSINT), бази даних правоохоронних органів, інформаційні системи та інші ресурси. [3].

Особливе значення у кримінальному аналізі має використання інформаційно-аналітичних продуктів, таких як аналітичні довідки, профілі злочинців, схеми зв'язків, кримінальні карти та інші візуалізаційні інструменти. Вони дозволяють наочно відображати отриману інформацію та забезпечують більш ефективне її використання у практичній діяльності підрозділів кримінальної поліції. Інформаційно-аналітична діяльність є основою сучасного управління у сфері правоохоронної діяльності та забезпечує формування обґрунтованих управлінських рішень [4, с. 239].

Особливе значення кримінальний аналіз має у протидії транснаціональній організованій злочинності, яка охоплює такі сфери, як торгівля людьми, незаконний обіг наркотичних засобів, відмивання доходів, одержаних злочинним шляхом, кіберзлочинність тощо. У цьому контексті аналітична діяльність забезпечує інтеграцію інформації з різних джерел, включаючи міжнародні бази даних, що дозволяє виявляти міждержавні зв'язки злочинних мереж та координувати зусилля правоохоронних органів різних країн.

Крім того, кримінальний аналіз виступає важливим інструментом інформаційного забезпечення кримінального провадження. Аналітичні продукти, такі як аналітичні довідки, профілі підозрюваних, часові та подієві діаграми, сприяють більш глибокому розумінню обставин кримінального правопорушення та підвищують якість доказової бази. Водночас результати кримінального аналізу можуть використовуватися для обґрунтування

процесуальних рішень, зокрема щодо обрання запобіжних заходів, проведення слідчих (розшукових) дій тощо.

Не менш важливою є прогностична функція кримінального аналізу, яка полягає у можливості передбачення розвитку злочинної ситуації на основі наявних даних. Використання методів математичного моделювання та машинного навчання дозволяє прогнозувати ймовірність вчинення злочинів у певних регіонах або певними групами осіб, що створює умови для своєчасного реагування та запобігання злочинній діяльності.

Список використаних джерел:

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

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

3. Білоус Р.В., Василинчук В.І., Таран О. В Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. Науковий вісник Національної академії внутрішніх справ. 2021. № 1 (118) С. 131-137

4.Калугін В.Ю. Використання інформаційних технологій під час розслідування кримінальних правопорушень. Матер. Міжнар. наук.-практ. конф., присв. 10-й річниці набуття чинності Кримінального процесуального кодексу України (м. Одеса, 9 грудня 2022 р.) / уклад.: Л. І. Аркуша, О. О. Торбас, В. А. Завтур ; Нац. ун-т «Одеська юридична академія». Одеса, 2022. С. 238-242.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Гайна Сергій Вікторович
здобувач вищої освіти 202 взводу Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України
(Одеський державний університет внутрішніх справ)
Форос Ганна Володимирівна
завідувачка кафедри кримінального аналізу та інформаційних технологій, к.ю.н., доцент
(Одеський державний університет внутрішніх справ)

Сучасний етап розвитку правоохоронної системи України характеризується підвищенням ролі інформаційно-аналітичного забезпечення діяльності підрозділів кримінальної поліції, особливо в умовах воєнного стану. Ефективна протидія злочинності, зокрема організованим її формам, безпосередньо залежить від якості збору, обробки, аналізу та використання інформації. Інформаційно-аналітична діяльність виступає ключовим елементом управлінських і оперативних процесів, оскільки забезпечує прийняття обґрунтованих рішень на основі систематизованих даних [1, с. 15].

Відповідно до Закону України «Про Національну поліцію», одним із основних завдань поліції є здійснення інформаційно-аналітичної діяльності з метою виявлення причин та умов вчинення правопорушень, прогнозування криміногенної ситуації та розроблення заходів щодо її стабілізації [2]. У цьому контексті підрозділи кримінальної поліції активно використовують сучасні інформаційні системи, бази даних, аналітичні інструменти та програмне забезпечення, що дозволяє підвищити ефективність оперативно-розшукової діяльності та кримінального аналізу.

В умовах воєнного стану значно зростає обсяг інформації, що підлягає обробці, а також ускладнюється її структура. Зокрема, з'являються нові джерела інформації, пов'язані з військовими діями, переміщенням населення, діяльністю диверсійних груп та кіберзагрозами. Це обумовлює необхідність впровадження сучасних методів кримінального аналізу, які дозволяють виявляти

приховані зв'язки між подіями, особами та об'єктами. Як зазначають А. О. Кисельов та Е. В. Копилов, кримінальний аналіз є ефективним інструментом інформаційно-аналітичного забезпечення, що дозволяє не лише фіксувати факти, а й прогнозувати розвиток злочинної діяльності [3, с. 48].

Особливе значення у діяльності підрозділів кримінальної поліції набуває використання відкритих джерел інформації (OSINT). Завдяки аналізу даних із соціальних мереж, відкритих реєстрів, медіа та інших інформаційних ресурсів, правоохоронні органи отримують можливість оперативно виявляти злочинні зв'язки, встановлювати місцезнаходження осіб та документувати протиправну діяльність. Як підкреслює І. А. Федчак, використання відкритих джерел інформації значно розширює можливості кримінального аналізу та сприяє підвищенню ефективності оперативної роботи [1, с. 73].

Важливим напрямом розвитку інформаційно-аналітичного забезпечення є інтеграція різних інформаційних систем та баз даних. Наявність єдиного інформаційного простору дозволяє забезпечити швидкий доступ до необхідної інформації, уникнути дублювання даних та підвищити ефективність взаємодії між різними підрозділами поліції. Водночас існують проблеми, пов'язані із захистом інформації, обмеженням доступу та необхідністю дотримання вимог законодавства щодо обробки персональних даних.

Крім того, важливу роль відіграє підготовка кадрів у сфері інформаційно-аналітичної діяльності. Працівники кримінальної поліції повинні володіти навичками роботи з інформаційними системами, аналізу великих масивів даних, використання аналітичного програмного забезпечення та інтерпретації отриманих результатів. Як зазначає Р. В. Білоус, ефективність інформаційно-аналітичної діяльності значною мірою залежить від рівня професійної підготовки працівників та їх здатності застосовувати сучасні аналітичні методи [4].

Таким чином, інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції є важливим інструментом підвищення ефективності протидії злочинності, особливо в умовах воєнного стану. Подальший розвиток цієї сфери повинен бути спрямований на впровадження сучасних інформаційних

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

Список використаних джерел:

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

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

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

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

КРИМІНАЛЬНИЙ АНАЛІЗ КІБЕРЗЛОЧИННОСТІ

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

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

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

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

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

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

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

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

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

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

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

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

Список використаних джерел:

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

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

РОЛЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Драч Владислав Максимович
курсант 202 взводу Навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України
Науковий керівник: ***Форос Ганна Володимирівна***
Завідувачка кафедри кримінального аналізу
та інформаційних технологій, к.ю.н., доцент

У сучасних умовах трансформації правоохоронної системи України інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції набуває визначального значення, оскільки саме воно забезпечує формування обґрунтованих управлінських та оперативних рішень. Основу цієї діяльності становлять процеси збору, систематизації, обробки, аналізу та інтерпретації інформації, що дозволяє виявляти закономірності злочинної діяльності, встановлювати причинно-наслідкові зв'язки та прогнозувати розвиток криміногенної ситуації [1, с. 22].

Відповідно до сучасних наукових підходів, інформаційно-аналітична діяльність повинна бути орієнтована не лише на фіксацію вже вчинених злочинів, а й на їх попередження. У цьому контексті важливу роль відіграє концепція intelligence-led policing (ILP), яка передбачає використання аналітичної інформації як основи для планування оперативно-розшукових заходів та визначення пріоритетних напрямів діяльності підрозділів кримінальної поліції. Застосування цієї концепції дозволяє перейти від реактивної до проактивної моделі протидії злочинності [3, с. 75].

Особливе місце в інформаційно-аналітичному забезпеченні займають сучасні інформаційні системи та бази даних, які забезпечують накопичення та обробку великих масивів інформації. Їх інтеграція у єдиний інформаційний простір дозволяє забезпечити швидкий доступ до даних, підвищити ефективність взаємодії між підрозділами та уникнути дублювання інформації. Як зазначають А. О. Кисельов та Е. В. Копилов, використання інформаційних систем у поєднанні з методами кримінального аналізу дозволяє

значно підвищити ефективність виявлення злочинних зв'язків та структури організованих груп [2, с. 64].

У сучасних умовах особливого значення набуває використання методів кримінального аналізу, які включають аналіз зв'язків, аналіз подій, часово-просторовий аналіз та профілювання осіб. Застосування цих методів дозволяє не лише встановлювати фактичні обставини злочину, а й формувати прогнози щодо подальшої діяльності злочинних груп. Як підкреслює І. А. Федчак, кримінальний аналіз забезпечує системне бачення злочинності та дозволяє приймати більш ефективні рішення у сфері правоохоронної діяльності [1, с. 71].

Окрему увагу слід приділити використанню відкритих джерел інформації (OSINT), які є важливим інструментом сучасного кримінального аналізу. Аналіз інформації з соціальних мереж, відкритих реєстрів, медіа та інших джерел дозволяє оперативно отримувати дані про осіб, події та об'єкти, що мають значення для розслідування злочинів. У наукових підходах, розроблених у межах діяльності ОДУВС під керівництвом Г. В. Форос, підкреслюється важливість інтеграції OSINT-інструментів у практичну діяльність підрозділів кримінальної поліції як складової сучасного інформаційно-аналітичного забезпечення [4].

Водночас ефективність інформаційно-аналітичної діяльності значною мірою залежить від рівня підготовки працівників. Недостатній рівень аналітичної компетентності, відсутність практичних навичок роботи з інформаційними системами та аналітичними інструментами знижує ефективність використання навіть найсучасніших технологій. У зв'язку з цим необхідним є удосконалення системи підготовки кадрів, орієнтованої на розвиток аналітичного мислення, навичок роботи з великими масивами даних та використання сучасного програмного забезпечення.

Таким чином, інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції є ключовим фактором підвищення ефективності протидії злочинності. Його розвиток повинен здійснюватися шляхом впровадження сучасних інформаційних технологій, інтеграції інформаційних ресурсів, розвитку кримінального аналізу та підвищення рівня професійної підготовки працівників.

Список використаних джерел:

1. Федчак І. А. Основи кримінального аналізу. Львів : ЛьвДУВС, 2020. 240 с.
2. Кисельов А. О., Копилов Е. В. Кримінальний аналіз у діяльності правоохоронних органів. Дніпро : ДДУВС, 2023. 220 с.
3. Реалізація філософії ILP в системі кримінального аналізу Національної поліції України : монографія. Одеса : ОДУВС, 2024.
4. Форос Г. В., Калугін В.Ю. Використання відеоаналітики та відеоспостереження в діяльності підрозділів Національної поліції України. Одеса : ОДУВС, 2025 URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/37bcde6e-0590-48eb-9897-f160badfa662/content

АНАЛІТИЧНІ ПРОДУКТИ ЯК РЕЗУЛЬТАТ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Кухтюк Юлія Віталіївна
курсант 202 взводу Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Науковий керівник: ***Форос Ганна Володимирівна***
завідувачка кафедри кримінального аналізу та інформаційних технологій, к.ю.н., доцент ОДУВС

У сучасних умовах розвитку суспільства та ускладнення криміногенної ситуації важливого значення набуває інформаційно-аналітичне забезпечення діяльності правоохоронних органів. Підрозділи кримінальної поліції щоденно працюють з великими обсягами інформації, що надходить з різноманітних джерел, зокрема оперативно-розшукових матеріалів, матеріалів кримінальних проваджень, державних реєстрів, статистичних даних та інших інформаційних ресурсів. Ефективна обробка та аналіз такої інформації є необхідною умовою успішної протидії злочинності. Саме тому важливим результатом інформаційно-аналітичної діяльності виступають аналітичні продукти, які використовуються для прийняття управлінських та оперативних рішень у діяльності підрозділів кримінальної поліції [3].

Інформаційно-аналітична діяльність у системі правоохоронних органів являє собою комплекс організаційних, правових та інформаційних заходів, спрямованих на збирання, накопичення, систематизацію та аналіз інформації про кримінальні правопорушення, осіб, причетних до їх вчинення, а також про фактори, що впливають на криміногенну ситуацію. Основною метою такої діяльності є отримання узагальнених відомостей, необхідних для забезпечення ефективної діяльності правоохоронних органів у сфері боротьби зі злочинністю [1].

Результатом інформаційно-аналітичної діяльності є створення аналітичних продуктів. Під аналітичними продуктами розуміють систематизовану інформацію, отриману в результаті аналітичної обробки даних, яка має практичне значення для прийняття управлінських або оперативних рішень. Такі продукти формуються на основі аналізу різних джерел інформації та дозволяють встановлювати взаємозв'язки між окремими подіями, особами та об'єктами, що має важливе значення для розкриття кримінальних правопорушень [2].

У діяльності підрозділів кримінальної поліції використовуються різні види аналітичних продуктів. До них належать аналітичні довідки, інформаційні огляди, аналітичні звіти, кримінальні профілі, прогнози розвитку криміногенної ситуації, а також схеми зв'язків між особами та подіями. Аналітичні довідки, як правило, містять узагальнену інформацію про певне кримінальне явище або подію, тоді як інформаційні огляди дозволяють оцінити стан злочинності на певній території або у певній сфері діяльності. Схеми зв'язків між особами використовуються для встановлення структури злочинних груп та визначення ролей окремих учасників злочинної діяльності.

Важливе місце серед аналітичних продуктів займають результати кримінального аналізу. Кримінальний аналіз являє собою спеціалізований вид інформаційно-аналітичної діяльності, який полягає у встановленні взаємозв'язків між інформацією про кримінальні правопорушення, особами, подіями та об'єктами . Також чимало проблемних моментів, які стосуються визначення та єдиного розуміння поняття й видів кримінального аналізу, нормативно-правового регулювання його вико-ристання в оперативно-розшуковій діяльності й, відпо-відно, у практичній діяльності оперативних

підрозділів Національної поліції України, застосування результатів(продуктів) кримінального аналізу тощо. [3].

У сучасних умовах значного розвитку інформаційних технологій важливу роль у створенні аналітичних продуктів відіграють автоматизовані інформаційні системи та електронні бази даних. Використання сучасних програмних комплексів дозволяє швидко обробляти великі обсяги інформації, встановлювати взаємозв'язки між різними подіями та особами, а також формувати аналітичні матеріали у зручному для використання вигляді. Такі технології значно підвищують ефективність діяльності правоохоронних органів та сприяють більш оперативному реагуванню на зміни криміногенної ситуації .

Окрему роль у формуванні аналітичних продуктів відіграє аналіз відкритих джерел інформації. У сучасному інформаційному суспільстві значна частина інформації про осіб та події може бути отримана з мережі Інтернет, соціальних мереж та інших відкритих ресурсів. Використання таких джерел інформації дозволяє розширити інформаційну базу для аналізу та підвищити ефективність інформаційно-аналітичної діяльності підрозділів кримінальної поліції.

Таким чином, аналітичні продукти є важливим результатом інформаційно-аналітичної діяльності підрозділів кримінальної поліції. Вони забезпечують узагальнення та систематизацію інформації, сприяють прийняттю обґрунтованих управлінських рішень та підвищують ефективність боротьби зі злочинністю. Подальший розвиток інформаційно-аналітичного забезпечення діяльності правоохоронних органів потребує впровадження сучасних інформаційних технологій, удосконалення методів кримінального аналізу та підвищення рівня професійної підготовки працівників поліції.

Список використаних джерел:

1. Закон України «Про Національну поліцію» від 02.07.2015. №580-VIII. URL: https://zakon.rada.gov.ua

2. Кримінальний процесуальний кодекс України від 13.04.2012. 4651-VI. URL: https://zakon.rada.gov.ua

3. Гончарук О. М., Ісмайлов К.Ю. Кримінальний аналіз у системі правоохоронних органів україни: поняття, мета й завдання. Одеса: ОДУВС, 2023. URL: https://ljd.dnuvs.ukr. education/ index.php

ДЕЯКІ ОСОБЛИВОСТІ ІНТЕЛЕКТУАЛЬНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ СЛІДЧОГО

Лемешко Юрій
аспірант закладу вищої освіти
«Міжнародний університет бізнесу і права»

Ефективність досудового розслідування безпосередньо залежить від якості інтелектуально-аналітичної діяльності слідчого, яка забезпечує логічне осмислення інформації, формування доказової бази та прийняття процесуальних рішень. У сучасних умовах ускладнення механізмів скоєння кримінальних правопорушень, зростання обсягів інформації, особливо з розвитком AI, суспільний резонанс, а також підвищення стандартів обґрунтованості рішень зумовлюють потребу в удосконаленні аналітичних підходів у діяльності органів досудового розслідування. Зазначене підсилює вимоги до когнітивної спроможності слідчого, здатності працювати в умовах невизначеності та забезпечувати відповідність результатів вимогам належності, допустимості й достовірності доказів [1; 2].

Теоретико-методологічні засади інтелектуально-аналітичної діяльності слідчого сформовано у межах криміналістики, кримінального процесу та більш сучасної моделі правоохоронної діяльності – Intelligence-Led Policing. У сучасному розумінні ILP інтегрує аналітичні, інформаційні та управлінські компоненти, формуючи безперервний цикл: збір даних → аналітична обробка → оцінка ризиків → прийняття рішень → зворотний зв'язок. Значний внесок у дослідження пізнавальної сутності розслідування, слідчого мислення та версійності здійснили українські науковці В. Шепітько, П. Біленчук, В. Гончаренко, М. Карчевський, М. Корнієнко, В. Салтевський, які обґрунтували, що встановлення обставин кримінального правопорушення є результатом складних логіко-аналітичних операцій, спрямованих на досягнення процесуальної істини [3; 4].

Процесуальні аспекти аналітичної діяльності, зокрема прийняття рішень, оцінка доказів і забезпечення їх допустимості, розкрито у працях В. Тертишника, Ю. Аленіна, О. Литвинова,

М. Шумила, які акцентують увагу на зв'язку аналітичних процедур із механізмом доказування та гарантіями прав людини [2; 5]. Особливої актуальності набуває забезпечення процесуальної придатності цифрових доказів, що вимагає дотримання стандартів фіксації, збереження та верифікації інформації.

Окремі напрями розвитку аналітичних підходів у правоохоронній діяльності, включно з інформаційно-аналітичним забезпеченням та використанням сучасних інструментів обробки даних, досліджуються у роботах В. В. Тіщенка, К. Ісмайлова О. Користіна, О. Долженкова, О. Фаріон, де підкреслюється зростаюча роль відкритої інформації в мережі Інтернет та необхідність систематизації аналітичних процедур і їх інтеграції у слідчу практику [1; 6-9, 11].

Водночас, попри значний рівень наукової розробленості, недостатньо дослідженими залишаються питання структурної організації інтелектуально-аналітичної діяльності, її алгоритмізації та стандартизації, що зумовлює необхідність подальших досліджень у цьому напрямі.

Наукова значущість дослідження полягає у поглибленні теоретичних уявлень про інтелектуально-аналітичну діяльність слідчого як самостійний елемент механізму досудового розслідування, а також у конкретизації її змісту, структури та функціонального призначення. Результати спрямовані на:

- уточнення понятійно-категоріального апарату;
- систематизацію підходів до аналізу доказової інформації;
- обґрунтування доцільності алгоритмізації аналітичної діяльності;
- розвиток положень щодо взаємозв'язку когнітивних процесів і доказування.

Отже, інтелектуально-аналітична діяльність слідчого є складною системою когнітивних, логічних і правових процесів, спрямованих на встановлення фактичних обставин кримінального правопорушення. Ключовою її особливістю є когнітивний характер, що проявляється у необхідності аналізу, узагальнення та інтерпретації інформації з метою формування цілісної картини події.

Також, важливою рисою є версійний характер діяльності, який передбачає висунення та перевірку слідчих версій як основного інструменту пізнання у кримінальному провадженні.

Іншою суттєвою ознакою є здійснення діяльності в умовах інформаційної невизначеності, що зумовлює прийняття рішень за наявності обмеженого обсягу даних.

Інтелектуально-аналітична діяльність має інтегративний характер, оскільки передбачає використання знань із різних галузей (криміналістичні, інформаційно-аналітичні, кібернетичні та правові методи), що забезпечує комплексний підхід до встановлення істини. Водночас вона є чітко орієнтованою на процес доказування, оскільки результати аналітичної діяльності повинні відповідати вимогам належності, допустимості та достовірності доказів [2].

Окремо слід відзначити тенденцію до алгоритмізації діяльності, що проявляється у використанні типових моделей розслідування, стандартизованих процедур та методик аналізу інформації [6]. Доцільно виділити базовий аналітичний цикл слідчого:

- збір та верифікація даних;
- структуризація інформації;
- аналітична обробка (зв'язки, закономірності, аномалії);
- формування версій;
- перевірка та процесуалізація результатів.

Відповідно до п. 2.6 Інструкції з організації діяльності органів досудового розслідування Міністерства внутрішніх справ України аналітична робота органів досудового розслідування забезпечує організацію збору даних, їх обробку та узагальнення, комплексне вивчення стану оперативної обстановки, результатів діяльності органу досудового розслідування для визначення головних проблем, які виявляють в управлінській діяльності органу досудового розслідування, недоліків і причин їх виникнення, надання практичної та методичної допомоги та зміцнення кадрів. Аналітична робота розроблення і вжиття заходів, спрямованих на усунення недоліків та вирішення наявних проблем [9].

У практиці досудового розслідування інтелектуально-аналітична діяльність реалізується через формування та перевірку слідчих версій у всіх правопорушеннях без винятку. Будь-то, наприклад, при розслідуванні крадіжок слідчий аналізує спосіб проникнення, характер викраденого майна та інші обставини, що дозволяє звузити коло підозрюваних, або у кримінальних провадженнях економічної спрямованості аналітична діяльність проявляється в дослідженні фінансових операцій, встановленні взаємозв'язків між

суб'єктами та виявленні протиправних схем руху коштів. Щодо Наприклад, при розслідуванні кіберзлочинів аналіз цифрових слідів (логів, IP-адрес, транзакцій) дозволяє встановити ланцюг подій та ідентифікувати суб'єктів правопорушення.

Також, використання сучасного інструментарію та методологій кримінального аналізу здатне суттєво покращити продуктивність та ефективність аналітичної діяльності. Результати аналітичних досліджень відіграють важливу роль у прогнозуванні криміногенної ситуації, виявленні та розшуку осіб, причетних до економічних злочинів, а також у визначенні методів, використаних для їх здійснення. Це дозволяє правоохоронним органам більш ефективно планувати свої дії та ресурси. Інформаційно-аналітичний підхід забезпечує підвищення ефективності стратегічного планування в правоохоронній діяльності. Це допомагає оптимізувати діяльність слідчих та оперативних підрозділів [10, с. 396].

Таким чином, інтелектуально-аналітична діяльність слідчого є визначальним елементом ефективного досудового розслідування, що забезпечує формування обґрунтованої доказової бази.До її основних особливостей належать:

- когнітивний та версійний характер;
- здійснення в умовах інформаційної невизначеності;
- інтегративність і міждисциплінарність;
- орієнтація на доказування;
- тенденція до алгоритмізації;
- використання цифрових та аналітичних технологій;
- орієнтація на ризик-менеджмент і прогнозування.

Подальший розвиток цієї діяльності пов'язаний із вдосконаленням методичного забезпечення, стандартизацією аналітичних процедур та підвищенням рівня професійної підготовки слідчих, здатними працювати з великими даними та інтелектуальними системами.

Список використаних джерел:

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Бутко Р., Денисенко Б., Ісмайлов К.Ю. та ін., за заг. ред. Користіна О.Є. Київ: «ВАІТЕ», 2024. 444 с.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

3. Криміналістика : підручник : у 2 т. Т. 1 / [В.Ю. Шепітько, В.А. Журавель, В.О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. Харків : Право, 2019. 456 с.

4. Криміналістика (криміналістична техніка): Курс лекцій / П.Д. Біленчук, А.П. Гель, М.В. Салтевський, Г.С. Семаков; Міжрегіон. акад. упр. персоналом. К., 2001. 216 с.

5. Тертишник В.І. Кримінально-процесуальне право України: підручник. 11-те вид., доповн. і перероб. Київ: Алерта, 2026. 674 с.

6. Тіщенко В. В. Криміналістика : навчально-методичний посібник / В. В. Тіщенко, О.О. Подобний. Одеса : Юридика, 2022. 236 с.

7. Навчальний посібник Тактичний кримінальний аналіз: теорія і практика / Н.П. Свиридюк, О.М. Цильмак, Заєць О.М., Ісмайлов К.Ю., Некрасов В.А. за заг. ред. Користіна О.Є.; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 216 с.

8. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. Південноукраїнський правничий часопис. 2016. № 2. С. 110-113.

9. Інструкція з організації діяльності органів досудового розслідування Міністерства внутрішніх справ України: Наказ МВС України від 09.08.2012 № 686. URL: https://zakon.rada.gov.ua/laws/show/z1770-12/en/ed20150715#Text

10. Биков І.О. Інформаційно-аналітичне забезпечення діяльності слідчих та оперативних підрозділів у боротьбі з економічними злочинами. Право і суспільство. № 1. Т. 2. 2024. С. 392-396.

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

АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В КОНТЕКСТІ ЗМІЦНЕННЯ ДЕРЖАВНОЇ СТІЙКОСТІ

Лунгол Ольга Миколаївна
кандидат педагогічних наук, доцент,
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
ORCID: ttps://orcid.org/0000-0001-8128-0072

В умовах глобальної цифровізації та триваючої гібридної агресії, кіберпростір перетворився на повноцінну арену протистояння, де кібертероризм виступає одним із найбільш деструктивних чинників впливу на національну безпеку. На відміну від класичних проявів тероризму, кібердиверсії спрямовані не лише на руйнування критичної інформаційної інфраструктури, а й на підрив суспільної довіри до державних інститутів, дестабілізацію процесів державотворення та нівелювання концепту державної стійкості.

Ефективність протидії таким загрозам сьогодні неможлива без якісної трансформації підходів до обробки інформації. Традиційні реактивні методи поступаються місцем проактивному аналітичному забезпеченню. Саме кримінальний аналіз у поєднанні з інструментами OSINT та технологіями штучного інтелекту стає фундаментом для виявлення прихованих закономірностей у діяльності терористичних угруповань, прогнозування векторів майбутніх атак та розробки превентивних заходів захисту державного суверенітету в цифровому вимірі.

Актуальність дослідження зумовлена необхідністю наукового переосмислення ролі аналітичних підрозділів правоохоронних органів як ключових суб'єктів забезпечення стійкості держави до новітніх кібервикликів.

Трансформація цифрового середовища зумовила еволюцію кібертероризму від поодиноких хакерських атак до системних багатовекторних операцій. Сучасна типологія цих загроз характеризується переходом від суто технічного пошкодження

інформаційних систем до комплексного впливу на соціально-політичну стабільність. Серед ключових тенденцій варто виділити:

- використання технологій синтетичних медіа (діпфейків) через створення високореалістичного маніпулятивного контенту. Дана тенденція стає потужним інструментом дискредитації керівництва держави та поширення панічних настроїв серед громадян нашої держави. Це створює загрозу когнітивній безпеці суспільства, дезорієнтуючи громадян та підриваючи довіру до офіційних джерел інформації;

- таргетовані атаки на державні реєстри та критичну інфраструктуру. Дані атаки характеризують спрямованість сучасного кібертероризму на блокування доступу до базових державних послуг та масову компрометацію персональних даних громадян. Втручання у роботу реєстрів не лише завдає економічних збитків, а й паралізує управлінські процеси, створюючи відчуття незахищеності та хаосу;

- когнітивні операції та інформаційно-психологічний тиск. Терористичні угруповання дедалі частіше використовують алгоритми соціальної інженерії для радикалізації населення та провокування внутрішніх конфліктів [1 – 3]. Використання соціальних мереж в наш час для поширення деструктивних наративів дозволяє здійснювати вплив на державні процеси та громадську думку в режимі реального часу.

Важливо наголосити, що першочерговою метою сучасного кібертероризму є не стільки фізичне руйнування об’єктів, скільки цілеспрямоване «розхитування» державної стійкості. Шляхом створення постійного цифрового тиску терористи намагаються зробити процеси державотворення нестабільними, уповільнити розвиток цифрових інституцій та змусити державу перейти у режим постійного кризового реагування замість планомірного стратегічного розвитку.

Ефективна відповідь на окреслені загрози потребує інтеграції сучасних інструментальних рішень, що корелюють із пріоритетними секціями даної конференції. Так, активний розвиток OSINT-технологій дозволяє проводити моніторинг Даркнету та аналіз активності у соціальних мережах для ідентифікації латентних осередків кібертероризму на ранніх етапах. Використання інструментів автоматизованого збору даних допомагає

деанонімізувати суб'єкти, що поширюють деструктивний контент, та виявляти зв'язки між окремими терористичними групами. Впровадження алгоритмів машинного навчання дозволяє здійснювати інтелектуальний аналіз аномалій у мережевому трафіку в режимі реального часу. Це забезпечує можливість прогнозування масштабних кібертерористичних операцій ще до моменту їх активної фази, перетворюючи систему захисту з реактивної на випереджальну. Побудова складних візуальних моделей зв'язків між фінансовими потоками, зокрема у сфері криптовалют, та конкретними терористичними актами є ключем до руйнування економічного підґрунтя кібертероризму. Аналітичне супроводження дозволяє не лише фіксувати злочин, а й простежувати весь ланцюг підготовки – від фінансування до реалізації.

У контексті сучасних викликів концепт державної стійкості має бути переосмислений: це не лише статичний захист периметра, а насамперед здатність державної системи до швидкого відновлення функціональності після деструктивного впливу. Якісне аналітичне забезпечення відіграє вирішальну роль у мінімізації «часу реакції» на інцидент. У ситуаціях кібертероризму на органи влади, кожна хвилина затримки збільшує ризики втрати керованості процесами державотворення. Використання результатів кримінального аналізу дозволяє органам правопорядку діяти за заздалегідь розробленими сценаріями, що базуються на прогнозних даних, забезпечуючи безперервність роботи критичної інфраструктури та збереження довіри суспільства до державних інститутів.

Отже, сучасний кібертероризм перестав бути виключно технічною проблемою, перетворившись на інструмент стратегічного впливу на процеси державотворення. Його головною метою є дестабілізація суспільно-політичної ситуації та підрив державної стійкості через когнітивні операції, використання діпфейків та атаки на критичні інформаційні ресурси. Забезпечення державної стійкості в цифрову епоху потребує переходу від реактивних моделей захисту до проактивного аналітичного супроводження. Побудова прогнозних моделей на основі кримінального аналізу дозволяє виявляти вектори терористичної активності ще на етапі їх планування. Найбільш ефективним інструментарієм протидії кібертероризму сьогодні є поєднання можливостей OSINT (наприклад, для виявлення осередків радикалізації та фінансових

потоків у Даркнеті) та алгоритмів штучного інтелекту (наприклад, для виявлення аномалій у трафіку та боротьби з маніпулятивним контентом).

Список використаних джерел:

1. Гуменюк В.В. Сучасний тероризм як інструмент дестабілізації та підриву процесів державотворення. Legal Bulletin, 1, 2026. С. 100–110. https://doi.org/10.31732/2708-339X-2026-10-A13

2. Сидор В.Д., Перепадін К.В. Теоретико-правові основи протидії інформаційному тероризму в умовах збройної агресії росії проти України. Legal Bulletin, 2025. С. 83-88.

3. 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

ВИКОРИСТАННЯ МЕТОДІВ КРИМІНАЛЬНОГО АНАЛІЗУ В ОПЕРАТИВНО-РОЗШУКОВОМУ ЗАБЕЗПЕЧЕННІ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Морозов Демид Анатолійович
професор кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Яремейчук Єгор Ігорович
курсант 202 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС

У сучасних умовах трансформації злочинності, її інтелектуалізації та використання новітніх технологій особливого значення набуває аналітична складова діяльності правоохоронних органів. Оперативно-розшукова діяльність (ОРД) виступає основним механізмом отримання інформації про злочини, однак ефективність її реалізації значною мірою залежить від рівня аналітичного забезпечення. У цьому контексті кримінальний аналіз є ключовим інструментом, що дозволяє систематизувати інформацію та

виявляти закономірності злочинної діяльності [1]. Закон України «Про оперативно-розшукову діяльність» визначає ОРД як систему гласних і негласних заходів, спрямованих на протидію злочинності [2]. У межах цієї діяльності здійснюється збір значних обсягів інформації, яка потребує належної обробки та інтерпретації. Саме кримінальний аналіз забезпечує перетворення розрізнених даних у структуровану інформацію, придатну для використання у кримінальному провадженні. Кримінальний аналіз охоплює сукупність методів дослідження інформації про злочини, злочинців та їх зв'язки. До основних методів належать аналіз зв'язків (link analysis), що дозволяє встановлювати взаємозв'язки між суб'єктами; аналіз подій (event analysis); просторовий аналіз (crime mapping); а також стратегічний і тактичний аналіз. Як зазначається у наукових дослідженнях, використання таких методів дозволяє не лише встановлювати факти, але й прогнозувати подальший розвиток криміногенної ситуації [3]. У практиці оперативних підрозділів кримінальний аналіз застосовується на всіх етапах оперативно-розшукового процесу. На етапі оперативного пошуку він використовується для виявлення підозрілих закономірностей та формування первинних версій. На етапі оперативної розробки — для встановлення структури злочинних груп, ролей учасників та каналів взаємодії. У подальшому результати аналітичної діяльності використовуються для планування слідчих (розшукових) дій та забезпечення доказування у кримінальному провадженні.

Відповідно до Кримінального процесуального кодексу України, доказами є фактичні дані, отримані у встановленому законом порядку [4]. У зв'язку з цим результати кримінального аналізу повинні бути не лише аналітично обґрунтованими, але й належним чином оформленими. Вони можуть виступати як орієнтуюча інформація або як підстава для проведення процесуальних дій, зокрема негласних слідчих (розшукових) дій. Важливу роль кримінальний аналіз відіграє у протидії організованій злочинності. Саме завдяки аналітичним методам стає можливим встановлення ієрархії злочинних угруповань, каналів постачання незаконних товарів, фінансових потоків та інших елементів злочинної діяльності. Це дозволяє не лише реагувати на вчинені злочини, але й попереджати їх. Конституція України закріплює принцип верховенства права та гарантує захист прав і свобод людини [5]. Тому

застосування кримінального аналізу в ОРД повинно здійснюватися з дотриманням принципів законності, пропорційності та обґрунтованості. Особливо це стосується використання персональних даних та інформації з різних джерел.

На сучасному етапі розвитку правоохоронної діяльності кримінальний аналіз активно поєднується з інформаційними технологіями, що дозволяє автоматизувати процеси обробки даних. Використання спеціалізованих аналітичних систем сприяє підвищенню точності та швидкості аналізу, що є критично важливим в умовах обмеженого часу.

Водночас існують проблеми застосування кримінального аналізу, серед яких: недостатній рівень технічного забезпечення, відсутність єдиних стандартів аналітичної діяльності, а також необхідність підвищення кваліфікації працівників. Вирішення цих проблем є важливим напрямом розвитку ОРД. Отже, кримінальний аналіз є невід'ємною складовою оперативно-розшукового забезпечення кримінального провадження. Його використання дозволяє підвищити ефективність діяльності правоохоронних органів, однак потребує належного нормативного та методичного забезпечення.

Список використаних джерел:

1. Ratcliffe J. H. Intelligence-Led Policing. Routledge, 2016.
2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII.
3. Europol. Serious and Organised Crime Threat Assessment (SOCTA). 2021.
4. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.
5. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР.
6. UNODC. Criminal Intelligence Manual for Analysts. Vienna, 2011.

ТЕОРИТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ

Меликов Руслан
Науковий співробітник
науково-дослідної лабораторії
з актуальних питань кримінального аналізу
доктор філософії в галузі права

У сучасних умовах розвитку суспільства та зростання рівня організованої й транснаціональної злочинності особливого значення набуває кримінальний аналіз як складова інформаційно-аналітичного забезпечення правоохоронної діяльності. Ефективність діяльності правоохоронних органів значною мірою залежить від здатності своєчасно виявляти кримінальні загрози, прогнозувати розвиток криміногенної ситуації та приймати обґрунтовані управлінські рішення. У зв'язку з цим розвиток кримінального аналізу в Україні є одним із пріоритетних напрямів реформування системи забезпечення громадської безпеки та правопорядку [1, с. 11–15].

Теоретичні засади кримінального аналізу ґрунтуються на використанні комплексу наукових методів збору, систематизації, оцінки та інтерпретації інформації про кримінальні правопорушення, осіб, причетних до їх учинення, а також фактори, що впливають на криміногенну ситуацію. Кримінальний аналіз визначається як інтелектуальний процес, спрямований на перетворення інформації в аналітичний продукт для забезпечення прийняття ефективних рішень у сфері протидії злочинності [4, с. 18–24].

Основними видами кримінального аналізу є оперативний, тактичний і стратегічний аналіз, кожен із яких виконує окремі функції у діяльності правоохоронних органів. На сучасному етапі в Україні активно впроваджуються міжнародні стандарти кримінального аналізу, зокрема концепція *Intelligence-Led Policing*, яка передбачає здійснення поліцейської діяльності на основі аналітичної інформації та оцінки ризиків [1, с. 27–35]. Такий підхід дозволяє правоохоронним органам не лише реагувати на вже вчинені кримінальні правопорушення, а й здійснювати їх превенцію шляхом аналізу

кримінальних тенденцій, встановлення взаємозв'язків між подіями та прогнозування можливих загроз [3, с. 75–77].

Практичне значення кримінального аналізу полягає у його використанні підрозділами Національної поліції України, Служби безпеки України та іншими суб'єктами сектору безпеки і оборони. Застосування сучасних інформаційно-аналітичних систем забезпечує можливість обробки великих масивів даних, встановлення зв'язків між особами, подіями та об'єктами, а також виявлення організованих злочинних груп. Особливо актуальним є використання кримінального аналізу у протидії кіберзлочинності, незаконному обігу наркотичних засобів, торгівлі людьми, тероризму та корупційним правопорушенням [3, с. 76–79].

Одним із перспективних напрямів розвитку кримінального аналізу є використання цифрових технологій, автоматизованих систем обробки даних, штучного інтелекту та методів OSINT-аналізу. Впровадження сучасних технологічних рішень сприяє підвищенню швидкості аналізу інформації та ефективності діяльності правоохоронних органів. Водночас важливою проблемою залишається недостатній рівень технічного забезпечення та професійної підготовки аналітиків. Саме тому особливого значення набуває вдосконалення системи підготовки фахівців у закладах вищої освіти зі специфічними умовами навчання, зокрема у закладах системи МВС України [4, с. 146–154].

Важливим напрямом розвитку кримінального аналізу в Україні є також міжнародне співробітництво з правоохоронними структурами держав Європейського Союзу та міжнародними організаціями, зокрема Європолом. Використання міжнародного досвіду сприяє адаптації української системи кримінального аналізу до європейських стандартів та підвищенню ефективності протидії транснаціональній злочинності [2].

Отже, кримінальний аналіз є важливим елементом сучасної правоохоронної діяльності та необхідною умовою ефективної протидії злочинності. Подальший розвиток кримінального аналізу в Україні пов'язаний із цифровізацією правоохоронної системи, удосконаленням нормативно-правового забезпечення, підготовкою кваліфікованих кадрів та розширенням міжнародної співпраці. Використання сучасних аналітичних технологій сприятиме підвищенню рівня громадської безпеки та ефективності діяльності правоохоронних органів.

Список використаних джерел:

1. Користін О. Є., Свиридюк Н. П., Цільмак О. М. та ін. Тактичний кримінальний аналіз: теорія та практика : навч. посіб. Одеса : ОДУВС, 2019. 216 с.
2. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. https://zakon.rada.gov.ua/laws/show/580-19#Text
3. Гончарук О. М., Ісмайлов К. Ю. Кримінальний аналіз у системі правоохоронних органів України: поняття, мета й завдання // *Правовий часопис Донбасу*. 2023. № 3. С. 74–79.
4. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : ЛьвДУВС, 2021. 288 с.
5. Біленчук П. Д., Кофанов А. В., Кобилянський О. Л. Криміналістична аналітика: інформаційні системи, інтегровані банки даних, електронні мережі : навч. посіб. Київ, 2010.

КРИТЕРІЇ ФОРМУВАННЯ АНАЛІТИЧНОГО ЗНАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Некрасов В. А.
кандидат юридичних наук, професор, професор кафедри кримінального права та кримінології навчально-наукового інституту права та психології,
Національна академія внутрішніх справ

У практиці аналітичної діяльності у сфері забезпечення економічної безпеки держави принципово важливо розрізняти результати, які залишаються на рівні узагальнення інформації, і результати, що дійсно формують нове знання, придатне для прийняття управлінських та правоохоронних рішень. Ця різниця найкраще пояснюється через базову аналітичну формулу *«дані → інформація → знання»*, яка відображає послідовність перетворення вихідних матеріалів у результат, здатний впливати на управління ризиками та протидію кримінальним загрозам у сфері економіки [1; 2]. Дані є сукупністю розрізнених фактів, фінансових показників, транзакцій, оперативних сигналів або окремих відомостей щодо діяльності економічних агентів, які самі по собі не мають

пояснювальної сили. Інформація виникає внаслідок їх структурування та узагальнення, коли стає можливим опис окремих тенденцій чи процесів. Однак лише на рівні знання відбувається розкриття внутрішніх закономірностей, причин і механізмів функціонування кримінальних економічних практик, а також формуються підстави для прогнозування та вибору управлінських або правоохоронних дій [2].

Помилка значної частини аналітичних продуктів у сфері економічної безпеки полягає в тому, що вони зупиняються на переході від даних до інформації. Аналітик систематизує фінансові показники, описує динаміку порушень або узагальнює статистику, однак не виходить на рівень пояснення механізмів криміналізації економічних процесів. Такий результат може використовуватись як довідковий матеріал, проте він не змінює розуміння природи загроз і не створює підстав для вироблення нових управлінських рішень. Натомість знання виникає лише тоді, коли аналітичний процес дозволяє перейти від фіксації фактів до розкриття внутрішньої логіки кримінальної діяльності – тобто коли аналітик пояснює не лише «що відбувається», а «чому це відбувається саме так», «які механізми це забезпечують» та «як ситуація розвиватиметься далі» [3].

Першою ознакою того, що в результаті аналізу отримано саме знання, є поява новизни або аналітичного інсайту. Йдеться не обов'язково про отримання нових даних, а про нове розуміння вже відомої інформації. Якщо після проведення аналізу змінюється уявлення про природу кримінальної загрози, встановлюються раніше неочевидні взаємозв'язки між економічними агентами, фінансовими потоками або кримінальними практиками, це свідчить про формування знання [2]. Наприклад, якщо аналіз фінансових операцій дозволяє встановити, що група підприємств використовує однакові транзитні компанії, координовані канали виведення коштів та спільних вигодоодержувачів, це свідчить не про окремі порушення, а про функціонування організованого механізму мінімізації податкових зобов'язань або легалізації доходів.

Другою ключовою ознакою є причинний характер висновків. Інформація описує явища, тоді як знання пояснює їхню природу. Якщо аналітичний продукт обмежується констатацією факту зростання кількості фіктивних фінансових операцій або збільшення

обсягів незаконного відшкодування ПДВ, це ще не знання. Знання виникає тоді, коли встановлюється причинно-наслідковий механізм: наприклад, зростання масштабів таких операцій може пояснюватися діяльністю транзитно-конвертаційних груп, існуванням стійкого попиту на кримінальні економічні практики, що відображає агресивність зовнішнього середовища для суб'єктів господарювання, недосконалістю механізмів фіскального контролю, функціонуванням систем політичної ренти через створення нормативно сприятливих умов для тіньових практик, наявністю корупційних механізмів, а також використанням цифрових платформ і технологічних рішень для приховування кінцевих бенефіціарних власників. Саме розуміння причин дозволяє впливати на ситуацію, а не лише фіксувати її прояви [4].

Третім важливим критерієм є здатність результату аналізу до прогнозування. Знання завжди має випереджальний характер: воно дозволяє не тільки пояснювати вже виявлені кримінальні практики, а й прогнозувати розвиток загроз. Якщо аналітичний висновок дозволяє змоделювати подальше поширення схем ухилення від оподаткування, оцінити ризик втрат державного бюджету або передбачити проникнення організованих кримінальних структур у критичні сектори економіки, це свідчить про досягнення рівня знання [3; 5]. Наприклад, якщо на основі виявлених закономірностей можна обґрунтовано прогнозувати, що за відсутності належних змін у механізмах фіскального контролю, регуляторній політиці та системі запобігання корупційним практикам окремий сектор економіки набуватиме ознак стійкого середовища для поширення кримінальних економічних практик, фіктивного експорту та прихованого виведення капіталу, – це свідчить про формування прогностичного знання, придатного для стратегічного управління ризиками економічної безпеки держави.

Четвертою ознакою є придатність результату аналізу до практичного застосування, або його операціоналізація. Знання відрізняється від інформації тим, що воно безпосередньо пов'язане з дією. Якщо результат аналізу не трансформується у конкретні варіанти управлінських, правоохоронних (кримінально-правового впливу) або превентивних заходів, він залишається на рівні довідкової інформації. Натомість знання завжди дає відповідь на питання «що необхідно робити», «які інструменти є найбільш

ефективними» та «чому саме цей варіант реагування є оптимальним» [5]. Саме ця логіка лежить в основі ризик-орієнтованого підходу, Intelligence-Led Policing та сучасних моделей аналітичного забезпечення державної політики у сфері економічної безпеки.

П'ятим критерієм є здатність аналітичного результату зменшувати рівень невизначеності. У межах логіки *«дані → інформація → знання»* саме знання забезпечує якісне звуження поля невідомого та створює основу для прийняття рішень в умовах складного безпекового середовища [3]. Якщо аналітичний продукт дозволяє виділити ключові ризики, визначити найбільш імовірні сценарії розвитку загроз та оцінити їхній вплив на економічну безпеку держави, це свідчить про його перехід на рівень знання.

Окрему увагу слід звернути на контрінтуїтивність як ознаку глибокого аналітичного знання. Практика протидії економічній злочинності демонструє, що поведінка складних соціально-економічних систем часто суперечить інтуїтивним очікуванням. Зовні легальні фінансові механізми можуть використовуватись як інструменти тіньової економіки, а найбільші ризики інколи формуються не в очевидно криміналізованих секторах, а у сферах із високим рівнем формальної легальності. Виявлення таких неочевидних залежностей свідчить про досягнення глибшого рівня аналітичного розуміння [4].

Ще однією важливою характеристикою знання є його переносимість. Якщо результат аналізу дозволяє сформувати модель, закономірність або ризик-профіль, придатний для використання в інших подібних ситуаціях, це означає перехід від інформації до узагальненого знання [2]. У сфері забезпечення економічної безпеки це дозволяє створювати типові профілі ризикових суб'єктів господарювання, моделі кримінальної економічної поведінки, індикатори фіктивної діяльності, сценарії використання кримінальних практик та системи раннього попередження про виникнення нових кримінальних загроз.

Таким чином, оцінка якості аналітичного продукту у сфері забезпечення економічної безпеки держави повинна базуватися на визначенні того, чи відбувся повноцінний перехід від даних через інформацію до знання. Якщо результат лише описує ситуацію або статистично фіксує окремі прояви кримінальної активності, він залишається на рівні інформації. Якщо ж аналітичний продукт

формує причинну модель кримінального явища, дозволяє прогнозувати розвиток загроз та безпосередньо впливає на вибір управлінських рішень, він набуває статусу знання.

Узагальнюючи, можна сформулювати, що результат аналітичної діяльності набуває статусу знання тоді, коли забезпечує завершений цикл перетворення *«дані → інформація → знання»*, у межах якого розкрито механізми криміналізації економічних процесів, визначено ймовірну поведінку системи, оцінено ризики для економічної безпеки держави та обґрунтовано варіанти управлінських, превентивних або правоохоронних дій. Саме такий результат є цільовим для сучасної аналітичної діяльності, орієнтованої не лише на опис кримінальних загроз, а на їх випереджальне виявлення та стратегічне стримування.

Список використаних джерел:

1. Ackoff R. L. From Data to Wisdom // Journal of Applied Systems Analysis. – 1989. – Vol. 16. – P. 3–9.

2. Nonaka I., Takeuchi H. The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. – New York: Oxford University Press, 1995. – 304 p.

3. Heuer R. J. Psychology of Intelligence Analysis. – Washington, DC: Center for the Study of Intelligence, CIA, 1999. – 199 p.

4. Meadows D. H. Thinking in Systems: A Primer. – White River Junction: Chelsea Green Publishing, 2008. – 218 p.

5. OECD. Strategic Foresight for Better Policies: Building Effective Governance in the Face of Uncertain Futures. – Paris: OECD Publishing, 2020. – 144 p.

КРИМІНАЛЬНИЙ АНАЛІЗ У ЦИФРОВОМУ СЕРЕДОВИЩІ: СУЧАСНІ МЕТОДИ ОБРОБКИ ВЕЛИКИХ ДАНИХ ТА ВИЯВЛЕННЯ АНОМАЛЬНОЇ АКТИВНОСТІ

Петрів Юрій Петрович
доктор філософії

Сучасний етап розвитку інформаційного суспільства характеризується масштабною цифровізацією соціально-економічних процесів, інтенсивним розвитком інформаційно-комунікаційних технологій та стрімким зростанням ролі цифрового середовища у функціонуванні державних інституцій, фінансових систем, правоохоронних органів, об'єктів критичної інфраструктури та глобальних комунікаційних мереж. Формування цифрової економіки та інтеграція інноваційних технологій у всі сфери суспільного життя створюють принципово нову архітектуру інформаційного простору, в межах якого щоденно генеруються надзвичайно великі обсяги даних. У сучасних умовах цифрові дані стають одним із ключових ресурсів функціонування держави, суспільства та систем безпеки, а їх ефективна обробка перетворюється на стратегічний елемент забезпечення національної та інформаційної безпеки. Водночас активна цифровізація супроводжується стрімким зростанням рівня кіберзлочинності, ускладненням механізмів реалізації кіберінцидентів та формуванням нових моделей злочинної діяльності у кіберпросторі [1-3].

Особливістю сучасної кіберзлочинності є її високий рівень технологічної адаптивності, використання автоматизованих засобів реалізації атак, механізмів анонімізації, технологій штучного інтелекту та розподілених інформаційних інфраструктур. У сучасному цифровому середовищі кіберзлочинні угруповання активно використовують великі масиви даних, автоматизовані бот-мережі, соціальні платформи, криптовалютні сервіси та ресурси даркнету для реалізації складних багаторівневих злочинних схем. За таких умов традиційні методи кримінального аналізу виявляються недостатньо ефективними, оскільки не здатні забезпечити оперативну обробку надвеликих обсягів інформації та своєчасне виявлення прихованих закономірностей у цифровому середовищі. Саме тому особливого значення набуває використання сучасних

методів обробки великих даних та інтелектуального аналізу інформації у процесі кримінального аналізу кіберінцидентів [3].

У сучасній науковій парадигмі великі дані розглядаються як складні інформаційні масиви, що характеризуються значними обсягами, високою швидкістю генерації, різноманітністю форматів та необхідністю оперативної обробки у режимі реального часу. У сфері кримінального аналізу великі дані включають інформацію про мережевий трафік, події інформаційної безпеки, цифрові сліди користувачів, лог-файли інформаційних систем, транзакційні дані, інформацію із соціальних мереж, телекомунікаційних платформ, відеоспостереження та відкритих джерел інформації. Аналіз зазначених масивів інформації дозволяє виявляти закономірності функціонування кіберзлочинних структур, прогнозувати розвиток кіберзагроз та формувати моделі підтримки прийняття управлінських рішень у сфері кібербезпеки.

Особливість використання великих даних у кримінальному аналізі полягає у необхідності інтеграції різнорідних джерел інформації та забезпечення комплексного дослідження цифрового середовища як складної динамічної системи. У межах системного підходу цифровий простір розглядається як багаторівнева мережа інформаційних взаємодій, у якій кіберзлочинність виступає дестабілізуючим фактором, здатним впливати на функціональну стійкість інформаційної інфраструктури. У таких умовах ефективний кримінальний аналіз потребує використання інтелектуальних методів обробки даних, здатних забезпечити автоматизоване виявлення аномальної активності, прогнозування кіберінцидентів та аналіз складних інформаційних взаємозв'язків між суб'єктами кіберпростору [2].

Одним із ключових напрямів сучасного кримінального аналізу є виявлення аномальної активності у цифровому середовищі. У контексті кібербезпеки аномальна активність розглядається як відхилення від типових моделей функціонування інформаційних систем, поведінки користувачів або мережевих процесів, що може свідчити про наявність кіберзагроз, шкідливої активності чи реалізації кіберінциденту. Особливістю сучасних кіберзагроз є їх здатність маскуватися під легітимні дії користувачів, що значно ускладнює процеси виявлення атак традиційними методами моніторингу. Саме тому використання інтелектуальних алгоритмів аналізу великих

даних стає необхідною умовою ефективного функціонування систем кримінального аналізу у цифровому середовищі [1-3].

Сучасні методи виявлення аномальної активності ґрунтуються на використанні алгоритмів машинного навчання, статистичного аналізу, нейронних мереж та технологій штучного інтелекту. Особливого значення набувають методи класифікації, кластеризації та предиктивної аналітики, які дозволяють автоматично виявляти нетипові патерни поведінки у великих масивах даних. Використання алгоритмів машинного навчання забезпечує можливість формування адаптивних моделей аналізу інформації, здатних самостійно виявляти приховані закономірності та прогнозувати потенційні кіберзагрози на основі історичних даних і поточних інформаційних потоків.

У процесі виявлення аномальної активності особливого значення набувають методи поведінкового аналізу користувачів та інформаційних систем. Сучасні кіберзлочинці дедалі частіше використовують механізми соціальної інженерії, викрадені облікові записи та інсайдерські загрози для реалізації атак на інформаційні системи. Аналіз поведінкових характеристик користувачів дозволяє виявляти відхилення від типових моделей активності, що можуть свідчити про компрометацію інформаційних ресурсів або реалізацію шкідливих дій. Використання технологій User and Entity Behavior Analytics створює можливість автоматизованого моніторингу цифрової активності та формування систем раннього попередження про потенційні кіберзагрози.

Не менш важливим напрямом є аналіз мережевого трафіку та подій інформаційної безпеки. У сучасних умовах інформаційні системи генерують значні обсяги телеметричних даних, які містять інформацію про функціонування мереж, активність користувачів та події безпеки. Використання технологій Big Data Analytics дозволяє здійснювати високошвидкісний аналіз зазначених інформаційних потоків, виявляти аномальні мережеві з’єднання, ознаки шкідливого програмного забезпечення та складні багатоступеневі сценарії кібератак. Особливого значення набуває інтеграція систем SIEM та SOAR із технологіями штучного інтелекту, що забезпечує автоматизовану кореляцію подій безпеки та підтримку прийняття рішень у режимі реального часу[3].

Важливу роль у сучасному кримінальному аналізі відіграє використання методів глибинного навчання та нейронних мереж. Глибинні нейронні архітектури дозволяють здійснювати аналіз складних нелінійних залежностей у великих масивах інформації, виявляти приховані патерни кіберзагроз та прогнозувати розвиток кіберінцидентів. Особливого значення набувають рекурентні нейронні мережі та архітектури типу LSTM, здатні аналізувати часові ряди та моделювати динаміку розвитку аномальної активності у цифровому середовищі. Використання зазначених технологій створює передумови для формування інтелектуальних систем кримінального аналізу, здатних адаптуватися до нових типів кіберзагроз та забезпечувати високий рівень точності аналітичних прогнозів.

У сучасних умовах важливого значення набуває інтеграція методів аналізу великих даних із технологіями OSINT та цифрової кримінальної аналітики. Відкриті джерела інформації, соціальні мережі, тематичні форуми, даркнет-ресурси та цифрові платформи містять значні обсяги інформації про кіберзагрози, механізми реалізації атак та діяльність кіберзлочинних угруповань. Використання інтелектуальних систем аналізу текстової інформації, технологій Natural Language Processing та семантичного аналізу дозволяє здійснювати автоматизоване виявлення інформаційних аномалій, аналізувати цифрову активність суб'єктів кіберпростору та формувати аналітичні моделі розвитку кіберзлочинності.

Особливого значення набуває використання системно-аналітичних підходів у процесі дослідження структури кіберзлочинних мереж. Сучасна кіберзлочинність дедалі частіше функціонує у формі розподілених децентралізованих мереж, що використовують механізми криптографічного захисту, анонімізації та автоматизованого управління. Аналіз таких структур потребує використання методів мережевого аналізу, теорії графів та когнітивного моделювання, які дозволяють виявляти ключові вузли інформаційної взаємодії, аналізувати маршрути поширення інформації та прогнозувати поведінку кіберзлочинних угруповань. Інтеграція зазначених підходів із технологіями Big Data Analytics створює можливість формування комплексних моделей кримінального аналізу у цифровому середовищі.

Водночас використання великих даних у сфері кримінального аналізу супроводжується низкою складних проблем та викликів. Однією з ключових проблем є забезпечення якості, достовірності та репрезентативності інформації, яка використовується для аналітичної обробки. Значна частина цифрових даних характеризується фрагментарністю, надлишковістю або наявністю маніпулятивного контенту, що може негативно впливати на результати аналітичного аналізу. Крім того, суттєвою проблемою залишається забезпечення конфіденційності персональних даних та дотримання прав людини у процесі обробки великих масивів інформації [1].

Не менш актуальною є проблема інтерпретованості результатів інтелектуального аналізу даних. Багато сучасних моделей машинного навчання функціонують за принципом «чорної скриньки», що ускладнює процес пояснення логіки формування аналітичних висновків та прийняття управлінських рішень. У контексті діяльності правоохоронних органів зазначена проблема набуває особливого значення, оскільки результати кримінального аналізу можуть використовуватися у процесах розслідування кіберзлочинів, оцінювання ризиків та формування управлінських стратегій у сфері кібербезпеки [1].

Перспективним напрямом розвитку кримінального аналізу у цифровому середовищі є створення інтегрованих інформаційно-аналітичних платформ, здатних забезпечити автоматизовану обробку великих даних, виявлення аномальної активності та підтримку прийняття рішень у сфері кібербезпеки. Використання технологій хмарних обчислень, штучного інтелекту, цифрових двійників та систем ситуаційної обізнаності створює передумови для формування адаптивних систем кримінального аналізу, здатних функціонувати в умовах високого рівня невизначеності та динамічного розвитку кіберпростору.

Таким чином, сучасний кримінальний аналіз у цифровому середовищі неможливий без використання інтелектуальних методів обробки великих даних та технологій виявлення аномальної активності. Інтеграція системного аналізу, машинного навчання, технологій штучного інтелекту та Big Data Analytics дозволяє суттєво підвищити ефективність виявлення кіберзагроз, прогнозування кіберінцидентів та підтримки прийняття управлінських рішень у сфері кібербезпеки. Подальший розвиток зазначеного

напряму потребує вдосконалення методологічних засад кримінального аналізу, розвитку цифрової інфраструктури, формування інтегрованих інформаційно-аналітичних систем та підготовки висококваліфікованих фахівців у сфері системного аналізу, науки про дані та кібербезпеки.

Список використаних джерел:

1. Основи кримінального аналізу: навчально-методичні рекомендації до вивчення навчальної дисципліни /уклад. Калугін В.Ю., О.А. Балтовський Одеса: ОДУВС, 2022. 58 с.
2. Основи кримінального аналізу: підручник / Бабенко А.М. та ін.; за заг. ред. Користіна О.Є. Одеса 2019. 296 с.
3. Тактичний кримінальний аналіз: теорія та практика; навчальний посібник / Користін О.Є., та ін.; за заг. ред. Користіна О.Є. МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 216 с.

АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОЦІНКИ КРИМІНОГЕННИХ РИЗИКІВ, ПОВ'ЯЗАНИХ ІЗ МІГРАЦІЙНИМИ ПРОЦЕСАМИ В УМОВАХ ВОЄННОГО СТАНУ

Погребняк Олена Геннадіївна
кандидат юридичних наук, викладач кафедри адміністративно-правових дисциплін, Одеського державного університету внутрішніх справ

В умовах воєнного стану міграційні процеси набувають складного, багатовимірного характеру, що безпосередньо впливає на криміногенну ситуацію в державі. Масові переміщення населення, зокрема внутрішня та транскордонна міграція, формують нові вразливості у сфері національної безпеки, що потребують системного аналітичного супроводу. Як показують сучасні дослідження, міграція в умовах збройного конфлікту виступає не лише соціальним, але й криміногенним фактором, який генерує ризики організованої злочинності, незаконного переправлення осіб та віктимізації мігрантів [1].

Аналітичне забезпечення оцінки криміногенних ризиків у міграційній сфері передбачає інтеграцію кримінологічного аналізу, даних прикордонного контролю, інформації правоохоронних органів та соціально-економічних індикаторів. У науковій літературі підкреслюється, що нерегулярна міграція в умовах збройного конфлікту формує специфічне криміногенне середовище, де одночасно зростає рівень злочинності серед мігрантів і рівень злочинів проти них [1]. Це вимагає побудови аналітичних моделей, здатних враховувати як об'єктивні (військові дії, переміщення населення), так і суб'єктивні (соціальна дезадаптація, правова невизначеність) фактори.

Умови воєнного стану в Україні актуалізують проблему організованої незаконної міграції та супутніх транснаціональних злочинних практик. Сучасні дослідження засвідчують, що в період воєнних дій відбувається трансформація каналів нелегального переміщення осіб, які дедалі частіше використовуються злочинними групами для отримання фінансової вигоди або прикриття інших кримінальних активностей [2]. Це створює додаткові виклики для правоохоронних органів та потребує впровадження інструментів прогнозної аналітики.

Ключовим елементом аналітичного забезпечення є побудова системи криміногенних ризик-індикаторів, які дозволяють ідентифікувати потенційно небезпечні міграційні потоки. До таких індикаторів належать: різке зростання транскордонних переміщень, зміна маршрутів міграції, концентрація вразливих груп населення, а також активізація нелегальних посередницьких структур. У наукових дослідженнях наголошується, що саме системний аналіз таких факторів дозволяє виявляти приховані закономірності криміногенних процесів у міграційній сфері [2].

Особливого значення набуває використання сучасних інформаційно-аналітичних технологій, включно з OSINT, геоаналітикою та системами кримінального аналізу даних. Їх застосування дозволяє здійснювати багаторівневу оцінку ризиків, прогнозувати можливі сценарії розвитку криміногенної ситуації та підвищувати ефективність управлінських рішень у сфері міграційної безпеки. У цьому контексті аналітичні системи виступають інструментом не лише фіксації, але й попередження кримінальних загроз, пов'язаних із міграційними процесами.

Таким чином, аналітичне забезпечення оцінки криміногенних ризиків у сфері міграції в умовах воєнного стану є комплексною міждисциплінарною проблемою, що поєднує елементи кримінології, інформаційної аналітики та державного управління. Його ефективність безпосередньо залежить від якості даних, рівня інтеграції інформаційних систем та здатності прогнозувати динаміку міграційних потоків у контексті воєнно-політичної нестабільності.

Список використаних джерел:

1. Lytvynov O. M., Orlov Yu. V., Yashchenko A. M., Yurtayeva K. V. Criminogenic risks of irregular migration in conditions of armed conflict in Ukraine // DIXI. 2025. Vol. 23, No. 2. P. 1–25. DOI: https://doi.org/10.16925/2357-5891.2021.02.09

2. Khalymon S., Chlevickaitė G., Kuryliuk Yu., Nikolaienko T., Stepanova Yu. War, martial law, and mobilisation: Exploring the characteristics of human smuggling at Ukraine's borders in 2022–2023. Security Journal. 2025. Vol. 23, No. 1. DOI: https://doi.org/10.1177/14773708251318476

МОДЕРНІЗАЦІЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ТА ЕКСПЕРТНО-КРИМІНАЛІСТИЧНОЇ ДІЯЛЬНОСТІ ПРАВООХОРНИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Чайка Ірина Вікторівна
курсант 202 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України
Науковий керівник: ***Морозов Демид Анатолійович***
професор кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС

Модернізація оперативно-розшукової та експертно-криміналістичної діяльності правоохоронних органів у сфері протидії організованій злочинності є комплексним процесом, що поєднує оновлення нормативно-правової бази з реальним впровадженням сучасних технологій і практичних інструментів у діяльність

правоохоронців. Правовою основою виступають Закон України «Про оперативно-розшукову діяльність» та Закон України «Про судову експертизу», які визначають межі та порядок здійснення оперативних заходів і проведення експертиз [1; 2]. Водночас сучасні умови потребують їх адаптації до цифрового середовища та нових форм злочинності.

У теоретичному аспекті криміналістика розглядає оперативно-розшукову діяльність як систему гласних і негласних заходів, спрямованих на виявлення та документування злочинної діяльності. На практиці це реалізується через проведення негласних слідчих (розшукових) дій, зокрема аудіо- та відеоконтролю, спостереження, контрольованих закупок. Наприклад, під час викриття організованих груп, що займаються збутом наркотиків, оперативні підрозділи документують факти передачі заборонених речовин за допомогою технічних засобів, а отримані матеріали в подальшому підтверджуються експертними дослідженнями, що забезпечує їх доказове значення [4, с. 520].

Сучасна теорія підкреслює важливість використання інноваційних технологій, зокрема штучного інтелекту, у діяльності правоохоронних органів. Практично це проявляється у використанні аналітичних систем для обробки великих масивів інформації: телефонних з'єднань, фінансових операцій, даних з відкритих джерел. Наприклад, під час розслідування економічних злочинів такі системи дозволяють швидко встановити зв'язки між підконтрольними підприємствами та виявити схеми відмивання коштів [5, с. 15].

Експертно-криміналістична діяльність у теорії розглядається як застосування спеціальних знань для дослідження доказів, а на практиці це знаходить відображення у проведенні широкого спектра експертиз. Зокрема, у справах щодо кіберзлочинності активно застосовуються комп'ютерно-технічні експертизи, які дозволяють відновлювати видалені файли, встановлювати IP-адреси та ідентифікувати осіб, причетних до злочину [6, с. 134]. У свою чергу, ДНК-експертизи широко використовуються для ідентифікації учасників організованих груп, що значно підвищує рівень доведеності вини.

Окремим напрямом модернізації є використання технічних засобів спостереження. Теоретично це обґрунтовується необхідністю підвищення ефективності збору інформації, а на практиці — застосуванням безпілотних літальних апаратів. Наприклад, дрони

використовуються для фіксації переміщення учасників злочинних угруповань або контролю за незаконною діяльністю на віддалених територіях. Проте практика свідчить, що недотримання процесуальних вимог може призвести до визнання таких доказів недопустимими [8, с. 169].

Крім того, важливим теоретичним принципом є міжвідомча взаємодія, яка на практиці реалізується через спільні операції Національної поліції, СБУ та прокуратури. Наприклад, при викритті організованих злочинних схем у фінансовій сфері здійснюється обмін інформацією між різними органами, що дозволяє комплексно підійти до розслідування та підвищити його ефективність [6, с. 210].

У контексті євроінтеграції теоретичні положення щодо гармонізації законодавства з європейськими стандартами знаходять практичне втілення у впровадженні електронних систем управління кримінальними провадженнями, підвищенні прозорості діяльності правоохоронних органів та посиленні контролю за дотриманням прав людини [7, с. 8].

Водночас практика виявляє низку проблем: недостатнє технічне оснащення окремих підрозділів, складність правового регулювання новітніх технологій, а також потребу у підвищенні кваліфікації працівників. Це підтверджує теоретичний висновок про необхідність комплексного підходу до модернізації, який включає як удосконалення законодавства, так і реальне впровадження сучасних методів роботи [3, с. 5].

Отже, поєднання теоретичних засад і практичних механізмів модернізації оперативно-розшукової та експертно-криміналістичної діяльності є ключовою умовою ефективної протидії організованій злочинності, що дозволяє не лише реагувати на злочини, а й попереджати їх у сучасних умовах.

Список використаних джерел:

1. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII (ред. від 09.08.2024). URL: https://zakon.rada.gov.ua/laws/show/2135-12

2. Про судову експертизу: Закон України від 25.02.1994 р. №4038-XII (чинна редакція від 01.01.2026). URL: https://ips.ligazakon.net/document/T403800

3. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про адміністративну процедуру»: Закон України від 10.10.2024 р. № 3410-IX.

4. Криміналістика: підручник / В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько. Харків: Право, 2024. 1008 с.
5. Шевчук О. О., Моргун Н. С. Використання штучного інтелекту в оперативно-розшуковій діяльності. Аналітично-порівняльне правознавство. 2026. № 1. URL: https://journal-app.uzhnu.edu.ua/article/view/353254
6. Криміналістика та судова експертиза: сучасний стан і перспективи розвитку: матеріали II Всеукр. наук.-практ. конф. (м. Київ, 20 червня 2025 р.) / відп. упоряд.: К. М. Ковальов та ін. Київ: ДНДЕКЦ МВС України, 2025. 788 с.
7. План заходів з виконання рекомендацій Європейської Комісії «Пакунок розширення 2023» / Розпорядження КМУ від 2025 р. URL: https://www.kmu.gov.ua/ storage/app/uploads/public/ 67f/62d /b04/67f62db04261d522958395.pdf
8. Асламов О., Єфімов В. Використання дронів в оперативно-розшуковій діяльності: практичні аспекти та правові обмеження. Матеріали конференцій МЦНД. 2024. С. 164–171.

АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Чернов Микола Миколайович
кандидат юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін,
Одеського державного університету внутрішніх справ

Сучасний стан організованої злочинності характеризується високим рівнем адаптивності злочинних угруповань до соціально-економічних, політичних та технологічних змін. Умови воєнного стану, активна цифровізація суспільних процесів, поширення транснаціональних кримінальних зв'язків та використання злочинними структурами сучасних інформаційно-комунікаційних технологій суттєво ускладнюють діяльність правоохоронних органів щодо виявлення, документування та припинення організованої злочинної діяльності. За таких обставин особливого значення набуває якісне аналітичне забезпечення процесу прийняття

управлінських рішень, яке дозволяє своєчасно оцінювати криміногенні загрози, прогнозувати розвиток оперативної обстановки та визначати найбільш ефективні напрями протидії організованій злочинності [1].

Аналітичне забезпечення управлінської діяльності у правоохоронній сфері являє собою сукупність організаційних, інформаційних, методичних та технологічних заходів, спрямованих на збір, обробку, узагальнення, оцінку та інтерпретацію інформації для підготовки обґрунтованих управлінських рішень. Основною метою такого забезпечення є формування достовірної інформаційної основи для визначення пріоритетів діяльності правоохоронних органів, розподілу ресурсів, планування оперативно-службових заходів та оцінювання результативності реалізованих заходів протидії організованій злочинності. Ефективність управлінських рішень безпосередньо залежить від повноти та якості аналітичної інформації, яка використовується керівництвом під час їх підготовки та реалізації [1].

Важливим напрямом розвитку аналітичного забезпечення є впровадження методів кримінального аналізу, які дозволяють досліджувати структуру злочинних мереж, встановлювати взаємозв'язки між учасниками організованих груп, виявляти закономірності їх діяльності та прогнозувати можливі напрями розвитку кримінальних процесів. Застосування інструментів аналізу зв'язків, геоінформаційного аналізу, аналізу соціальних мереж та методів обробки великих масивів даних створює передумови для переходу від реактивної моделі діяльності правоохоронних органів до проактивної моделі, орієнтованої на попередження злочинної діяльності. Дослідження сучасних підходів до аналізу організованої злочинності свідчать, що використання мережевого аналізу дозволяє більш ефективно виявляти структуру злочинних об'єднань та оцінювати ступінь впливу окремих учасників на функціонування кримінальних мереж [2].

Особливої актуальності набуває інтеграція різнорідних інформаційних ресурсів у єдині аналітичні системи. Об'єднання даних оперативно-розшукової діяльності, кримінальних проваджень, фінансового моніторингу, відкритих джерел інформації та міжнародних інформаційних ресурсів сприяє формуванню комплексної картини криміногенної ситуації. Використання сучасних

інформаційно-аналітичних платформ забезпечує автоматизацію процесів виявлення ризиків, аналізу тенденцій та підтримки прийняття управлінських рішень на стратегічному, оперативному та тактичному рівнях управління [1].

Водночас ефективність аналітичного забезпечення значною мірою залежить від рівня підготовки аналітичного персоналу та впровадження сучасних методологічних підходів до аналізу інформації. Фахівці з кримінального аналізу повинні володіти компетентностями у сфері системного аналізу, інформаційних технологій, статистичного моделювання, аналізу даних та оцінювання ризиків. Лише за умови комплексного поєднання сучасних технологій і професійної аналітичної діяльності можливо забезпечити належний рівень інформаційної підтримки управлінських процесів у сфері протидії організованій злочинності [2].

Таким чином, аналітичне забезпечення є одним із ключових елементів сучасної системи протидії організованій злочинності. Його розвиток повинен ґрунтуватися на впровадженні інноваційних методів кримінального аналізу, інтеграції інформаційних ресурсів, використанні сучасних інформаційних технологій та вдосконаленні професійної підготовки аналітиків. Реалізація зазначених напрямів сприятиме підвищенню обґрунтованості управлінських рішень, оптимізації використання ресурсів правоохоронних органів та підвищенню ефективності державної політики у сфері протидії організованій злочинності.

Список використаних джерел:

1. Europol. European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025. Luxembourg : Publications Office of the European Union, 2025. 100 p. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf .

2. Nicolás-Carlock J. R., Luna-Pla I. Organized crime behavior of shell-company networks in procurement: prevention insights for policy and reform. PLOS ONE. 2025. Vol. 20, No. 1. URL: https://arxiv.org/abs/2307.10028 .

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ ПРАВОПОРУШЕННЯМ У ПРИКОРДОННІЙ СФЕРІ

Ширкунов Олексій Дмитрійович
курсант факультету безпеки державного кордну
Каштелян Сергій Олександрович
доцент кафедри прикордонної служби,
кандидат військових наук, доцент

Сучасні виклики, що стоять перед державним кордоном України, вимагають від правоохоронних органів не лише фізичної присутності на рубежах, а й впровадження нових інтелектуальних методів роботи. Традиційне патрулювання місцевості, хоч і залишається основою охорони, часто виявляється недостатньо ефективним проти організованих злочинних угруповань, які використовують технічні новинки та складні схеми для перетину кордону або контрабанди. [1, С. 552-555] У таких умовах саме кримінальний аналіз стає ключовим інструментом, який дозволяє прикордонникам діяти на випередження, перетворюючи звичайний збір інформації на реальну перевагу над правопорушниками.

Кримінальний аналіз у прикордонній сфері за своєю суттю є процесом глибокого вивчення всіх наявних даних про порушення закону на кордоні. Це робота з інформацією, що надходить з різних джерел: від технічних засобів спостереження, оперативних даних, статистики затримань та результатів огляду транспортних засобів. Головна мета аналітика полягає у тому, щоб знайти приховані закономірності, які неможливо побачити при поверхневому погляді на ситуацію. Це дозволяє прикордонній службі відмовитися від простого реагування на події та перейти до їх прогнозування.

Одним із найважливіших аспектів такої роботи є аналіз часу та місця вчинення правопорушень. Вивчення статистики дозволяє чітко визначити «гарячі точки» на ділянці кордону, де злочинці з'являються найчастіше. Це може бути пов'язано з особливостями рельєфу, наявністю лісових масивів або віддаленістю підрозділів охорони. Аналізуючи ці фактори разом із часовими показниками, наприклад, графіком зміни нарядів чи погодними умовами, аналітики допомагають командирам ефективніше

розставляти сили, концентруючи увагу саме на небезпечних напрямках у найбільш вірогідний час порушення. [2, С. 236-240]

Окрім географічного аналізу, надзвичайно важливою є робота з профілюванням порушників. На основі аналізу попередніх затримань створюється детальний портрет особи, яка може бути причетна до незаконної діяльності. Це допомагає інспекторам на пунктах пропуску швидше виявляти підозрілих осіб у загальному потоці людей. Такий підхід базується на вивченні поведінкових ознак, маршрутів подорожі та документів. Водночас аналіз допомагає розкривати складні мережі зв'язків, виявляючи організаторів, які зазвичай знаходяться далеко від лінії кордону, але керують процесами контрабанди чи незаконного переправлення осіб.

Практична значущість кримінального аналізу також полягає в суттєвій економії державних ресурсів. Завдяки точним аналітичним прогнозам зникає потреба в однаково інтенсивному патрулюванні всієї протяжності кордону.[3, С.150-160] Сили та засоби спрямовуються туди, де вони дійсно потрібні, що підвищує результативність роботи при менших витратах пального та людських зусиль. Це робить систему охорони кордону гнучкою та здатною швидко адаптуватися до змін у тактиці злочинців.

Попри значні переваги, розвиток цього напряму в Україні стикається з певними викликами, серед яких головним є необхідність підготовки кваліфікованих фахівців, здатних працювати з великими масивами даних. Також важливою залишається технічна складова: забезпечення підрозділів сучасним програмним забезпеченням для візуалізації зв'язків та створення електронних карт. Перспективним шляхом розвитку є посилення обміну аналітичною інформацією з колегами з сусідніх країн, що дозволяє бачити повну картину злочинної діяльності ще до того, як правопорушник наблизиться до державного рубежу.[4, С. 126-131]

На завершення варто підкреслити, що роль кримінального аналізу в прикордонній сфері лише зростатиме. Він перетворює прикордонну службу на сучасний, високотехнологічний орган, де головною зброєю стає інформація та вміння нею користуватися. Саме якісний аналіз дозволяє забезпечити надійний захист кордонів, роблячи їх прозорими для чесних громадян і непрохідними для порушників закону.

Список використаних джерел:

1. Ланде Д. В. OSINT у кібербезпеці : навчальний посібник. Київ : ТОВ «Інжинірінг». 2024. С. 552 -555

2. Федчак І. Кримінальний аналіз : навчальний посібник Львівського державного університету Внутрішніх справ. 2014. С. 236 – 240.

3. Кіреєва О. Основи кримінального аналізу : навчальний посібник Хмельницького Видавництва НАДПСУ, 2022. С. 150-160.

4. Кудінов С., Шехавцов Р., науковий посібник : Методичні рекомендації щодо використання OSINT-інструментів у діяльності правоохоронних органів. Київ: НАВС. 2023. С. 126-131.

СЕКЦІЯ 2.
РОЗВИТОК СИСТЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

КІБЕРБЕЗПЕКА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ОРГАНАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ВИКЛИКИ ВОЄННОГО СТАНУ

Бичкова О.О.
студентка юридичного факультету
ЧНУ імені Петра Могили
інспектор ГУНП в Одеській області, м. Одеса, Україна

В умовах повномасштабної агресії проти України кіберпростір став повноцінним театром воєнних дій. Державні установи, і насамперед органи системи Міністерства внутрішніх справ та Національної поліції України (НПУ), перебувають під постійними атаками ворожих хакерських угруповань. Оскільки підрозділи поліції практично повністю перейшли на цифрові рейки, ключовим об'єктом захисту стає Система електронного документообігу (СЕД), яка акумулює службову інформацію, персональні дані співробітників та громадян, а також відомості, що становлять таємницю досудового розслідування. Забезпечення надійної кібербезпеки каналів передачі, обробки та зберігання службової документації в підрозділах документального забезпечення наразі є критично важливою умовою збереження стійкості всієї системи правопорядку.

Проблема вразливості систем електронного документообігу державних органів перед цілеспрямованими кібератаками (APT-атаками) залишається однією з найгостріших у сфері національної безпеки. За даними Державної служби спеціального зв'язку та захисту інформації України, понад 60 % усіх кіберінцидентів у державному секторі починаються із методів соціальної інженерії, зокрема цільового фішингу (Spear Phishing), спрямованого на працівників канцелярій та діловодів [1, с. 15]. Зловмисники маскують шкідливі вкладення (віруси-шифрувальники, трояни) під виглядом офіційних запитів, судових рішень або звернень громадян. Дослідження

Радбезу ООН показують, що успішна кібератака на інформаційні ресурси правоохоронних органів може призвести до блокування операційної діяльності відомства, витоку конфіденційних баз даних та втрати цифрових доказів, що завдає колосальних збитків державним інтересам [2, с. 31]. У відповідь на ці загрози виникає нагальна потреба модернізації організаційних та технічних протоколів кіберзахисту електронного діловодства.

Сучасні виклики кібербезпеки вимагають відходу від пасивного захисту периметра мережі до концепції «нульової довіри» (Zero Trust). Це означає, що кожен документ, який надходить до СЕД НПУ із зовнішніх джерел (електронна пошта, урядові портали, флеш-носії), повинен проходити багаторівневу автоматизовану перевірку. Особливу небезпеку становлять макроси у файлах форматів .doc/.docx та приховані скрипти в PDF-документах. Міжнародний досвід захисту поліцейських мереж доводить, що використання технологій автоматичного очищення та реконструкції вмісту файлів (Content Disarm and Reconstruction - CDR) дозволяє нейтралізувати приховані кіберзагрози ще до моменту, коли працівник підрозділу документального забезпечення відкриє документ на своєму робочому місці. Таким чином, кібербезпека документообігу є базовим елементом загальної системи кіберзахисту НПУ.

Правову основу забезпечення кібербезпеки в органах поліції становить комплекс національного законодавства та стратегічних документів. Конституція України визначає захист суверенітету і територіальної цілісності держави як найважливішу функцію всього суспільства, що в сучасних реаліях прямо поширюється на кіберпростір [3]. Базовий Закон України «Про основні засади забезпечення кібербезпеки України» відносить інформаційні системи МВС та Нацполіції до об'єктів критичної інформаційної інфраструктури, які підлягають першочерговому та посиленому захисту [4]. Також діяльність підрозділів документального забезпечення регламентується Законом України «Про захист інформації в інформаційно-комунікаційних системах», який вимагає обов'язкової сертифікації СЕД та створення Комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю [5].

У контексті євроінтеграційних зобов'язань України важливим орієнтиром є Директива ЄС про заходи для високого спільного рівня кібербезпеки в межах Союзу (Директива NIS 2), яка висуває

жорсткі вимоги до кібергігієни суб'єктів державного сектору, управління ризиками ланцюгів постачання програмного забезпечення та обов'язкового звітування про кіберінциденти [6]. Крім того, Стратегія кібербезпеки України, затверджена Указом Президента, прямо наголошує на необхідності безперервного моніторингу безпеки відомчих правоохоронних мереж в режимі 24/7.

Станом на першу половину 2026 року в Національній поліції України триває розгортання оновлених контурів безпеки СЕД. Ключовим технологічним кроком є інтеграція Системи електронного документообігу з Галузевим центром кіберзахисту МВС та Системою управління кіберінцидентами (SIEM). Будь-який електронний документ, що надходить на адресу поліції від зовнішніх кореспондентів, спочатку потрапляє в ізольоване хмарне середовище («пісочницю» / Sandbox), де аналізується його поведінка. Тільки після отримання позитивного цифрового маркера безпеки документ стає доступним інспектору канцелярії для реєстрації та накладання електронного цифрового підпису (ЕЦП).

Порівняно зі стандартами НАТО та практикою провідних країн, де кібербезпека правоохоронних органів базується на повній ізоляції службових мереж від публічного інтернету (інтранет-системи), Україна змушена будувати гібридні моделі захисту, оскільки поліція має залишатися відкритою для комунікації з громадянами в умовах війни. Наприклад, у Поліції безпеки Естонії (Kapo) електронний документообіг розділений на три незалежні контури безпеки залежно від грифу обмеження доступу, а обмін даними між ними відбувається через суворо контрольовані односпрямовані шлюзи (Data Diodes) [7]. У Федеральному бюро розслідувань США (FBI) діє жорстка система автентифікації персоналу, що включає біометричний контроль та поведінковий аналіз дій користувача в мережі для виявлення внутрішніх загроз (Insider Threats) [8].

З метою підвищення рівня кібербезпеки електронного документообігу НПУ в умовах сучасних загрози, доцільно впровадити такі організаційно-технічні заходи:

- розробити та впровадити обов'язковий відомчий стандарт регулярного навчання (кібертренінгів) для працівників підрозділів документального забезпечення з питань розпізнавання методів соціальної інженерії та фішингу;

- забезпечити перехід СЕД НПУ на технологію багатофакторної автентифікації (MFA) для всіх користувачів, із прив'язкою до апаратних ключів безпеки;
- впровадити технологію CDR для автоматичного видалення активного вмісту (макросів, посилань) із вхідних файлів офісних форматів перед їх реєстрацією;
- посилити контроль за використанням персональних цифрових підписів (ЕЦП) та запровадити автоматизований моніторинг аномальних дій користувачів у системі документообігу в неробочий час.

Реалізація цих кроків дозволить мінімізувати ризики успішних кібератак на органи Національної поліції України, захистить конфіденційну службову інформацію та забезпечить безперебійне функціонування підрозділів документального забезпечення в умовах сучасних гібридних загроз.

Список використаних джерел:

1. Аналітичний звіт про стан кібербезпеки в Україні у 2025 році / Держспецзв'язку. К., 2026. 54 с.

2. Cyber Threats to Law Enforcement Information Systems: Global Report 2024 / UN Security Council Counter-Terrorism Committee. New York, 2024. 120 p.

3. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР: поточ. ред. від 01.01.2020 р. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/ show/254к /96-вр#Text (дата звернення: 05.05.2026).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 01.01.2026 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 11.05.2026).

5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 16.11.2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 10.05.2026).

6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX: 32022L2555 (date of access: 14.05.2026).

7. Ilves K. Cyber Security Architecture of Estonian Law Enforcement Agencies. Tallinn: Academy of Security Sciences, 2025. 142 p.
8. FBI Information Security Program: Annual Report to Congress. Washington D.C.: FBI CJIS Division, 2024. 98 p.

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ У СИСТЕМІ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Давиденко В'ячеслав Віталійович
кандидат юридичних наук, доцент, ректор
Одеського державного університету внутрішніх справ.

Стрімка цифровізація суспільних відносин, активне впровадження інформаційно-комунікаційних технологій у діяльність органів державної влади, правоохоронних структур, фінансових установ, об'єктів критичної інфраструктури та приватного сектору зумовлюють формування принципово нової архітектури безпекового середовища, в межах якого кіберпростір перетворюється не лише на платформу функціонування сучасних інформаційних систем, але й на середовище реалізації складних транснаціональних кіберзлочинних практик. У сучасних умовах кіберзлочинність характеризується високим рівнем адаптивності, латентності, автоматизації та технологічної складності, що істотно ускладнює процеси виявлення, локалізації, аналізу та прогнозування кіберзагроз традиційними методами правоохоронної діяльності. Особливого значення набувають проблеми забезпечення своєчасного реагування на кіберінциденти, прогнозування потенційних атак, виявлення аномальної поведінки в інформаційних системах, аналізу цифрових слідів та побудови інтелектуальних моделей оцінювання криміногенних ризиків у кіберпросторі [1,2].

Трансформація сучасного кіберпростору у складну багаторівневу систему інформаційних взаємодій супроводжується постійним збільшенням обсягів цифрових даних, які генеруються як у процесі функціонування інформаційних систем, так і внаслідок діяльності суб'єктів кіберпростору. Вказані дані формують

надзвичайно складні масиви структурованої, напівструктурованої та неструктурованої інформації, обробка яких потребує використання інтелектуальних методів аналізу даних, здатних забезпечити виявлення прихованих закономірностей, аномалій, взаємозв'язків та потенційних загроз. Саме тому в сучасних умовах особливого значення набуває інтелектуальний аналіз даних як комплексна міждисциплінарна система методів, алгоритмів та технологій, спрямованих на автоматизоване отримання нових знань із великих масивів інформації для підтримки прийняття управлінських та оперативно-аналітичних рішень у сфері кібербезпеки та кримінального аналізу [1,3].

У контексті діяльності правоохоронних органів інтелектуальний аналіз даних набуває статусу стратегічного інструменту інформаційно-аналітичного забезпечення, оскільки дозволяє інтегрувати різнорідні інформаційні потоки, здійснювати оперативний моніторинг кіберзагроз, формувати моделі прогнозування кіберінцидентів та автоматизувати процеси аналітичної обробки інформації. На відміну від класичних методів аналізу, сучасні технології Data Mining, Machine Learning, Deep Learning та Big Data Analytics забезпечують можливість опрацювання надвеликих обсягів інформації у режимі реального часу, що є критично важливим у сфері протидії кіберзлочинності. Особливого значення набуває здатність інтелектуальних систем аналізувати мережевий трафік, виявляти ознаки шкідливого програмного забезпечення, здійснювати поведінковий аналіз користувачів, прогнозувати сценарії розвитку кіберзагроз та формувати автоматизовані рекомендації для прийняття рішень [1].

Сучасні кіберзагрози мають комплексний характер та реалізуються через багаторівневі механізми впливу на інформаційні системи, що потребує застосування системного підходу до організації процесів кіберзахисту. У межах системного аналізу кіберпростір розглядається як складна динамічна система, що включає сукупність взаємопов'язаних елементів, серед яких інформаційні ресурси, мережеві інфраструктури, програмно-апаратні комплекси, людський фактор, канали передачі даних та механізми інформаційної взаємодії. У такій системі кіберзагроза виступає як дестабілізуючий фактор, здатний порушити функціональну стійкість системи, знизити рівень її інформаційної безпеки та

спричинити значні соціально-економічні й безпекові наслідки. Саме тому виявлення та прогнозування кіберзагроз повинно ґрунтуватися на комплексному аналізі взаємозв'язків між елементами інформаційного середовища, оцінюванні ризиків та моделюванні потенційних сценаріїв реалізації кіберінцидентів [3].

Інтелектуальний аналіз даних у системі забезпечення кібербезпеки правоохоронних органів реалізується через використання широкого спектра методів математичного моделювання, статистичного аналізу, штучного інтелекту та машинного навчання. Одним із найбільш поширених напрямів є застосування алгоритмів класифікації для автоматичного розпізнавання кіберзагроз на основі попередньо визначених характеристик. У процесі реалізації такого підходу використовуються методи дерева рішень, випадкового лісу, опорних векторів, нейронних мереж та байєсівських класифікаторів, які дозволяють здійснювати високоточне виявлення підозрілої активності в інформаційних системах. Водночас ефективність подібних моделей значною мірою залежить від якості навчальних вибірок, репрезентативності даних та здатності алгоритмів адаптуватися до нових типів кіберзагроз.

Особливого значення набуває використання методів кластеризації для виявлення прихованих структур у масивах інформації та групування об'єктів за подібними характеристиками. У контексті кібербезпеки зазначені методи дозволяють ідентифікувати аномальні мережеві з'єднання, виявляти нетипову поведінку користувачів, аналізувати структуру бот-мереж та встановлювати закономірності функціонування шкідливих програмних комплексів. Кластерний аналіз забезпечує можливість виявлення нових, раніше невідомих типів кіберзагроз, що є надзвичайно важливим у контексті постійної еволюції засобів кібератак та зростання рівня їх технологічної складності.

Важливу роль у системі прогнозування кіберзагроз відіграють технології глибинного навчання, які забезпечують здатність автоматизованих систем самостійно виявляти складні нелінійні залежності у великих масивах даних. Використання багатошарових нейронних мереж дозволяє реалізувати механізми інтелектуального аналізу мережевого трафіку, розпізнавання патернів атак, прогнозування поведінки кіберзлочинців та автоматичного виявлення ознак компрометації інформаційних систем. Особливого

значення набувають рекурентні нейронні мережі та архітектури типу LSTM, які здатні аналізувати часові ряди та прогнозувати розвиток кіберзагроз на основі попередніх сценаріїв атак [1].

Не менш важливим напрямом є застосування технологій обробки природної мови для аналізу інформації з відкритих джерел, соціальних мереж, тематичних форумів та даркнет-середовища. Використання OSINT-технологій у поєднанні з інтелектуальним аналізом даних дозволяє правоохоронним органам здійснювати моніторинг інформаційного простору з метою виявлення ознак підготовки кібератак, поширення шкідливого програмного забезпечення, незаконного обігу персональних даних та функціонування кіберзлочинних угруповань. Аналіз текстової інформації, автоматизоване виділення сутностей, побудова семантичних зв'язків та виявлення інформаційних аномалій створюють передумови для формування систем раннього попередження про потенційні кіберзагрози.

У сучасних умовах особливого значення набуває концепція проактивного кіберзахисту, яка передбачає не лише реагування на вже реалізовані кіберінциденти, але й прогнозування потенційних загроз та попередження їх виникнення. Реалізація такого підходу є неможливою без використання інтелектуальних систем аналізу даних, здатних забезпечити автоматизоване оцінювання ризиків, виявлення слабких місць інформаційної інфраструктури та формування сценаріїв можливих кібератак. У межах зазначеної концепції особливу роль відіграють предиктивні моделі, які використовують історичні дані, статистичні закономірності та поведінкові характеристики для прогнозування майбутніх подій у сфері кібербезпеки.

Водночас впровадження інтелектуального аналізу даних у діяльність правоохоронних органів супроводжується низкою проблем організаційного, технологічного та правового характеру. Однією з ключових проблем є необхідність забезпечення високого рівня якості та достовірності даних, що використовуються для навчання інтелектуальних моделей. Наявність неповних, суперечливих або застарілих даних може суттєво знижувати ефективність систем прогнозування та призводити до формування помилкових управлінських рішень. Крім того, значною проблемою залишається забезпечення інтерпретованості моделей машинного навчання, оскільки складні нейронні архітектури нерідко функціонують за принципом

«чорної скриньки», що ускладнює процес обґрунтування прийнятих рішень у межах правоохоронної діяльності.

Не менш актуальними залишаються питання інформаційної безпеки самих інтелектуальних систем аналізу даних. Сучасні кіберзлочинці активно використовують методи маніпулювання навчальними вибірками, атак на моделі машинного навчання та механізми обходу систем автоматичного виявлення загроз. У зв'язку з цим особливого значення набуває розроблення стійких до атак інтелектуальних систем, здатних функціонувати в умовах активної протидії з боку кіберзлочинних структур. Додатково актуалізується проблема захисту персональних даних та забезпечення балансу між ефективністю аналітичної діяльності й дотриманням прав людини у сфері цифрової безпеки.

Перспективним напрямом розвитку інтелектуального аналізу даних у діяльності правоохоронних органів є інтеграція технологій штучного інтелекту з системами ситуаційної обізнаності, цифровими платформами кримінального аналізу та автоматизованими центрами реагування на кіберінциденти. Використання SIEM-систем, SOAR-платформ та технологій Threat Intelligence створює передумови для формування єдиного інформаційно-аналітичного середовища, здатного забезпечити комплексний моніторинг кіберпростору, автоматизовану кореляцію подій безпеки та оперативне реагування на загрози. У поєднанні з технологіями Big Data та хмарними обчисленнями зазначені рішення дозволяють суттєво підвищити швидкість та ефективність аналізу інформації [1-3].

Особливу роль у системі інтелектуального аналізу даних відіграє кримінальний аналіз як міждисциплінарний напрям інформаційно-аналітичної діяльності, спрямований на виявлення закономірностей злочинної активності, прогнозування криміногенних процесів та підтримку прийняття управлінських рішень. У сфері кібербезпеки кримінальний аналіз дозволяє інтегрувати інформацію про кіберінциденти, поведінкові характеристики кіберзлочинців, маршрути поширення шкідливого програмного забезпечення та фінансові операції у цифровому середовищі. На основі комплексного аналізу цифрових слідів формуються аналітичні профілі кіберзлочинних угруповань, визначаються закономірності їх діяльності та прогнозуються потенційні напрями реалізації кіберзагроз.

Таким чином, інтелектуальний аналіз даних у системі виявлення та прогнозування кіберзагроз виступає одним із ключових елементів сучасної моделі забезпечення кібербезпеки правоохоронних органів. Використання технологій штучного інтелекту, машинного навчання, математичного моделювання та системного аналізу дозволяє суттєво підвищити ефективність інформаційно-аналітичної діяльності, забезпечити своєчасне виявлення кіберзагроз, прогнозування потенційних кіберінцидентів та підтримку прийняття управлінських рішень у сфері протидії кіберзлочинності. Подальший розвиток зазначеного напряму потребує комплексного вдосконалення нормативно-правового забезпечення, розвитку інформаційної інфраструктури, підготовки висококваліфікованих фахівців у сфері кримінального аналізу та кібербезпеки, а також інтеграції сучасних інтелектуальних технологій у практичну діяльність правоохоронних органів України.

Список використаних джерел:

1. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень: навчальний посібник. Одеса: РВВ ОДУВС. 2022. 176 с.

2. Основи кримінального аналізу: навчально-методичні рекомендації до вивчення навчальної дисципліни /уклад. Калугін В.Ю., О.А. Балтовський Одеса: ОДУВС, 2022. 58 с.

3. Сучасні підходи щодо адаптивного автоматизованого управління складними системами в умовах невизначеності: монографія. /Кокошко ВИС та ін.; за заг. ред. Форос Г.В. Одеса: ОДУВС, 2020. 180 с.

КІБЕРБЕЗПЕКА В УКРАЇНІ: ЕТАПИ ЕВОЛЮЦІЇ ТА ОСНОВНІ НАПРЯМКИ РОЗВИТКУ В СУЧАСНИХ РЕАЛІЯХ

Гузенко Олена Павлівна
кандидат економічних наук, доцент
доцент кафедри економіки та публічного управління
ННІ права та соціального менеджменту
Донецький державний університет внутрішніх справ

Кібербезпека в Україні сприяє формуванню системи захисту інформаційних електронних потоків, які відіграють пріоритетну роль в прийняті управлінських рішень на різних рівнях. В основу правової бази кібербезпеки законодавець поклав створення базової платформи безпечного кіберпростору для захисту держави, суспільства та громадян, а також посилення спроможностей протидії кіберзагрозам. Проте плинність часу, сучасні воєнні виклики вказали на необхідність осучаснення існуючих правових норм і стандартів, що призвело до необхідності впровадження нових правових ініціатив, які більш придатні до сучасних реалів. Актуальним для вирішення залишається питання не лише переосмислення та розуміння ключових напрямків розвитку та забезпечення кібербезпеки в сучасних реаліях, а, й визначення еволюційних етапів її становлення. Все вище викладене свідчить про актуальність напрямку вивчення.

У колі наукової спільноти питання зміцнення та розвитку кібербезпеки не втрачає своєї актуальності та знаходить відображення в монографічних дослідженнях, стає предметом обговорення на різних наукових дискусійних платформах різного рівня. О. Довгань, А. Тарасюк та Т. Ткачук [1] у монографічних дослідженнях розкрили кібербезпеку з позиції «суспільства знань», а проблемі теоретико-правового аспекту кібербезпеки держави присвятила свою працю Н.І.Логінова [2]. Однак ряд питань з позиції обраної проблематики вивчення залишаються дискусійними, неоднозначними та потребують більш поглибленого дослідження.

Правова платформа, розробки та затвердження кібербезпеки в Україні пройшла певний еволюційний шлях. На початку в 2014 році питання стосувалося захисту інформаційних потоків в державних органах з урахуванням заходів кібербезпеки. Наступним кроком, у 2014-2017 роках з початком воєнних дій в окремих

областях Україні, збільшилася кількість кібератак, виникла нагальна потреба швидкого реагування, з метою їх нівелювання та розробки нормативно-правового забезпечення. Саме в цей період було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» [3], який визначив основні напрямки захисту. Окрім цього, законодавець затверджує Положення про Національний координаційний центр кібербезпеки [4], основним завданням якого стало забезпечення координації діяльності суб'єктів національної безпеки, прогнозування реальних(потенційних) кіберзагроз та оперативне реагування на них.

З 2017-2021 роки почався процес інституціоналізації та стратегічного розвитку, котрий відзначився затвердженням Стратегії кібербезпеки України [5], яка мала за мету створення безпечного кіберпростору з урахуванням захисту національних інтересів.

Одним із основних еволюційних етапів, ми вважаємо, є період з 2022-2026 роки, який характеризується наступними сегментами: активна адаптація цифрових інструментів та адаптивну безпеку в системі кіберзахисту; впровадження ризик-орієнтованого підходу, що дозволяє швидко оновлювати та вдосконалювати правову базу кібербезпеки з врахуванням появи нових видів загрози. та ризиків; впровадження асиметричних інструментів стримування кібератак, на базі світового досвіду та посилення зв'язків співпраці з іноземними партнерами; осучаснення системи захисту критичної інфраструктури тощо.

Окрему увагу варто приділити основним напрямкам зміцнення кібербезпеки в умовах сьогодення Серед них найбільш пріоритетними виступають: посилення захисту державних мереж, які представлено об'єктами критичної інфраструктури; посилення взаємодії з зарубіжними партнерами з питань оперативного виявлення та протидії кібератакам; адаптацію новітніх цифрових інструментів з метою осучаснення систем моніторингу та шифрування для захисту закритих даних; вдосконалення методів навчання державних службовців основам безпеки в інтернеті, з метою протидія фішингу та дезінформації; осучаснення законодавчої платформи в системі кіберзахисту з позиції адаптації до воєнних реалій та розбудови системи створення національних кібервійськ.

Таким чином, в Україні необхідно продовжити вдосконалювати систему розвитку та зміцнення кібербезпеки в умовах сьогодення. Активно впроваджувати світовий досвід, продовжувати співпрацю з зарубіжними партнерами, забезпечувати розробку

змін до існуючих правових важелів націлених на розширення мережі використання цифрових інструментів, інноваційних методів захисту від кібератак.

Список використаних джерел:

1. Кібербезпека «суспільства знань»: монографія/ О. Довгань, А.Тарасюк,Т. Ткачук. Київ-Одеса: Фенікс, 2021. 176 с.

2. Логінова Н. І. Кібернетична безпека держави: теоретико-правовий аспект: монографія. Харків: Право, 2023. 224 с.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 06.05.2026 року).

4. Про Національний координаційний центр кібербезпеки: положення затверджене Указом Президента України від 7 червня 2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 06.05.2026 року).

5. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12(дата звернення: 06.05.2026 року)

РОЗВИТОК СИСТЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

Єпіфанцева Вероніка Філіпівна
здобувач вищої освіти бакалавра
1 курс, 1 група, «Правоохоронна діяльність»
Одеського державного університету внутрішніх справ
Науковий керівник: ***Домніцак Володимир Володимирович***
Завідувач науково-дослідної лабораторії
з актуальних питань кримінального аналізу
кандидат юридичних наук, доцент

У XXI столітті інформаційні технології стали ключовим елементом функціонування сучасного суспільства. Практично всі сфери діяльності людини пов’язані з використанням цифрових систем: державне управління, банківський сектор, медицина, освіта, транспорт, енергетика та оборонна галузь. Разом із розвитком цифровізації стрімко зростає кількість кіберзагроз, які

можуть становити серйозну небезпеку як для окремих громадян, так і для держави загалом. У сучасних умовах кібербезпека перетворилася на один із ключових напрямів національної безпеки України [1, с. 12].

Для України проблема кіберзахисту має особливе значення через складну геополітичну ситуацію та постійний тиск у кіберпросторі. Сучасні конфлікти дедалі частіше мають гібридний характер, коли поряд із військовими діями використовуються інформаційні операції, кібератаки та дестабілізація цифрової інфраструктури. Саме тому розвиток системи кібербезпеки є необхідною умовою забезпечення стабільності держави та захисту її інформаційного простору [2, с. 25].

Сучасні кіберзагрози мають складний і багаторівневий характер. Якщо раніше основними небезпеками були комп'ютерні віруси або окремі випадки несанкціонованого доступу до систем, то сьогодні кібератаки часто є добре спланованими операціями. Зловмисники використовують спеціалізоване шкідливе програмне забезпечення, фішингові кампанії, атаки на сервери та мережі, методи соціальної інженерії, а також інструменти для викрадення або знищення інформації [3, с. 41].

Одним із найбільш поширених типів кіберзагроз є фішинг. Його суть полягає у введенні користувача в оману з метою отримання конфіденційної інформації, наприклад логінів, паролів або банківських даних. Найчастіше такі атаки здійснюються через електронну пошту або підроблені вебсайти. Значна частина успішних атак відбувається саме через людський фактор, адже навіть найсучасніші технічні системи не можуть повністю захистити від помилок користувачів [4, с. 87].

Ще однією серйозною проблемою є DDoS-атаки, під час яких зловмисники перевантажують сервери великою кількістю запитів, через що ресурси стають недоступними для користувачів. Такі атаки можуть бути спрямовані на державні установи, банки, засоби масової інформації або підприємства критичної інфраструктури. Метою подібних дій є порушення роботи систем, створення паніки та зниження довіри до державних інституцій.

Україна вже неодноразово ставала об'єктом масштабних кібератак. Одним із найвідоміших прикладів стала атака вірусу Petya у 2017 році. Унаслідок цієї атаки було порушено роботу

державних установ, банків, транспортних компаній, аеропортів та багатьох приватних підприємств. Шкідливе програмне забезпечення швидко поширювалося комп'ютерними мережами та блокувало доступ до інформації. Збитки від цієї атаки були значними не лише для України, а й для міжнародних компаній, що ще раз підтвердило глобальний характер кіберзагроз [2, с. 64].

Після масштабних кібератак питання кібербезпеки стало одним із пріоритетів державної політики. Україна почала активніше розвивати систему кіберзахисту, удосконалювати законодавство та створювати спеціалізовані органи для боротьби з кіберзлочинністю. Важливим етапом стало ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» [1].

На сьогодні в Україні функціонують різні структури, відповідальні за кібербезпеку. Одну з ключових ролей виконує Державна служба спеціального зв'язку та захисту інформації України. Вона забезпечує захист державних інформаційних ресурсів, організовує реагування на кіберінциденти та координує діяльність у сфері технічного захисту інформації. Також важливу роль відіграє CERT-UA — урядова команда реагування на комп'ютерні надзвичайні події [5].

Крім державних структур, активну участь у забезпеченні кібербезпеки беруть підрозділи кіберполіції. Вони займаються розслідуванням кіберзлочинів, виявленням шахрайських схем, боротьбою з незаконним обігом персональних даних та протидією кіберзлочинним угрупованням. З розвитком цифрових технологій кількість кіберзлочинів постійно зростає, тому діяльність кіберполіції стає дедалі важливішою [6, с. 49].

Сучасна система кібербезпеки неможлива без міжнародної співпраці. Оскільки кіберпростір не має державних кордонів, більшість загроз мають міжнародний характер. Україна активно співпрацює з країнами Європейського Союзу, НАТО та міжнародними організаціями у сфері обміну інформацією про кіберзагрози, проведення спільних навчань і впровадження сучасних стандартів безпеки [7].

Особливу увагу слід приділити захисту критичної інфраструктури. До таких об'єктів належать енергетичні системи, транспортні мережі, банківський сектор, телекомунікації та медичні

установи. Порушення роботи цих систем може призвести до серйозних економічних і соціальних наслідків.

У сучасних умовах важливого значення набуває використання новітніх технологій у сфері кіберзахисту. Одним із перспективних напрямів є застосування штучного інтелекту для аналізу мережевої активності та виявлення підозрілих дій. Системи на основі машинного навчання можуть автоматично виявляти аномалії та реагувати на потенційні загрози значно швидше, ніж людина [8].

Ще одним важливим аспектом є проблема підготовки кваліфікованих спеціалістів у сфері кібербезпеки. Через швидкий розвиток технологій виникає постійна потреба у фахівцях, здатних працювати з сучасними системами захисту інформації. Українські заклади вищої освіти поступово розширюють програми підготовки спеціалістів із кібербезпеки, однак попит на таких працівників залишається дуже високим.

Не менш важливою є цифрова грамотність населення. Багато кібератак стають успішними саме через необережність користувачів. Використання простих паролів, відкриття підозрілих електронних листів, встановлення програм із ненадійних джерел можуть призвести до витоку персональних даних або зараження пристроїв шкідливим програмним забезпеченням [3, с. 96].

Отже, в умовах стрімкого розвитку інформаційних технологій та постійного зростання кількості кіберзагроз питання кібербезпеки набуває особливого значення для України. Сучасні кібератаки можуть впливати не лише на окремі інформаційні системи, а й на функціонування державних органів, банківського сектору, енергетики та критичної інфраструктури загалом. Саме тому формування ефективної системи кіберзахисту є одним із ключових напрямів забезпечення національної безпеки держави.

Україна вже має значний досвід протидії масштабним кіберінцидентам, що стало поштовхом до вдосконалення законодавства, створення спеціалізованих структур та розвитку міжнародного співробітництва у сфері кібербезпеки. Водночас сучасні виклики потребують постійного оновлення технологій захисту, впровадження інноваційних рішень та підготовки висококваліфікованих фахівців.

Таким чином, ефективний розвиток системи кібербезпеки України можливий лише за умови комплексного підходу, який поєднує

державну підтримку, сучасні технології, міжнародну взаємодію та відповідальне ставлення користувачів до захисту інформації.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України»
2. НІСД — Національний інститут стратегічних досліджень Дубов Д. В. *Кібербезпека України: сучасні виклики та механізми протидії*. — Київ : НІСД, 2021. — 176 с.
3. Видавництво «Ліра-К» Корченко О. Г., Архипов О. Є. *Основи кібербезпеки та кіберзахисту*. — Київ : Ліра-К, 2020. — 304 с.
4. ХНУРЕ — Харківський національний університет радіоелектроніки Білоус В. Т. *Інформаційна безпека та захист інформації в інформаційно-телекомунікаційних системах*. — Харків : ХНУРЕ, 2019. — 250 с.
5. CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події України
6. Наукові публікації України Коваленко В. П. *Кіберзлочинність у сучасному інформаційному суспільстві* // Науковий вісник. — 2022. — №4. — С. 45–52.
7. OECD Digital Security Outlook 2023
8. NATO Cooperative Cyber Defence Centre of Excellence

СИСТЕМНО-АНАЛІТИЧНІ ПІДХОДИ ДО МОДЕЛЮВАННЯ РИЗИКІВ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

Жук Іван Васильович
доктор філософії, викладач кафедри
кримінально-правових дисциплін,
Одеського державного університету внутрішніх справ.

Сучасний етап розвитку глобального інформаційного суспільства характеризується масштабною цифровою трансформацією практично всіх сфер суспільного життя, що супроводжується інтенсивним впровадженням інформаційно-комунікаційних технологій у державне управління, фінансовий сектор, правоохоронну

діяльність, систему національної безпеки, освіту, охорону здоров'я та функціонування об'єктів критичної інфраструктури. Формування цифрової економіки, розвиток технологій штучного інтелекту, інтернету речей, хмарних сервісів, великих даних та кіберфізичних систем суттєво змінюють архітектуру сучасного соціально-економічного середовища, створюючи нові можливості для інноваційного розвитку держави та суспільства. Водночас зазначені процеси супроводжуються виникненням принципово нових ризиків та загроз, пов'язаних із трансформацією кіберпростору у складне багаторівневе середовище функціонування кіберзлочинності. У сучасних умовах кіберзлочинність виступає одним із найбільш динамічних та технологічно адаптивних видів злочинної діяльності, що характеризується високим рівнем латентності, транснаціональним характером, використанням механізмів анонімізації, автоматизації атак та штучного інтелекту [1].

Особливістю сучасної кіберзлочинності є її здатність до швидкої адаптації до нових технологічних умов, що значно ускладнює процеси виявлення, прогнозування та нейтралізації кіберзагроз традиційними методами правоохоронної діяльності. Сучасні кіберінциденти дедалі частіше реалізуються у формі складних багатоступеневих атак, які поєднують технічні, соціальні, психологічні та інформаційні механізми впливу на інформаційні системи. За таких умов особливого значення набуває формування нових концептуальних підходів до дослідження ризиків кіберзлочинності, заснованих на інтеграції системного аналізу, математичного моделювання, інтелектуального аналізу даних та сучасних інформаційно-аналітичних технологій. Саме системно-аналітичний підхід дозволяє забезпечити комплексне дослідження закономірностей функціонування кіберпростору, оцінювання ризиків та прогнозування можливих сценаріїв розвитку кіберзагроз у процесі цифрової трансформації суспільства.

У сучасній науковій парадигмі кіберпростір розглядається як складна динамічна система, що включає значну кількість взаємопов'язаних елементів, серед яких інформаційні ресурси, телекомунікаційні мережі, цифрові сервіси, програмно-апаратні комплекси, користувачі інформаційних систем та механізми інформаційної взаємодії. Функціонування такої системи супроводжується постійною генерацією інформаційних потоків, високим рівнем

невизначеності та значною кількістю потенційних ризиків, що створює передумови для виникнення кіберзагроз різного рівня складності. У межах системного аналізу ризик кіберзлочинності розглядається як імовірність реалізації негативного сценарію розвитку подій у кіберпросторі, що може призвести до порушення конфіденційності, цілісності або доступності інформації, дестабілізації функціонування інформаційних систем та завдання шкоди державним, суспільним чи приватним інтересам [2].

Особливого значення у процесі дослідження кіберзлочинності набуває концепція системного ризику, відповідно до якої кіберзагрози розглядаються не ізольовано, а як елементи складної мережі взаємопов'язаних ризикогенних факторів. Такий підхід дозволяє враховувати взаємозалежність між різними компонентами інформаційної інфраструктури, а також аналізувати ефекти каскадного поширення кіберінцидентів у межах цифрового середовища. У сучасних умовах навіть локальний кіберінцидент здатний спричинити масштабні наслідки для функціонування державних систем управління, фінансового сектору, транспортної інфраструктури та критично важливих об'єктів. Саме тому моделювання ризиків кіберзлочинності потребує використання комплексних системно-аналітичних підходів, здатних враховувати нелінійний характер розвитку кіберзагроз та багатовимірність сучасного кіберпростору.

У процесі моделювання ризиків кіберзлочинності особливу роль відіграють методи системного аналізу, які забезпечують можливість структуризації складних інформаційних процесів, виявлення взаємозв'язків між елементами системи та формування моделей поведінки кіберзлочинних структур. Системний аналіз дозволяє розглядати кіберзлочинність як адаптивну систему, здатну до самоорганізації, модифікації механізмів функціонування та використання новітніх технологій для реалізації злочинної діяльності. У межах зазначеного підходу значна увага приділяється дослідженню структури кіберзагроз, аналізу джерел ризиків, оцінюванню рівня уразливості інформаційних систем та прогнозуванню потенційних сценаріїв реалізації кіберінцидентів [3].

Важливим напрямом системно-аналітичного моделювання є використання методів математичного аналізу та статистичного прогнозування ризиків. Сучасні інформаційні системи генерують

надзвичайно великі обсяги даних про функціонування мереж, поведінку користувачів, мережевий трафік та кіберінциденти, що створює передумови для використання технологій Big Data та інтелектуального аналізу даних у процесі оцінювання ризиків кіберзлочинності. Використання математичних моделей дозволяє формалізувати процеси розвитку кіберзагроз, оцінювати ймовірність виникнення кіберінцидентів та прогнозувати потенційні наслідки кібератак. У сучасних умовах особливого значення набувають методи регресійного аналізу, теорії ймовірностей, марковських процесів, теорії графів та імітаційного моделювання, які забезпечують можливість комплексного дослідження динаміки розвитку кіберзлочинності.

Не менш важливим напрямом є використання когнітивного моделювання для аналізу ризиків кіберзлочинності. Когнітивний підхід дозволяє досліджувати причинно-наслідкові зв'язки між різними факторами ризику та формувати сценарії розвитку кіберзагроз залежно від зміни параметрів інформаційного середовища. Використання когнітивних карт створює можливість візуалізації взаємозв'язків між елементами системи кібербезпеки, визначення ключових факторів впливу та моделювання поведінки складних динамічних систем. У контексті цифрової трансформації суспільства зазначений підхід дозволяє враховувати не лише технічні аспекти кіберзагроз, але й соціальні, організаційні, психологічні та економічні чинники, що впливають на розвиток кіберзлочинності.

Особливого значення набуває інтеграція системного аналізу із технологіями штучного інтелекту та машинного навчання. Сучасні кіберзагрози характеризуються високим рівнем динамічності та здатністю до постійної модифікації, що потребує використання адаптивних інтелектуальних систем аналізу інформації. Використання алгоритмів машинного навчання дозволяє автоматизувати процеси виявлення аномалій, аналізу мережевого трафіку, прогнозування кібератак та оцінювання ризиків функціонування інформаційних систем. Особливого значення набувають нейронні мережі, алгоритми класифікації, кластеризації та предиктивної аналітики, які забезпечують можливість формування інтелектуальних моделей прогнозування розвитку кіберзагроз у режимі реального часу [3].

У сучасних умовах кіберзлочинність дедалі частіше набуває ознак організованої мережевої діяльності, що функціонує у глобальному цифровому середовищі. Кіберзлочинні угруповання використовують механізми криптографічного захисту, технології анонімізації, децентралізовані інформаційні мережі та ресурси даркнету для реалізації злочинних схем. У зв'язку з цим особливого значення набувають методи мережевого аналізу та моделювання соціальних графів, які дозволяють досліджувати структуру кіберзлочинних мереж, виявляти ключові вузли інформаційної взаємодії та прогнозувати поведінку суб'єктів кіберпростору. Інтеграція мережевого аналізу із системним моделюванням створює передумови для формування комплексних моделей оцінювання ризиків кіберзлочинності у цифровому середовищі.

Не менш важливим аспектом є використання системно-аналітичних підходів у процесі підтримки прийняття управлінських рішень у сфері кібербезпеки. У сучасних умовах управління кіберризиками потребує оперативного аналізу значних обсягів інформації, оцінювання динаміки розвитку загроз та формування ефективних стратегій реагування на кіберінциденти. Використання інтелектуальних систем підтримки прийняття рішень дозволяє автоматизувати процеси аналізу інформації, прогнозування ризиків та формування рекомендацій для суб'єктів управління. У межах таких систем реалізуються механізми інтеграції даних із різних джерел, автоматизованого моніторингу інформаційного середовища та оцінювання рівня кіберзагроз у режимі реального часу [3].

Водночас процес моделювання ризиків кіберзлочинності супроводжується низкою складних проблем методологічного та технологічного характеру. Однією з ключових проблем є високий рівень невизначеності сучасного кіберпростору, що обумовлений динамічністю розвитку технологій, швидкою модифікацією механізмів кібератак та постійною зміною структури інформаційного середовища. Значна частина кіберзагроз має латентний характер, що ускладнює процеси збору достовірної інформації та формування адекватних моделей прогнозування. Крім того, сучасні кіберінциденти нерідко мають комплексний характер, поєднуючи технічні, інформаційно-психологічні та соціальні механізми впливу, що потребує використання міждисциплінарних підходів до аналізу ризиків.

Особливого значення набуває проблема забезпечення достовірності та повноти інформації, яка використовується для моделювання ризиків кіберзлочинності. У сучасному цифровому середовищі значна кількість інформації характеризується фрагментарністю, суперечливістю та наявністю маніпулятивного контенту, що може суттєво впливати на якість аналітичних оцінок. У зв'язку з цим необхідним є вдосконалення механізмів верифікації інформації, розвитку систем цифрової ідентифікації та формування інтегрованих інформаційно-аналітичних платформ кримінального аналізу.

Перспективним напрямом розвитку системно-аналітичних підходів до моделювання ризиків кіберзлочинності є інтеграція технологій цифрових двійників, хмарних обчислень, штучного інтелекту та систем ситуаційної обізнаності. Використання цифрових моделей інформаційної інфраструктури дозволяє здійснювати імітаційне моделювання кіберінцидентів, аналізувати наслідки потенційних кібератак та оцінювати ефективність механізмів кіберзахисту. У поєднанні із технологіями Big Data та інтелектуального аналізу даних зазначені підходи створюють передумови для формування адаптивних систем управління ризиками кіберзлочинності, здатних функціонувати в умовах високого рівня невизначеності та динамічного розвитку цифрового середовища.

Таким чином, системно-аналітичні підходи до моделювання ризиків кіберзлочинності виступають одним із ключових напрямів розвитку сучасної системи забезпечення кібербезпеки в умовах цифрової трансформації суспільства. Інтеграція системного аналізу, математичного моделювання, інтелектуального аналізу даних та технологій штучного інтелекту дозволяє забезпечити комплексне дослідження кіберзагроз, прогнозування сценаріїв розвитку кіберінцидентів та підтримку прийняття управлінських рішень у сфері кібербезпеки. Подальший розвиток зазначеного напряму потребує вдосконалення методологічних засад кримінального аналізу, розвитку інформаційної інфраструктури, підготовки висококваліфікованих фахівців у сфері системного аналізу та кібербезпеки, а також інтеграції сучасних цифрових технологій у практичну діяльність правоохоронних органів України.

Список використаних джерел:

1. Бірман, В. М. Системний аналіз: підручник / В. М. Бірман. Київ: Знання, 2022. 416 с.

2. Мельник, О. В. Системний аналіз: навчальний посібник / О. В. Мельник, В. В. Кожушко. Київ: Видавничий дім «Академія», 2022. 304 с.

3. Системний аналіз: теорія і практика / В. В. Коваленко, В.М. Коваленко. 2-ге вид., перероб. та доп. К.: НТУУ «КПІ імені Ігоря Сікорського»,

ЩОДО ВИКЛИКІВ ТА КІБЕРЗАГРОЗ НАЦІОНАЛЬНОМУ КІБЕРПРОСТОРУ УКРАЇНИ

Звездін Ігор Валерійович, *аспірант*
Одеського державного університету внутрішніх справ.

Сучасний національний кіберпростір України функціонує в умовах системного та довготривалого впливу гібридних загроз, які інтегрують кібернетичні, інформаційно-психологічні та воєнні компоненти. У цих умовах кіберпростір фактично набуває статусу окремого операційного середовища, в якому здійснюється не лише несанкціоноване втручання в інформаційні системи, але й цілеспрямований вплив на процеси державного управління, економічну стабільність та суспільну довіру до інституцій. Особливістю сучасного етапу є зростання масштабованості атак та їхньої адаптивності, що ускладнює традиційні підходи до кіберзахисту та потребує переходу до моделі кіберстійкості як ключового принципу функціонування державних інформаційних систем [1].

Актуальний стан кібербезпеки України у 2025–2026 роках характеризується поступовим удосконаленням інституційної та технологічної складової національної системи захисту кіберпростору. Зокрема, відзначається посилення координаційної ролі державних органів у сфері реагування на кіберінциденти, а також розширення механізмів взаємодії між суб'єктами критичної інфраструктури та правоохоронними структурами. Водночас, попри позитивну динаміку розвитку нормативної бази та організаційних процедур, зберігається низка системних проблем, серед яких недостатній рівень уніфікації технічних стандартів захисту, обмеженість ресурсного забезпечення окремих секторів та нерівномірність впровадження сучасних технологій кіберзахисту на

регіональному рівні. Це створює асиметрії у загальній архітектурі національної кібербезпеки, що потенційно може бути використано зловмисниками [1].

Окремого наукового аналізу потребує трансформація характеру кіберзагроз, яка відбувається під впливом стрімкого розвитку технологій штучного інтелекту та автоматизованих систем атак. Сучасні кіберзлочинні угруповання дедалі частіше використовують алгоритми машинного навчання для автоматизації фішингових кампаній, створення адаптивного шкідливого програмного забезпечення та обходу систем виявлення вторгнень. Це формує якісно новий рівень загроз, за якого атаки стають більш швидкими, менш передбачуваними та значно складнішими для ідентифікації традиційними методами аналізу. Відповідно, зростає потреба у впровадженні інтелектуальних систем кібермоніторингу, здатних здійснювати поведінковий аналіз мережевого трафіку та виявляти аномалії в режимі реального часу [2].

Важливою складовою проблематики є також нормативно-правове та організаційне забезпечення кібербезпеки, яке в умовах воєнного стану набуває особливої значущості. У 2025 році було посилено механізми державного управління у сфері реагування на кіберінциденти шляхом запровадження більш уніфікованих процедур координації між різними рівнями суб'єктів кіберзахисту. Це дозволило підвищити швидкість реагування на інциденти та рівень взаємодії між державним і приватним сектором. Однак залишаються проблемні аспекти, пов'язані з недостатньою інтеграцією приватних компаній у національну систему обміну кіберінформацією, а також з обмеженим рівнем міжнародної інтеграції у сфері спільного протидії транснаціональним кіберзагрозам [1].

Окремим критичним фактором, що впливає на стан національного кіберпростору, є людський ресурс і рівень кіберобізнаності персоналу. Практика показує, що значна частина успішних кіберінцидентів реалізується не через технічні вразливості, а через соціоінженерні атаки, які експлуатують недостатній рівень обізнаності користувачів. Це підкреслює необхідність формування системної політики кіберосвіти, яка повинна охоплювати як державний сектор, так і приватні організації. Формування культури кібергігієни є стратегічним елементом зниження загального рівня

кіберризиків у національному масштабі та потребує довгострокових інвестицій у навчання та підготовку кадрів [2].

Таким чином, сучасні виклики та кіберзагрози національному кіберпростору України мають комплексний, багаторівневий характер і охоплюють технологічні, організаційні, правові та людські аспекти. Ефективна протидія цим загрозам можлива лише за умови подальшого розвитку інтегрованої системи кібербезпеки, яка базується на принципах кіберстійкості, міжвідомчої взаємодії, застосування інтелектуальних технологій аналізу даних та активної міжнародної співпраці у сфері кіберзахисту.

Список використаних джерел

1. Рада національної безпеки і оборони України. *Огляд стану кібербезпеки 2025*. Київ: НКЦК при РНБО України, 2026. URL: https://www.rnbo.gov.ua/ua/Diialnist/7559.html .

2. Кабінет Міністрів України. *Постанова №1533 від 26.11.2025 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»*. Офіційний портал Верховної Ради України, 2025–2026. URL: https://www.golos.com.ua/article/388876 .

ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Капуляк Віталій Петрович
доктор філософії, доцент кафедри
адміністративно-правових дисциплін
Одеського державного університету внутрішніх справ

Сучасний етап розвитку цифрового суспільства в Україні характеризується різким зростанням інтенсивності та складності кіберзагроз, що обумовлює необхідність формування цілісної системи принципів забезпечення кібербезпеки. У законодавчому вимірі базові засади державної політики у сфері кібербезпеки закріплено в Законі України «Про основні засади забезпечення кібербезпеки України», який визначає організаційно-правові основи захисту критичної інфраструктури, державних інформаційних ресурсів та прав громадян у кіберпросторі [1]. У контексті воєнного стану ці принципи набувають особливої актуальності, оскільки кіберпростір

стає окремим доменом гібридного протистояння, що вимагає інтеграції оборонних, правоохоронних та цивільних інституцій.

Одним із ключових принципів забезпечення кібербезпеки є принцип системності та комплексності, який передбачає узгоджене функціонування всіх суб'єктів національної системи кібербезпеки. Оновлені стратегічні документи підкреслюють необхідність розвитку координації між державними органами, приватним сектором та міжнародними партнерами, а також формування єдиного простору обміну кіберінформацією [2]. Такий підхід відповідає сучасним міжнародним стандартам, зокрема NIST Cybersecurity Framework та ISO/IEC 27001, які імплементуються в українську практику через нормативні акти та урядові рішення.

Наступним фундаментальним принципом є принцип ризик-орієнтованого управління кібербезпекою. Його сутність полягає у переході від формального дотримання вимог до постійної оцінки кіберризиків та адаптації захисних механізмів відповідно до рівня загроз. Уряд України запроваджує нові підходи до оцінювання стану кіберзахисту, які базуються на міжнародних стандартах і передбачають обов'язкове застосування ризик-менеджменту для об'єктів критичної інфраструктури [3]. Це дозволяє забезпечити більш гнучку та ефективну модель реагування на кіберінциденти.

Важливе значення має принцип кіберстійкості критичної інфраструктури, який передбачає здатність державних та приватних систем зберігати функціональність навіть в умовах кібератак. Відповідні урядові документи наголошують на необхідності впровадження багаторівневих механізмів захисту, безперервного моніторингу та швидкого відновлення інформаційних систем після інцидентів [2; 3]. У цьому контексті кіберстійкість розглядається як ключовий елемент національної безпеки, особливо в умовах воєнних загроз.

Окремим принципом виступає принцип міжнародної інтеграції та гармонізації кіберполітики. Україна активно імплементує європейські підходи до регулювання кібербезпеки, зокрема положення директиви NIS2 та рекомендації ENISA, що сприяє підвищенню сумісності національної системи кіберзахисту з міжнародними стандартами [3]. Така інтеграція дозволяє посилювати механізми транскордонного обміну інформацією про загрози та підвищувати ефективність спільного реагування на кіберінциденти.

Не менш значущим є принцип розвитку людського потенціалу та кіберосвіти. Сучасні підходи до кібербезпеки підкреслюють, що людський фактор залишається одним із ключових елементів кіберзахисту, а тому потребує постійного підвищення кваліфікації фахівців і формування культури кібергігієни в суспільстві [2]. У рамках реалізації державної кіберстратегії передбачено розвиток системи підготовки кадрів та підвищення рівня обізнаності населення щодо кіберзагроз.

Таким чином, система принципів забезпечення кібербезпеки в Україні формується як багаторівнева та динамічна конструкція, що поєднує правові, організаційні, технічні та міжнародні компоненти. Її розвиток відбувається у напрямі посилення кіберстійкості, ризик-орієнтованого управління та інтеграції до європейського безпекового простору, що є необхідною умовою забезпечення національної безпеки в умовах сучасних кіберзагроз.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 (зі змінами станом на 2025 р.). – Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 .

2. Ukraine’s Cybersecurity Strategy 3.0: A Course Toward Cyber Resilience, Digital Sovereignty, and Proactive Cyber Defense // National Security and Defense Council of Ukraine. 2026. URL: https://www.rnbo.gov.ua/en/Diialnist/7637.html .

3. Government Adopts New Standardised Procedure for Cybersecurity Status Assessment // Government portal of Ukraine. 2026. URL: https://cip.gov.ua/en/news/uryad-zatverdiv-novii-poryadok-o cinyuvannya-stanu-kiberzakhistu .

РОЛЬ ДЕРЖАВНИХ ТА НЕДЕРЖАВНИХ ОРГАНІВ ТА ОРГАНІЗАЦІЙ У ПРОТИДІЇ КІБЕРБУЛІНГУ В УКРАЇНІ ТА СВІТІ

Кіріка Діана Володимирівна
кандидатка юридичних наук, доцентка,
доцентка кафедри адміністративної діяльності ННІ № 3
Харківського національного університету внутрішніх справ
Кіріка Вадим Георгійович
учень Кам'янець-Подільського ліцею № 18,
презер МАН України

Співпраця державних та недержавних органів та організацій у протидії кібербулінгу зумовлена стрімким поширенням цифрових технологій, активним використанням соціальних мереж і онлайн-платформ серед дітей та молоді, а також зростанням кількості випадків кібербулінгу в інформаційному просторі України та світу. У сучасних умовах кібербулінг став однією з найбільш небезпечних форм психологічного насильства, що негативно впливає на емоційний стан, психічне здоров'я та соціалізацію особистості. Кіберзагрози, зокрема через кібербулінг, зумовлюють необхідність міжнародної співпраці та координації дій. Така взаємодія реалізується через обмін інформацією, створення спільних робочих груп, участь у міжнародних заходах і розвитку національних стратегій кібербезпеки відповідно до міжнародних стандартів.

Особливої гостроти дана проблема набуває в умовах цифровізації суспільства та воєнного стану в Україні, коли значна частина комунікації, навчання і соціальної взаємодії відбувається в онлайн-середовищі. Це створює нові ризики для підростаючого покоління та потребує ефективної системи реагування з боку держави, правоохоронних органів, закладів освіти, громадських організацій і міжнародних партнерів.

Кіберзлочинність не знає кордонів, тому створення спільних ініціатив, обмін інформацією про кіберзагрози та координація дій між державами допоможуть створити безпечніший цифровий простір. Розбудова національної кіберстійкості не є суто внутрішньою справою, а потребує співпраці між державами, регіональними та міжнародними установами, корпоративним сектором,

науковцями та громадянським суспільством [1]. Ця співпраця може приймати різні форми та охоплювати багато аспектів, включаючи обмін інформацією, спільні дослідження та розвиток технологій. Державні установи, наприклад правоохоронні та розвідувальні служби, можуть ділитися даними про кіберзагрози з приватними компаніями, які часто мають актуальну інформацію про нові методи атак і вразливості.

Багато країн беруть участь у спільних навчальних програмах і тренінгах, спрямованих на розвиток знань і навичок, спроможніх значно знизити ймовірність успішної кібератаки. У Великій Британії школи зобов'язані впроваджувати політики протидії кібербулінгу, тому вчителі перевіряють цифровий контент учнів, застосовуючи дисциплінарні заходи. У Швеції школи розробляють плани безпечного середовища, а відповідальність за реагування на булінг і кібербулінг покладається на директорів і педагогів. В Іспанії та Ірландії відповідні дії охоплюються нормами про традиційний булінг і погрози, а в ряді країн – через інститут харасменту як форми дискримінації. У Великій Британії, Франції, Румунії, Угорщині та Австрії відповідальність настає, зокрема, за використання інформаційно-комунікаційних технологій для переслідувань. Окремі країни запроваджують відповідальність онлайн-платформ і провайдерів, а також превентивні механізми захисту дітей, зокрема маркування шкідливого контенту, експертизу цифрових продуктів та спеціалізовані мобільні додатки для звернень до поліції. Поряд із цим поширюються лінії допомоги, онлайн-підтримка, інформаційні кампанії та освітні проєкти, включно з використанням аудіовізуальних і культурних форм впливу.

До органів та організацій, що протидіють кібербулінгу у світі належать: UNICEF (проводить міжнародні кампанії проти булінгу; створює освітні програми; підтримує країни у розробці політик безпеки в інтернеті), UNESCO (розробляє рекомендації щодо безпечної поведінки онлайн; досліджує масштаби кібербулінгу у різних країнах), International Telecommunication Union (ITU) (запускає глобальні ініціативи цифрової безпеки; створює рекомендації для урядів); StopBullying.gov та Cyberbullying Research Center – як офіційні платформи США містить поради, гарячі лінії та ресурси щодо протидії кібербулінгу; проводить дослідження кібербулінгу та готує матеріали для освітніх закладів і державних

інституцій; European Union Safer Internet Programme, що являє собою мережу центрів «Safer Internet Center» у країнах ЄС та має гарячі лінії, центри допомоги, навчальні програми.

В Україні такими органів та організацій, що протидіють кібербулінгу, є: Міністерство освіти і науки України (МОН), яке впроваджує програми протидії булінгу в закладах освіти та зобов'язує школи розробляти плани реагування на булінг; Національна поліція України (кіберполіція), яка реагує на скарги щодо кібербулінгу, маючи онлайн-форми для подання заяв про кіберзлочини; Міністерство цифрової трансформації України зокрема платформа «Дія. Цифрова освіта» – курси з цифрової грамотності та кібербезпеки та кампанії щодо безпечної поведінки в інтернеті; Уповноважений Верховної Ради України з прав людини, який розглядає звернення щодо порушень прав людини, включаючи булінг та може ініціювати перевірки освітніх закладів; Ла Страда–Україна – Гаряча лінія для дітей і підлітків – 116 111, яка працює цілодобово і безкоштовно, надаючи консультації щодо булінгу, насильства, небезпек онлайн; StopBullying – українські громадські ініціативи, які проводять тренінги в школах та розробляють навчальні матеріали для вчителів, дітей і батьків; ChildFund Alliance – українські проєкти, які реалізовують інформаційні кампанії проти насильства серед дітей, включно з кібербулінгом.

Першими комплексними кроками, що робить держава у напрямку забезпечення прав дитини в цифровому середовищі та протидії цькуванню в Інтернеті є Національна стратегія захисту дітей у цифровому середовищі на 2021–2026 рр. [2], інститут Освітнього омбудсмена, який розглядає звернення учасників освітнього процесу та за результатами такого розгляду може надсилати подання щодо проведення службових розслідувань, надавати рекомендації, вимагати відновлення прав або припинення порушення прав; аналізує дотримання законодавства стосовно учасників освітнього процесу, які постраждали від булінгу (цькування), стали його свідками або вчинили булінг (цькування); може безперешкодно відвідувати заклади освіти, представляти інтереси осіб у суді [3].

Вважаємо за необхідне приділити окрему увагу Департаменту кіберполіції – міжрегіональному територіальному підрозділу Національної поліції України (далі – НПУ), що входить до структури кримінальної поліції НПУ та згідно із законодавством України

здійснює оперативно-розшукову діяльність [4]. Саме цей Департамент НПУ несе відповідальність за законотворення, захист жертв, кримінальне переслідування, превентивні заходи, розслідування кіберзлочинів.

Важливу роль у протидії кібербулінгу в Україні відіграють і громадські організації та неурядові ініціативи, які займаються просвітництвом, правовою допомогою, інформаційною підтримкою, допомогою жертвам, через Всеукраїнську ініціативу (bullyingstop.org.ua) або ініціативи, які входять до складу Центр безпечного Інтернету. Державні та приватні організації можуть об'єднати зусилля для проведення досліджень кібербезпеки. Це може включати розробку нових технологій безпеки, а також дослідження методів запобігання кіберзлочинам. Спільні ініціативи можуть призвести до створення більш ефективних рішень, які враховують як державні, так і комерційні інтереси, при цьому освіта відіграє ключову роль у покращенні кібербезпеки. Державні установи можуть співпрацювати з приватними компаніями для розробки навчальних програм, семінарів та онлайн-курсів з підвищення обізнаності про кіберзагрози та методи захисту. Так наприклад, з метою більшого залучення приватного сектору до протидії кіберзагрозам, в ЄС була створена Європейська платформа публічно-приватного партнерства стійкості. В рамках агентства Європол діє Європейський Центр протидії кіберзлочинності [5].

Комплексний підхід до вирішення проблеми кіберзлочинності потребує спільних зусиль усіх зацікавлених сторін. Вивчення особливостей співпраці державних і недержавних організацій сприятиме формуванню комплексного підходу до захисту учасників цифрового середовища та підвищенню ефективності національної системи кібербезпеки України. Практика показує, що протидія кібербулінгу є більш результативною за умови координації діяльності кіберполіції, органів державної влади, освітніх установ, громадських організацій та міжнародних інституцій. Створення спільних робочих груп, форумів дозволяє ефективно взаємодіяти між різними секторами. Обмін інформацією, спільні дослідження, освітні програми та законодавчі ініціативи можуть значно покращити кібербезпеку та захистити як організації, так і громадян від кіберзагроз.

Список використаних джерел:

1. Upgrading National Cyber Resilience. Tallinn: E-Governance Academy, 2022. URL:https://ega.ee/wp-content/uploads/2021/05 /NCSI-Cyber-Resilience-Digi_F.pdf
2. Національна Стратегія захисту дітей в цифровому середовищі на 2021 – 2026 роки. URL: https://thedigital.gov.ua/ documents/legislation/natsionalna-strategiya-zakhistu-ditey-v-tsifrovomu-seredovishchi-na-2021-2026-roki
3. Протидія кібербулінгу: суб'єкти реагування та механізми захисту порушених прав дитини. *HAS | Higher school of advocacy:* веб-сайт. URL: https://www.hsa.org.ua/blog/protydiya-kiberbulingu-sub-yekty-reaguvannya-ta-mehanizmy-zahystu-porushenyh-prav-dytyny
4. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 № 85 (в редакції наказу Національної поліції України від 07.11.2019 № 1136).
5. Ramses A. Wessel, 2015. «Towards EU cybersecurity law: Regulating a new policy field,» Chapters, in: *Research Handbook on International Law and Cyberspace,* chapter 19, pages 403–425, Edward Elgar Publishing. URL: https://ideas.repec.org /h/elg/ eechap/15436_19.html

ДО ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ В СУЧАСНИХ УМОВАХ РОЗВИТКУ

Кадала Віталій Віталійович
кандидат юридичних наук, доцент,
доцент кафедри господарсько-правових
дисциплін та економічної безпеки
Донецький державний університет внутрішніх справ

В умовах воєнного конфлікту кібербезпека виступає запорукою підтримки рівня національної безпеки, що сприяє захищеності інформаційних потоків, котрі з використовуються як при воєнних діях, так і в процесах розвитку країни взагалі. Наявні гібридні загрози та їх вплив на систему кібербезпеки вказують на

необхідність постійного осучаснення змісту заходів націлених на їх мінімізацію. В умовах воєнного конфлікту рольовий сегмент кібербезпеки зростає та вказує на доцільність посилення системи захисту енергетичних та транспортних мереж, фінансово-банківської системи країни, представників підприємницького сектору, державних установ від кібератак, котрі можуть призвести до викривлення інформаційного потоку, а, як наслідок, до прийняття хибних рішень або взагалі втрати інформації. Все окреслене свідчить про необхідність та доцільність на базі системного підходу впроваджувати заходи зміцнення рівня кібербезпеки в країні, котра охоплена воєнним конфліктом. Зазначене підкреслює сучасність і актуальність обраного напрямку вивчення.

Проблематичні та правові аспекти процесу кібербезпеки доволі часто виступають предметом досліджень в працях вітчизняних науковців. Результати проведених досліджень оприлюднюються на тематичних науково-практичних конференціях різного рівня, викладаються в форматі дисертаційних та монографічних досліджень. Так, ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту стали предметом вивчення О.Д. Довгань та І.М. Дороніна [1]. Натомість, системі виявлення вторгнень та функціональній стійкості розподілених інформаційних систем до кібернетичних загроз було присвячено монографічні дослідження Н.В. Лукова-Чуйко, С.В. Толюпа, В.С. Наконечний, М.М. Браіловський [2]. Не зменшуючи цінність та результативність наукових розробок вітчизняних науковців, варто зауважити, що окремі питання процесу кібербезпеки викладено фрагментарно, що вказало на доцільність поглиблення окремих питань обраної проблематики.

Варто зазначити, за останні роки в Україні законодавець ініціював ряд правових регуляторів, які створили доволі потужну платформу для розвитку кібербезпеки. Базовим законодавчим регулятором виступає Закон України «Про основні засади забезпечення кібербезпеки України» [3]. Цінність зазначеного правового регулятора полягає в тому, що законодавець деталізував правові норми і стандарти, розкрив види об'єктів кіберзахисту, а також визначив повноваження державних органів, які виступають учасниками процесу кібербезпеки.

У 2025 році, з метою розвитку та вдосконалення процесу кібербезпеки законодавець приймає Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [4]. Правовим регулятором законодавець закріплює ряд інноваційних компонентів: в контексті об'єктів критичної інфраструктури змінено підхід до формування різних видів профілів безпеки (базових, цільових, галузевих) на ризикоорієнтований, що надасть можливість приймати більш змістовні управлінські рішення з урахуванням існуючих викликів сьогодення; вдосконалення роботи національна команда реагування CERT-UA, на базі впровадження інноваційних, цифрових інструментів у питаннях розслідування кібератак, надання допомоги у запобіганні та усуненні наслідків, проведення постійного моніторингу кіберзагроз, та посилення взаємодії з міжнародними партнерами; впровадження обов'язкової сертифікації захисту інформаційного потоку на відповідність стандартам кібербезпеки. Окрім цього, акцентовано увагу законодавцем на тому, що вводиться заборона використання програмного забезпечення з країн-агресорів для державних та критичних інфраструктурних систем [4].

Можна констатувати, що правова база системи кібербезпеки включає Євроінтеграційні норми і стандарти в контексті NIS2. Основне призначення NIS2 полягає у введенні особистої відповідальності керівництва представників підприємницького сектору за кіберризики та посилення вимог до ланцюгів постачання, з метою запобігання виробничим ризикам.

Таким чином, Україна має доволі потужну правову базу щодо забезпечення кібербезпеки, котра постійно оновлюється за рахунок введення законодавчих ініціатив. Важливим сегментом формування правового регулювання системи кібербезпеки виступають процеси адаптації національного законодавства до стандартів ЄС, особливо в контексті NIS2.

Список використаних джерел:

1. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: АртЕк, 2018. 106 с.

2. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз: монографія / Н.В. Лукова-Чуйко, С.В. Толюпа, В.С. Наконечний, М.М. Браіловський. Київ: Формат, 2021. 407 с.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.05.2026 року)

4. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27 березня 2025 року, № 4336-IX**.** URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 05.05.2026 року)

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОНЛАЙН-ЗАГРОЗАМ ДЛЯ ДІТЕЙ ЗАСОБАМИ ЦИФРОВОЇ РОЗВІДКИ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Кочман Костянтин Павлович,
аспірант денної форми ІІІ курсу
Кафедри кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ

Глибока цифрова трансформація суспільних відносин і триваючий правовий режим воєнного стану зумовили якісно нову конфігурацію загроз життю, здоров'ю та правам дитини. Помітна частина дитячого населення України вимушено перебуває у дистанційному форматі навчання та комунікації, тривалий час проводячи у соціальних мережах, месенджерах та ігрових платформах. У цих умовах формується розширений «цифровий слід» неповнолітнього, який стає об'єктом інтересу не лише комерційних операторів, а й кіберзлочинців, зокрема ворожих спецслужб.

Завдання Національної поліції України та її Департаменту кіберполіції щодо формування безпекового середовища для дітей вимагає поєднання сучасних інструментів цифрової розвідки з виваженим адміністративно-правовим механізмом.

До основних онлайн-загроз для дітей у 2025-2026 рр. належать:

- кібергрумінг (online grooming) – налаштування довірчого контакту дорослого з дитиною з метою її подальшого сексуального розбещення;
- створення, поширення та споживання матеріалів сексуального насильства над дітьми (CSAM), що активно розповсюджуються через закриті чати месенджерів, файлообмінні платформи та сегмент даркнету;
- секстортинг – шантаж дитини інтимними матеріалами, отриманими шляхом маніпуляції;
- кібербулінг та мова ворожнечі в адресу неповнолітніх;
- вербувальна активність ворожих спецслужб та деструктивних угруповань, спрямована на залучення підлітків до диверсійної, підпалювальної чи розвідувальної діяльності;
- шахрайство щодо акаунтів і платіжних інструментів неповнолітніх.

Цифрова розвідка з відкритих джерел (OSINT) та її прикладний підвид – розвідка у соціальних мережах (SOCMINT) виступає ефективним інструментом виявлення зазначених загроз на ранніх стадіях. Моніторинг публічних каналів і чатів дозволяє виявляти патерни груминг-поведінки, маркери розповсюдження CSAM, координаційні точки вербування неповнолітніх. У поєднанні з технологіями штучного інтелекту (perceptual hashing для CSAM-сигнатур, NSFW-класифікатори, NLP-моделі для розпізнавання маніпулятивних розмов) цифрова розвідка перетворюється на превентивний інструмент захисту дітей.

Адміністративно-правовою основою діяльності органів Національної поліції у цій сфері є багаторівневий комплекс актів. На міжнародному рівні – Конвенція ООН про права дитини (1989) і Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Лансаротська конвенція, 2007), ратифікована Україною. На національному рівні – Закон України «Про охорону дитинства», Закон України «Про Національну поліцію», Закон України «Про основні засади забезпечення кібербезпеки

України», стаття 156-1 Кримінального кодексу України (домагання дитини для сексуальних цілей), стаття 173-4 Кодексу України про адміністративні правопорушення (булінг). Окреме значення мають положення Закону України «Про захист персональних даних», які обмежують межі дозволеного збирання й опрацювання інформації навіть у разі правомірної правоохоронної мети.

Період 2025-2026 рр. позначений якісним оновленням політико-правового ландшафту в цьому напрямі. Розпорядженням Кабінету Міністрів України від 14 липня 2025 р. № 708-р схвалено Національну стратегію захисту прав дитини у сфері юстиції на період до 2028 року, в якій окрема стратегічна ціль присвячена забезпеченню прав і свобод дитини в Інтернеті, запобіганню експлуатації та зловживанням щодо дітей у цифровому середовищі [3]. Документ прямо називає такі ризики, як онлайн-груминг, поширення матеріалів сексуального насильства над дітьми, кібербулінг та секстортинг. Розпорядженням Кабінету Міністрів України від 2 травня 2025 р. № 432-р затверджено Концепцію цифрової гігієни дітей дошкільного віку [4], що формує превентивний контур ще на стадії дошкільної освіти.

Паралельно посилюється інституційна архітектура кіберзахисту. Прийнятим Верховною Радою України 27 березня 2025 р. Законом про внесення змін до законодавства щодо захисту інформації та кіберзахисту державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури (законопроект № 11290) [1] передбачено формування єдиної національної системи реагування на кіберінциденти за участі CERT-UA, галузевих команд реагування, Національної поліції та СБУ. Така система створює технічне й правове підґрунтя для оперативного обміну інформацією про виявлені онлайн-загрози, зокрема щодо неповнолітніх.

Окремий вимір становить підготовка до системного використання технологій штучного інтелекту. Розпорядженням Кабінету Міністрів України від 9 травня 2025 р. № 457-р затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки, який передбачає, серед іншого, підготовку до IV кварталу 2026 року законопроекту щодо правового врегулювання у сфері ШІ та запровадження механізмів застосування ШІ для аналізу й прогнозування в державних органах [5]. Як справедливо зазначає М. А. Погорецький, інтеграція алгоритмічних

систем у процес доказування потребує визначення процесуального статусу їх результатів, верифікаційних процедур і механізмів оскарження [7]. Це особливо актуально для розслідування злочинів проти дітей, де AI-детекція CSAM, deepfake-контенту та маніпулятивних патернів комунікації стає ключовим інструментом.

Не менш важливим є питання процесуального закріплення цифрових слідів, виявлених засобами розвідки. О. Д. Квашук обґрунтовано наголошує, що ключовою для допустимості електронних доказів є цілісність ланцюга збереження від моменту їх виявлення до судового розгляду [2]. Л. В. Мілімко та Я. В. Жидовцев вказують на необхідність законодавчого закріплення категорії цифрових доказів у КПК України з урахуванням європейської практики [6]. У контексті злочинів проти дітей це передбачає особливі вимоги до фіксації скриншотів листування, дампів каналів, метаданих файлів CSAM – з одночасним дотриманням принципу мінімізації травматизації дитини-потерпілої. Серед основних проблем адміністративно-правового забезпечення цієї сфери слід виокремити:

- фрагментарність повноважень, коли Кіберполіція, ювенальна превенція, СБУ та органи освіти діють у межах різних відомчих логік, що ускладнює міжвідомчу координацію;
- обмежену юрисдикцію щодо платформ, серверні потужності яких розташовані за межами України;
- колізію між принципом таємниці листування та необхідністю проактивного сканування контенту на наявність CSAM;
- недостатню кадрову забезпеченість підрозділів спеціалістами з цифрової розвідки та цифрової криміналістики.

Перспективними напрямами розвитку є гармонізація національного законодавства з Регламентом Європейського Парламенту та Ради (ЄС) 2024/1689 («AI Act») у частині систем високого ризику, до яких потенційно належать ШІ-інструменти правоохоронної аналітики; запровадження інституту «трастових повідомлювачів» (trusted flaggers) у взаємодії з платформами електронних комунікацій; формування міжвідомчих робочих груп з виявлення жертв CSAM за участі Кіберполіції, Офісу Генерального прокурора, Уповноваженого Президента з прав дитини та міжнародних партнерів (Europol, NCMEC).

Висновок. Отже, протидія онлайн-загрозам для дітей у діяльності Національної поліції України дедалі більше базується на

синергії технологічних інструментів цифрової розвідки та належно сформованого адміністративно-правового механізму. Ухвалення у 2025 році низки концептуальних актів (розпорядження Кабінету Міністрів України № 708-р, № 457-р, № 432-р) та Закону № 11290 створило міцну стратегічну основу для подальших кроків.

Проте зміцнення цієї сфери потребує ухвалення спеціального законодавства про штучний інтелект із чітким процесуальним статусом результатів роботи AI-систем у досудовому розслідуванні, деталізації відомчих процедур збирання цифрових слідів засобами OSINT/SOCMINT із гарантіями прав дитини-потерпілої, формування сталих міжвідомчих координаційних механізмів і програм підвищення кваліфікації працівників ювенальної превенції та Кіберполіції у сфері цифрової розвідки.

Реалізація цих заходів забезпечить ефективне виконання конституційного обов'язку держави щодо охорони дитинства в умовах безпекових викликів воєнного часу та цифрової трансформації.

Список використаних джерел:

1. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27 березня 2025 р. (законопроект № 11290). URL: https://itd.rada.gov.ua/billinfo/Bills/Card/55573 (дата звернення: 10.05.2026).

2. Квашук О. Д. Використання електронних доказів у кримінальному провадженні. Центральноукраїнський вісник права та публічного управління. 2025. № 2. DOI: https://doi.org/ 10. 32782/cuj-2025-2-5.

3. Про схвалення Національної стратегії захисту прав дитини у сфері юстиції на період до 2028 року та затвердження операційного плану заходів з її реалізації у 2025—2028 роках: Розпорядження Кабінету Міністрів України від 14 липня 2025 р. № 708-р. URL: https://zakon.rada.gov.ua/laws/show/708-2025-%D1%80 (дата звернення: 12.05.2026).

4. Про схвалення Концепції цифрової гігієни дітей дошкільного віку: Розпорядження Кабінету Міністрів України від 2 травня 2025 р. № 432-р. URL: https://zakon.rada.gov.ua/laws/show/432-2025-%D1%80 (дата звернення: 11.05.2026).

5. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025—2026 роки : Розпорядження Кабінету Міністрів України від 9 травня 2025 р. № 457-р. URL: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80 (дата звернення: 13.05.2026).
6. Мілімко Л. В., Жидовцев Я. В. Електронні докази в кримінальному судочинстві України. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Т. 3. № 88. DOI: https://doi.org/10.24144/2307-3322.2025.88.3.45.
7. Погорецький М. А. Штучний інтелект у доказуванні в досудовому та судовому провадженнях: доктринальні засади і практика застосування. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Т. 4. № 91. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.56.

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ МОНІТОРИНГУ ДЛЯ ВИЯВЛЕННЯ ТА АНАЛІЗУ КІБЕРІНЦИДЕНТІВ

Макаров Артур Ігорович
кандидат юридичних наук, викладач кафедри кримінально-правових дисциплін, Одеського державного університету внутрішніх справ

Сучасний розвиток цифрової інфраструктури характеризується різким зростанням кількості та складності кіберзагроз, що зумовлює необхідність удосконалення підходів до виявлення та аналізу кіберінцидентів. Традиційні системи моніторингу, засновані на сигнатурному підході, виявляються недостатньо ефективними в умовах динамічних та раніше невідомих атак. У цьому контексті інтелектуальні системи моніторингу, що базуються на методах машинного навчання, аналізі великих даних та технологіях штучного інтелекту, стають ключовим інструментом забезпечення кібербезпеки інформаційних систем. Зокрема, сучасні підходи передбачають інтеграцію алгоритмів виявлення аномалій у мережевому трафіку та автоматизовану класифікацію подій

безпеки, що дозволяє значно підвищити швидкість реагування на інциденти та зменшити вплив людського фактора [1].

Інтелектуальні системи моніторингу кіберінцидентів базуються на поєднанні технологій SIEM (Security Information and Event Management), машинного навчання та методів глибокого аналізу даних. Їх ключовою особливістю є здатність до адаптивного навчання на основі історичних даних про атаки та поведінкові патерни користувачів і систем. Це дозволяє виявляти складні багатовекторні атаки, які не можуть бути ідентифіковані традиційними методами кореляційного аналізу подій. Додатково використання моделей глибокого навчання сприяє підвищенню точності прогнозування потенційних кіберінцидентів, що має критичне значення для превентивного захисту інформаційної інфраструктури [1].

Важливою складовою інтелектуальних систем моніторингу є використання гібридних моделей аналізу, які поєднують статистичні методи, графові підходи та нейронні мережі. Така інтеграція дозволяє здійснювати багаторівневу оцінку кіберризиків та формувати контекстуалізовану картину кіберсередовища. Особливо ефективним є застосування технологій обробки природної мови для аналізу журналів подій та кіберінтелекту (Threat Intelligence), що забезпечує автоматизоване вилучення індикаторів компрометації (IOC) і побудову моделей загроз у режимі реального часу. Це створює передумови для переходу від реактивної до проактивної моделі кіберзахисту [2].

Суттєвим напрямом розвитку інтелектуальних систем моніторингу є їх інтеграція з архітектурами генеративного штучного інтелекту, що дозволяє не лише виявляти інциденти, але й моделювати сценарії їх розвитку. Використання глибоких нейронних мереж і гіперграфових структур сприяє підвищенню точності класифікації складних інцидентів, а також забезпечує пояснюваність прийнятих рішень у системах кіберзахисту. Це особливо важливо для критичної інфраструктури, де необхідна не лише автоматизація виявлення загроз, але й можливість інтерпретації результатів аналізу для прийняття управлінських рішень [2].

Таким чином, інтелектуальні системи моніторингу кіберінцидентів є ключовим елементом сучасної архітектури кібербезпеки, що забезпечує перехід до проактивної, адаптивної та самонавчальної моделі захисту інформаційних систем. Подальший

розвиток цих систем пов'язаний із поглибленням інтеграції штучного інтелекту, розширенням використання великих даних та вдосконаленням методів аналізу складних мережевих структур кіберзагроз.

Список використаних джерел:

1. Schmitt, M. *Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection*. arXiv preprint arXiv:2401.01342, 2025. URL: https://arxiv.org/abs/2401.01342

2. Mishra, S., Alfahidah, R. A., Alharbi, F. *BERT-spaCy hybrid NLP and blockchain-enhanced adaptive CTI for IOC extraction and threat prediction*. Scientific Reports, 16, 8147 (2026). DOI: https://doi.org/10.1038/s41598-025-34505-2

КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: НОВІ ТЕХНОЛОГІЧНІ ВИКЛИКИ

Моргунова Тетяна Іванівна
к.т.н., доцент, доцент кафедри
кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ
Шипрінський Нікіта Олегович
здобувач першого (бакалаврського)
рівня вищої освіти спеціальності 081 «Право»
Одеського державного університету внутрішніх справ

Сучасний етап розвитку економіки характеризується глибокою цифровою трансформацією, яка охоплює практично всі сфери діяльності підприємств, організацій та державних інституцій.

Цифрова трансформація відбувається, коли організації впроваджують цифрові технології у всі свої операції [1].

Інтенсивне впровадження цифрових технологій сьогодні вже не виглядає як щось нове або виняткове, швидше як звична частина розвитку підприємств, хоча ще кілька років тому це сприймалося інакше. Хмарні сервіси, аналітика великих даних, рішення на основі штучного інтелекту, різні пристрої Інтернету речей поступово вбудовуються у повсякденну діяльність і дають

відчутний ефект, особливо коли мова йде про оптимізацію процесів або скорочення витрат. Разом із цим виникає інша сторона питання, яку іноді недооцінюють, – збільшення кількості кіберзагроз, причому не тільки кількісно, а й за складністю. Через це вже складно говорити про кібербезпеку як про окрему функцію, швидше це стає частиною загальної логіки управління, хоча не всі підприємства до цього готові.

Якщо дивитися на практику, то стає помітно, що кібербезпека поступово виходить за межі технічних підрозділів. У багатьох випадках вона вже впливає на стратегічні рішення, навіть якщо це прямо не визнається. Будь-який збій в інформаційній системі, або навіть незначний витік даних, може створити проблеми, які важко швидко компенсувати. Особливо це відчувається у компаніях, що працюють на зовнішніх ринках, де додається ще й фактор різних вимог і правил, інколи досить суперечливих. До речі, іноді саме регуляторні обмеження створюють більше труднощів, ніж самі технічні ризики.

Останнім часом змінюється і характер самих кіберзагроз. Якщо раніше це були переважно поодинокі спроби втручання, то зараз частіше йдеться про складніші сценарії, де поєднуються різні підходи. Наприклад, атаки типу «ransomware» або «фішинг» вже стали майже буденністю, але при цьому вони постійно змінюються і адаптуються.

«Ransomware» – це тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати комп'ютер [2].

«Фішингові» атаки мають на меті викрасти або пошкодити конфіденційну інформацію, примушуючи людей обманом розкрити свої персональні дані, зокрема паролі й номери кредитних карток [3].

Додаються ще й ризики, пов’язані з постачальниками програмного забезпечення, що іноді випадає з уваги. Усе це накладається на збільшення кількості пристроїв у мережі, і межі цієї мережі вже не так просто окреслити, як це було раніше.

Окремо варто згадати про хмарні технології, які, з одного боку, дійсно спрощують багато процесів. Підприємства отримують доступ до ресурсів без значних інвестицій у власну інфраструктуру,

але при цьому виникає певна залежність від зовнішніх провайдерів. Не завжди зрозуміло, де проходить межа відповідальності, і це інколи створює додаткові ризики. Часто буває так, що рішення впроваджують швидше, ніж встигають продумати їх захист, і потім доводиться виправляти ситуацію вже в процесі роботи.

Ситуація з Інтернетом речей виглядає ще складнішою. Різні сенсори, контролери, допоміжні пристрої активно використовуються у виробництві та логістиці, і це дійсно підвищує ефективність. Але одночасно з'являється багато точок потенційного доступу, і далеко не всі вони достатньо захищені. Іноді один слабкий елемент може вплинути на всю систему, що вже неодноразово підтверджувалося на практиці. У невеликих компаніях це питання взагалі часто відкладається на потім, поки не виникає реальна проблема.

Ще один момент, який останнім часом активно обговорюється, – використання штучного інтелекту. Його застосовують і для захисту, і для атак, що виглядає дещо парадоксально. Алгоритми допомагають швидше виявляти відхилення або підозрілі дії, але водночас можуть використовуватись для створення складніших схем впливу. Наприклад, генерація текстів для «фішингових» повідомлень або спроби обійти системи «автентифікації». У цьому сенсі розвиток технологій не завжди однозначно покращує ситуацію, інколи навпаки ускладнює її.

У цьому контексті доцільно систематизувати ключові технологічні виклики кібербезпеки в умовах цифрової трансформації. З цією метою в табл. 1 узагальнено основні напрями загроз та їх практичні прояви.

Таблиця 1

Основні технологічні виклики кібербезпеки в умовах цифрової трансформації

Напрям цифровізації	Основні кіберзагрози	Практичні прояви	Наслідки для підприємства
Хмарні технології	Несанкціонований доступ, витік даних	Злам облікових записів, помилки конфігурації	Фінансові втрати, порушення конфіденційності
Інтернет речей	Вразливість пристроїв, відсутність оновлень	Захоплення контролю над пристроями	Збої в операційній діяльності

Великі дані	Несанкціонована обробка інформації	Маніпуляції з аналітичними результатами	Прийняття помилкових управлінських рішень
Штучний інтелект	Зловживання алгоритмами	Генерація фальшивого контенту, обхід захисту	Репутаційні втрати
Ланцюги постачання	Атаки через сторонніх постачальників	Інфікування програмного забезпечення	Масове поширення загроз

Якщо узагальнити наведені положення, то кібербезпека в умовах цифрових змін уже складно сприймається як окремий напрям роботи, вона швидше розчиняється в загальній системі управління підприємством. Тут переплітаються технічні рішення, організаційні підходи і навіть управлінські звички, які склалися раніше і не завжди швидко змінюються. Окремо варто згадати про персонал, бо саме на цьому рівні часто виникають слабкі місця. Практика показує, що значна кількість інцидентів пов'язана не стільки зі складними атаками, скільки з банальною необережністю або недостатнім розумінням ризиків. І це не завжди легко виправити лише інструкціями чи формальними навчаннями.

У реальній діяльності підприємств поступово приживається ризик-орієнтований підхід, хоча він не завжди впроваджується послідовно. Ідентифікація ризиків, їх оцінка, визначення пріоритетів – усе це виглядає логічно, але на практиці часто залежить від доступних ресурсів і навіть від особистого бачення керівництва. При цьому важливо, щоб цей процес не зводився до одноразових дій, адже кіберзагрози змінюються досить швидко, інколи навіть швидше, ніж очікується. Виходить, що система управління ризиками повинна бути постійно в русі, хоча забезпечити таку безперервність вдається не всім.

Щодо міжнародних стандартів, то їх значення важко заперечити, особливо для підприємств, які працюють із закордонними партнерами. Вони задають певні орієнтири і створюють відчуття впорядкованості у підходах до захисту інформації. Водночас пряме перенесення стандартів у практику не завжди дає очікуваний результат, оскільки доводиться враховувати локальні умови, вимоги законодавства і навіть специфіку галузі. Іноді цей процес

виглядає дещо формальним, коли головною метою стає відповідність документам, а не реальне підвищення рівня безпеки.

Якщо говорити про подальший розвиток систем кібербезпеки, то можна виділити кілька напрямів, які зазвичай згадуються, хоча вони не завжди реалізуються в повному обсязі. Насамперед це інтеграція питань безпеки у стратегічне управління, що виглядає очевидним, але потребує певної перебудови підходів. Далі – розвиток систем моніторингу, які дозволяють реагувати на інциденти швидше, ніж це було раніше. Також важливим залишається питання підготовки персоналу, причому не лише вузьких спеціалістів, а й звичайних працівників. І, звичайно, використання сучасних технологій, включаючи штучний інтелект, хоча тут теж не все однозначно, бо разом із новими можливостями з'являються і додаткові ризики, про які іноді згадують уже після впровадження.

Підсумовуючи, слід зазначити, що цифрова трансформація створює не лише нові можливості, але й суттєві ризики, пов'язані з кібербезпекою. Ефективне протидіяння цим ризикам можливе лише за умови комплексного підходу, який поєднує технічні рішення, організаційні заходи та стратегічне бачення розвитку підприємства. У сучасних умовах кібербезпека стає невід'ємною складовою конкурентоспроможності та стійкості підприємств, особливо тих, що функціонують у міжнародному середовищі.

Список використаних джерел:

1. Що таке цифрова трансформація? *SAP*: офіційний веб-сайт компанії SAP. 2023. 27 груд. 2023 р. URL: https:/ /www.sap.com/ukraine /resources/what-is-digital-transfor ma tion

2. Ransomware. *Вікіпедія*: вільна онлайн-енциклопедія. URL: https://uk.wikipedia.org/wiki/Ransomware (дата звернення: 18.04.2026).

3. Що таке фішинг? *Microsoft*: офіційний веб-сайт компанії Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 18.04.2026).

ІНТЕГРАЦІЯ БЕЗПІЛОТНИХ ПОВІТРЯНИХ СУДЕН У СИСТЕМУ МОНІТОРИНГУ ПОВІТРЯНОГО ПРОСТОРУ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ DRONE ID

Мукоіда Руслан Вікторович
професор кафедри тактико-спеціальної та спеціальної фізичної підготовки факультету підготовки фахівців для підрозділів превентивної поліції Національної поліції України Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент
Аносєнков Анатолій Анатолійович
доцент кафедри тактико-спеціальної та спеціальної фізичної підготовки факультету підготовки фахівців для підрозділів превентивної поліції Національної поліції України Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Глобальна практика свідчить про перехід від добровільної ідентифікації до жорсткого мандатного впровадження Remote ID як передумови для подальшої інтеграції безпілотників у цивільну авіацію. Провідні регулятори — Федеральне авіаційне управління США (FAA) та Агентство авіаційної безпеки Європейського Союзу (EASA) — вже встановили чіткі терміни та технічні вимоги до систем Drone ID.

Сучасна еволюція авіаційного простору характеризується стрімким насиченням безпілотними повітряними суднами (далі – БПС), що вимагає радикального переосмислення систем ідентифікації та контролю. Технологія Drone ID, або Remote ID (далі – RID), постає як фундаментальний інструмент забезпечення прозорості, безпеки та підзвітності в умовах, коли традиційні методи радіолокаційного спостереження виявляються недостатніми для моніторингу малорозмірних апаратів на низьких висотах. Ця технологія функціонує як цифровий номерний знак, що в режимі реального часу транслює критично важливу інформацію про політ, дозволяючи правоохоронним органам та авіаційним регуляторам відрізняти легітимних користувачів від потенційних загроз [1].

Система Drone ID базується на трансляції даних за допомогою існуючих бездротових протоколів, що забезпечує низьку вартість

впровадження та широку сумісність із мобільними пристроями. Основна технічна концепція передбачає два механізми: трансляційну ідентифікацію (Broadcast RID) та мережеву ідентифікацію (Network RID). Трансляційна модель передбачає безпосередню передачу радіосигналу від БПС до наземних приймачів за допомогою Bluetooth або Wi-Fi. Це дозволяє будь-якій особі з відповідним програмним забезпеченням на смартфоні отримати доступ до публічних даних про політ у радіусі прямої видимості сигналу.

Фізична передача повідомлень у трансляційній моделі реалізується через кілька стандартів, кожен із яких має специфічні характеристики дальності та енергоспоживання. Bluetooth 4 Legacy Advertising забезпечує підтримку застарілих пристроїв, тоді як Bluetooth 5 Long Range Advertising значно розширює радіус детекції. Wi-Fi Neighbor Awareness Network (NAN) та Wi-Fi Beacon дозволяють інтегрувати дані ідентифікації безпосередньо в структуру пакетів бездротових мереж. Важливою особливістю є те, що пристрої на базі Android зазвичай підтримують обидва типи протоколів (Bluetooth та Wi-Fi) за умови вимкнення обмеження сканування (Wi-Fi scan throttling), тоді як пристрої на базі iOS наразі обмежені переважно детекцією через Bluetooth.

Мережева дистанційна ідентифікація (Network Remote ID) використовує інтернет-з'єднання, зазвичай через мережі 4G або 5G, для передачі даних до централізованого постачальника послуг (USS) або хмарної платформи. Ця модель є критичною для операцій поза межами прямої видимості (BVLOS), оскільки вона не обмежена радіусом дії локального передавача та дозволяє здійснювати глобальний моніторинг повітряного простору [2]. Гібридні системи, що поєднують обидва методи, вважаються найбільш перспективними для довгострокового впровадження, оскільки вони забезпечують як локальну прозорість для патрульних офіцерів, так і стратегічну інтеграцію в системи управління безпілотним рухом (UTM) [3].

Інформаційна структура повідомлення Drone ID є стандартизованою та включає кілька обов'язкових елементів: унікальний ідентифікатор БПС (серійний номер або сесійний ID), географічні координати (широта, довгота), геометричну висоту, швидкість, а також місцезнаходження оператора або точки зльоту та часову мітку. Такий набір даних дозволяє не лише ідентифікувати апарат, а й миттєво локалізувати особу, яка ним керує, що є критично важливим для правоохоронних органів у разі виявлення порушень.

Для правоохоронних органів технологія Drone ID є критично важливим інструментом, що забезпечує перехід від реактивного до проактивного управління безпекою повітряного простору. Вона дозволяє реалізувати концепцію "прозорого неба", де кожен легітимний політ є видимим та підзвітним.

Враховуючи міжнародний досвід та специфіку національного контексту, пропонується системний підхід до інтеграції технології Drone ID у діяльність правоохоронних органів України.

По-перше законодавчі та регуляторні ініціативи повинні включати обов'язкову сертифікацію та маркування БПС. Необхідно на рівні підзаконних актів встановити вимогу щодо наявності системи дистанційної ідентифікації для всіх БПС, що ввозяться або виробляються в Україні (за винятком іграшок вагою до 250 г). Це має бути синхронізовано з європейськими класами C1–C6.

По-друге пропонується створити національний реєстр операторів БПС. База даних повинна бути інтегрована з інформаційною системою МВС. Кожен оператор після проходження онлайн-навчання має отримати унікальний ідентифікатор, який обов'язково вноситься у програмне забезпечення дрона.

Також потрібно створити правове підґрунтя, щодо легалізація даних з ідентифікаторів як доказів, а саме пропонується зміни до КУпАП та КПК України щодо визнання даних системи Drone ID (у поєднанні з часовими мітками та координатами) належними доказами у справах про порушення правил використання повітряного простору та інших правопорушень.

З метою забезпечення технічного аспекту реалізації легалізація даних з ідентифікаторів дронів, як доказів пропонується:

— забезпечити розгортання мережі наземних приймачів RID у великих містах та навколо об'єктів критичної інфраструктури доцільно встановити стаціонарні сенсори для детекції сигналів Bluetooth/Wi-Fi RID. Це дозволить автоматично сповіщати чергові частини про появу несанкціонованих дронів;

— створити умови, щодо рзробки вітчизняного модуля "свій-чужий" для потреб правоохоронців та ЗСУ. Необхідно стимулювати виробництво модулів Remote ID із захищеним каналом передачі даних, які дозволяли б силам ППО миттєво ідентифікувати дрони державних структур;

— розробити та впровадити мобільні засоби ідентифікації для патрульних. Забезпечення підрозділів патрульної поліції та

Нацгвардії планшетами зі спеціалізованим ПЗ, здатним зчитувати Drone ID та автоматично звіряти його з державним реєстром у режимі реального часу.

Список використаних джерел:

1. Дистанційна ідентифікація дронів (Remote Identification of Drones) [Електронний ресурс] / Федеральне авіаційне управління США (FAA). — 2024. — Режим доступу: https://www.faa.gov/uas/getting_started/remote_id. — Назва з екрана. — Дата звернення: 27.02.2026.

2. Мережевий Remote ID та майбутнє операцій з дронами (Network Remote ID and the Future of Drone Operations) [Електронний ресурс] / Elsight. — 2023. — Режим доступу: https://www.elsight.com/blog/network-remote-id-and-the-future-of-drone-operations/. — Назва з екрана. — Дата звернення: 27.02.2026.

3. Розробка системи моніторингу UTM на основі мережевого Remote ID з алгоритмом виявлення у формі перевернутої краплі (Development of UTM Monitoring System Based on Network Remote ID with Inverted Teardrop Detection Algorithm) [Електронний ресурс] / World Scientific. — 2025. — Режим доступу: https://www.worldscientific.com/ doi/epdf/10.1142/ S23 01385025500074. — Назва з екрана. — Дата звернення: 27.02.2026.

КІБЕРЗАГРОЗИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: СУЧАСНИЙ СТАН, ТЕНДЕНЦІЇ ТА НАПРЯМИ ПРОТИДІЇ

Нікітін Анатолій Анатолійович
доктор юридичних наук, доцент, проректор
Одеського державного університету внутрішніх справ

Захист критичної інфраструктури належить до пріоритетних напрямів забезпечення національної безпеки України, особливо в умовах повномасштабної військової агресії Російської Федерації, яка супроводжується системними кібератаками на об'єкти енергетики, транспорту, фінансового сектору та державного управління. Критична інфраструктура є основою стабільного функціонування держави та суспільства, проте її дедалі глибша залежність від

цифрових технологій та автоматизованих систем управління робить її особливо вразливою до кіберзагроз різного характеру [2]. Лише протягом 2024 року в інформаційному просторі України було зафіксовано понад три мільйони подій інформаційної безпеки, серед яких близько двадцяти восьми тисяч отримали статус критичних, що засвідчує безпрецедентний масштаб і динаміку кіберзагроз, з якими стикається держава [2].

Аналіз сучасного стану кіберзагроз для об'єктів критичної інфраструктури України дозволяє виокремити кілька основних типів атак, що становлять найбільшу небезпеку. До них належать програми-вимагачі, спрямовані на блокування роботи інформаційних систем з метою отримання викупу; розподілені атаки на відмову в обслуговуванні (DDoS), що паралізують роботу державних і комерційних онлайн-сервісів; методи соціальної інженерії, орієнтовані на маніпулювання персоналом для отримання несанкціонованого доступу до систем; а також експлойти нульового дня, що використовують ще не виявлені вразливості програмного забезпечення [2]. Окремо слід відзначити поширення кібершпигунства та інформаційно-психологічних операцій, які в умовах війни набувають гібридного характеру та поєднуються з традиційними засобами впливу на суспільну свідомість і ухвалення управлінських рішень.

Найбільш уразливими до кіберзагроз залишаються сектори енергетики, транспорту, фінансової системи та цифрової інфраструктури, що пояснюється їхньою стратегічною важливістю для функціонування держави та потенційно масштабними наслідками успішних атак на ці об'єкти [2]. Водночас, як зазначається у дослідженнях із проблематики кіберборотьби та кібероборони, ефективний захист критичної інфраструктури вимагає не лише технічних рішень, а й комплексного інституційного підходу, що охоплює формування цілісних кіберзахисних стратегій на загальнодержавному рівні [1]. Сучасні виклики у сфері кібербезпеки критичної інфраструктури зумовлюють необхідність постійного перегляду методів оцінювання та управління ризиками кібератак з урахуванням динамічного характеру загроз і появи нових технік ураження інформаційних систем [1].

Серед тенденцій розвитку кіберзагроз для критичної інфраструктури України на сучасному етапі варто відзначити поступову трансформацію тактик зловмисників від одиничних точкових атак до скоординованих, багатовекторних кампаній, що

поєднують технічні засоби впливу з елементами дезінформації та психологічних операцій. Зростає також роль державно підтримуваних суб'єктів кіберзлочинності, які діють в інтересах держави-агресора та володіють значно більшими ресурсами й технічними можливостями порівняно зі звичайними кіберзлочинними угрупованнями. Така тенденція суттєво ускладнює завдання правоохоронних і спеціалізованих органів кібербезпеки, оскільки вимагає застосування методів і засобів, традиційно притаманних протидії державному кібершпигунству та кібертероризму, а не лише класичній кіберзлочинності.

Важливим напрямом удосконалення національної системи захисту критичної інфраструктури є врахування міжнародного досвіду та імплементація передових стандартів кібербезпеки. Аналіз провідних практик, зокрема методології ENISA Threat Landscape та вимог європейської директиви NIS2, демонструє ефективність багаторівневого підходу до кіберзахисту, що включає моніторинг мереж у реальному часі, застосування автоматизованих інструментів управління вразливостями, удосконалення систем оцінки ризиків, впровадження багатофакторної автентифікації та системне підвищення кіберобізнаності персоналу [2]. Імплементація зазначених підходів у вітчизняну практику відповідає курсу України на європейську інтеграцію та узгоджується з вимогами актуального національного законодавства у сфері захисту критичної інфраструктури, прийнятого протягом 2025 року.

Напрями подальшої протидії кіберзагрозам для критичної інфраструктури України мають передбачати розбудову трирівневої організаційно-технічної моделі кіберзахисту, яка охоплює організаційно-керівний рівень взаємодії основних суб'єктів національної системи кібербезпеки, технологічний рівень обміну інформацією та моніторингу, а також базовий рівень захищеності інформаційної інфраструктури на місцях [1]. Окремої уваги потребує посилення міжвідомчої координації між органами державної влади, операторами критичної інфраструктури та спеціалізованими підрозділами кібербезпеки, що дозволить забезпечити оперативне виявлення кіберінцидентів і своєчасне реагування на них. Не менш важливим є розвиток публічно-приватного партнерства у сфері кібербезпеки, оскільки значна частина об'єктів критичної інфраструктури перебуває у приватній власності та потребує узгоджених підходів до захисту.

Таким чином, кіберзагрози для критичної інфраструктури України на сучасному етапі характеризуються зростанням масштабів, технологічної складності та гібридного характеру атак, що поєднують технічні засоби впливу з інформаційно-психологічними операціями. Ефективна протидія цим загрозам потребує системної інтеграції організаційних, технологічних і правових заходів захисту, врахування передового міжнародного досвіду та постійного вдосконалення національної нормативно-правової бази. Лише комплексний і узгоджений підхід усіх заінтересованих суб'єктів здатний забезпечити належний рівень кіберстійкості об'єктів критичної інфраструктури в умовах перманентного зростання кіберзагроз.

Список використаних джерел:

1. Мурасов Р. К. ., Фараон , С. І. і Гук, О. М. . (2025) «Кібербезпека критичної інфраструктури: оцінювання та управління ризиками кібератак», Сучасні інформаційні технології у сфері безпеки та оборони. Київ, Україна, 54(3), с. 75–83. doi: 10.33099/2311-7249/2025-54-3-75-83.

2. Ільєнко А., Телющенко, В., & Дубчак О. (2025). Сучасні кіберзагрози критичної інфраструктури України та світу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 150–164. https://doi.org/10.28925/2663-4023.2023.27.719.

ПРОБЛЕМИ ВСТАНОВЛЕННЯ СУБ'ЄКТА КІБЕРЗЛОЧИНУ В УМОВАХ АНОНІМНОСТІ ЦИФРОВОГО СЕРЕДОВИЩА

Підгородинський Вадим Миколайович
доктор юридичних наук, професор, проректор
Одеського державного університету внутрішніх справ

Сучасний розвиток інформаційно-комунікаційних технологій формує принципово нове середовище вчинення злочинів, у якому традиційні підходи до встановлення особи правопорушника втрачають свою ефективність. Кіберзлочинність дедалі частіше характеризується високим рівнем анонімності, що досягається завдяки використанню VPN-сервісів, мереж Tor, проксі-серверів, криптовалютних транзакцій та інших технологій приховування

цифрових слідів. У таких умовах проблема атрибуції суб'єкта злочину стає однією з ключових у кримінальному провадженні, оскільки встановлення реальної особи правопорушника ускладнюється багаторівневою технічною інфраструктурою приховування даних та глобальним характером цифрових комунікацій [1].

Анонімність цифрового середовища створює ситуацію, коли між фактичним виконавцем злочину та його цифровими слідами формується складний багатошаровий бар'єр. Як зазначається у наукових дослідженнях, використання технологій обфускації трафіку, шифрування та розподілених мереж суттєво обмежує можливості правоохоронних органів щодо ідентифікації джерела кіберінциденту [1]. У результаті цього цифрові сліди, які традиційно могли б слугувати прямим доказом, набувають опосередкованого характеру і потребують складної багатовекторної інтерпретації із залученням технічної, криміналістичної та аналітичної експертизи.

Додатковою проблемою встановлення суб'єкта кіберзлочину є специфіка цифрових доказів, які відзначаються високою вразливістю до модифікації, втрати або підміни. У науковій літературі підкреслюється, що цифрові сліди вимагають суворого дотримання процедур їх збирання, збереження та верифікації, оскільки будь-яке порушення цілісності даних може поставити під сумнів їх доказову силу [2]. У контексті анонімних мереж це набуває особливого значення, оскільки навіть технічно коректно отримана інформація може не містити достатніх атрибутів для ідентифікації конкретної фізичної особи.

Окрему складність становить проблема юрисдикційної фрагментації цифрового простору. Кіберзлочини часто мають транскордонний характер, коли етапи підготовки, виконання та приховування злочину здійснюються в різних країнах. Це створює правові бар'єри для оперативного доступу до даних та їх використання в кримінальному процесі. Як зазначається у дослідженнях проблем кримінального права в цифрову епоху, відсутність уніфікованих міжнародних процедур обміну даними суттєво ускладнює процес встановлення особи правопорушника та знижує ефективність розслідувань.

Важливим аспектом проблеми є також обмеженість традиційних криміналістичних методів у цифровому середовищі. Методи дактилоскопії, трасології або класичної ідентифікації особи не можуть бути безпосередньо застосовані до кіберпростору, де основним об'єктом аналізу виступають лог-файли, мережеві пакети,

метадані та поведінкові цифрові патерни. У зв'язку з цим дедалі більшого значення набувають методи поведінкового профілювання, аналізу цифрових відбитків пристроїв та алгоритми штучного інтелекту, однак їх точність залишається обмеженою через можливість імітації або спотворення поведінкових характеристик користувача [1; 3].

Водночас слід враховувати, що анонімність у кіберпросторі має не лише технічний, але й соціально-правовий вимір. Баланс між правом на приватність та потребами кримінального правосуддя створює додаткові обмеження для правоохоронних органів. Надмірне розширення інструментів цифрового моніторингу може вступати в конфлікт із принципами прав людини та захисту персональних даних, що додатково ускладнює процес ідентифікації суб'єкта злочину.

Таким чином, встановлення суб'єкта кіберзлочину в умовах анонімності цифрового середовища є комплексною проблемою, що поєднує технічні, криміналістичні та правові виклики. Її вирішення потребує інтеграції сучасних аналітичних технологій, розвитку міжнародного співробітництва та вдосконалення методології цифрової криміналістики. Лише комплексний підхід, що поєднує технічну атрибуцію, поведінковий аналіз та правову координацію, може забезпечити підвищення ефективності ідентифікації кіберзлочинців у сучасних умовах.

Список використаних джерел:

1. Keating L. Technical and Legal Limitations in Unmasking Anonymous Actors // ResearchGate. – 2025. – URL: https://www.researchgate.net/publication/396960927_TECHNICAL_AND_LEGAL_LIMITATIONS_IN_UNMASKING_ANONYMOUS_ACTORS

2. Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility // Analytical and Comparative Jurisprudence. – 2025. – Vol. 3(5). – P. 315–321. – DOI: https://doi.org/10.24144/2788-6018.2025.05.3.46

3. Swate C., Sithungu S., Lebea K. An Analysis of Cyberwarfare Attribution Techniques and Challenges // ECCWS Proceedings. – 2025. – DOI: https://doi.org/10.34190/eccws.23.1.2190

ВПЛИВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ (ІПСО) НА КІБЕРБЕЗПЕКУ УКРАЇНИ

Пилипенко Євгенія Олексіївна
кандидат юридичних наук, старший дослідник
старший науковий співробітник науково-дослідної лабораторії
з актуальних питань кримінального аналізу
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції
Національної поліції України
Одеського державного університету внутрішніх справ

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII, кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [1].

У свою чергу, ІПСО – це інформаційно-психологічна операція (Psychological Operations, PSYOPS), що являє собою сплановані дії з поширення дезінформації, пропаганди та маніпулятивних даних для впливу на емоції, настрої, критичне мислення та поведінку цільової аудиторії. Її мета – змінити сприйняття подій, спровокувати паніку або вплинути на прийняття рішень на користь ініціатора, що особливо активно використовується в умовах війни для підриву морального духу [2].

До елементів ІПСО відносяться дезінформація, пропаганда, перебільшення певної інформації або применшення іншої, диверсії в тилу, кібератаки тощо.

Дезінформація – це спеціально перекручені факти. Пропаганда – нав'язування «правильної» точки зору. Кібератаки – поширення фейкових повідомлень через зламані акаунти чи сайти. Усі ці інструменти працюють разом, щоб збити людину з пантелику [2].

ІПСО безумовно має негативний вплив на кібербезпеку України. Серед основних ключових аспектів негативного впливу ІПСО на кібербезпеку України виокремлюють такі [3]:

- маніпуляція людським фактором (соціальна інженерія). ІПСО часто використовують для підготовки ґрунту під кібератаки. Через створення паніки або недовіри зловмисники змушують користувачів нехтувати правилами безпеки, відкривати шкідливі посилання або розголошувати паролі.

- використання ботоферм. Для масового поширення дезінформації та маніпулювання відкритими даними залучаються ботоферми. Це дозволяє не лише формувати викривлене сприйняття реальності, а й здійснювати автоматизовані атаки на інформаційну інфраструктуру.

- дестабілізація через кібератаки. Проведення технічних атак супроводжується активним висвітленням у медіа для створення відчуття незахищеності, підриву довіри до державних інституцій та зниження морального духу;

- таргетований вплив у соцмережах: Використання методів таргетингу дозволяє спрямовувати деструктивний контент на конкретні групи осіб, що може призвести до несанкціонованого доступу або витоку конфіденційної інформації через «слабкі ланки» в організаціях;

- загрози цілісності та доступності даних. ІПСО можуть бути спрямовані на зміну (фальсифікацію) даних або блокування доступу до офіційних джерел інформації, що порушує основні принципи інформаційної безпеки: конфіденційність, цілісність та доступність.

Протидіяти ІПСО складно, але можливо. Для цього необхідно уважно перевіряти джерела, зберігати спокій і ділитися лише тією інформацією, що пройшла перевірку. Перевіряючи інформацію, треба зіставляти її з іншими надійними джерелами та фактами, зберігаючи критичне мислення, врівноваженість та здоровий глузд [4].

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення: 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#n5 (дата звернення: 26.04.2026).

2. Що таке ІПСО, чому важливо це знати і які операції зараз проводить росія проти України. *Український тиждень. Зміст має значення.* URL: https://tyzhden.ua/shcho-take-ipso-chomu-vazhlyvo-

tse-znaty-i-iaki-operatsii-zaraz-provodyt-rosiia-proty-ukrainy/ (дата звернення: 26.04.2026).

3. Chamika Hiruni. Psychological Warfare in the Digital Age: The Role of Cyber Operations in Modern PsyOps. Psychological Warfare in the Digital Age. November 2024. DOI:10.13140 /RG.2.2.34079.37283.

4. Що таке ІПСО: сенс, загроза та як протидіяти. *Chernigivlisgosp.com.ua*. URL: https://chernigivlisgosp.com.ua/ shho-take-ipso-sens-zagroza-ta-yak-protidiyati/ (дата звернення: 26.04.2026).

КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Постолова Карина Юріївна
здобувачка вищої освіти 202 взводу
Навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції Національної поліції України
(Одеський державний університет внутрішніх справ)
Форос Ганна Володимирівна
завідувачка кафедри кримінального аналізу та інформаційних технологій, к.ю.н., доцент
(Одеський державний університет внутрішніх справ)
https://orcid.org/0000-0002-9504-3681

У сучасних умовах стрімкого розвитку інформаційних технологій та активної цифровізації всіх сфер суспільного життя особливого значення набуває питання забезпечення кібербезпеки. Постійне зростання обсягів інформації та розширення можливостей використання кіберпростору поряд із беззаперечними перевагами зумовлює появу нових викликів і загроз, пов’язаних із кіберзлочинністю, витоком даних та несанкціонованим втручанням у функціонування інформаційних систем. У зв’язку з цим підвищується роль правоохоронних органів, зокрема підрозділів кримінальної поліції, діяльність яких значною мірою залежить від ефективного інформаційно-аналітичного забезпечення та належного рівня кібербезпеки.

Правову основу кібербезпеки становить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відповідно до ст. 5 Закону, правоохоронні органи є суб'єктами забезпечення кібербезпеки та здійснюють запобігання використанню кіберпростору в протиправних цілях, виявлення, реагування на кіберінциденти та інформаційний обмін [2].

Національна поліція України відповідно до Закону України «Про Національну поліцію» від 02.07.2015 № 580-VIII наділена повноваженнями щодо запобігання, виявлення, припинення та розкриття кіберзлочинів, а також підвищення поінформованості громадян про безпеку в кіберпросторі [3, с. 374]. Департамент кіберполіції утворено постановою Кабінету Міністрів України від 13.10.2015 № 831 як міжрегіональний територіальний орган у структурі кримінальної поліції.

Важливе значення мають Будапештська конвенція про кіберзлочинність (ратифікована Україною у 2005 році), Закон України «Про критичну інфраструктуру» (2021) та Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (Постанова КМУ від 19.06.2019 № 518). Кримінальний кодекс України містить статті 361–363-1, що передбачають відповідальність за комп'ютерні злочини.

Нормативна база створює підґрунтя для інтеграції кібербезпеки в діяльність поліції, проте законодавче регулювання має певні прогалини, зокрема в механізмах міжвідомчої взаємодії та процедурній роботі з цифровими доказами [1, с. 393].

Департамент кіберполіції входить до структури кримінальної поліції Національної поліції України та є міжрегіональним територіальним органом. Він забезпечує реалізацію державної політики у сфері протидії кіберзлочинності та здійснює оперативно-розшукову діяльність.

Основні завдання Департаменту включають: реалізацію державної політики протидії кіберзлочинності; завчасне інформування населення про новітні кіберзлочини; впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, загрози та злочини; реагування на запити закордонних партнерів через Національну цілодобову мережу контактних пунктів (понад 90 країн); підвищення кваліфікації працівників поліції щодо застосування комп'ютерних технологій; участь у міжнародних операціях.

Кіберполіція виконує функції попередження, виявлення, фіксації кіберзлочинів та розслідування інцидентів у кіберпросторі. Вона забезпечує інформаційно-аналітичну підтримку підрозділів кримінальної поліції шляхом моніторингу кіберінцидентів, аналізу загроз, збору індикаторів компрометації (IoC) та передачі аналітичних даних. Ефективна протидія серйозним інцидентам потребує спільної роботи CERT-UA і поліції: технічні фахівці швидко інформують правоохоронців, якщо атака має ознаки злочину, що дозволяє трансформувати технічний інцидент у кримінальне провадження [1, с. 399–401; 4].

Кібербезпека визначається як стан захищеності життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз [2; 3, с. 375].

Для підрозділів кримінальної поліції кібербезпека є елементом інформаційної безпеки, що включає захист баз даних, систем документообігу, сервісу «102», автоматизованих диспетчерських систем від внутрішніх і зовнішніх загроз. Вона забезпечує: виявлення та нейтралізацію кіберзагроз під час оперативно-розшукових заходів; дотримання принципів конфіденційності, цілісності та доступності інформації; збір, обробку та використання цифрових доказів; координацію з CERT-UA для оперативного обміну даними [1, с. 398–401; 3, с. 376].

Впровадження сучасних програмно-аналітичних платформ для моніторингу кіберінцидентів і аналізу загроз дозволяє перетворювати розрізнені дані на якісну аналітичну інформацію, що підвищує ефективність управлінських рішень та профілактичної роботи в кримінальній поліції [1, с. 400].

Серед основних проблем виокремлюються: низький рівень цифрової зрілості та технічної спроможності правоохоронних органів порівняно зі швидкістю розвитку кіберзагроз; недостатня підготовка кадрів, брак фінансування та сучасного програмно-аналітичного забезпечення; фрагментарність координації між поліцією, CERT-UA та приватним сектором; проблеми збору цифрових доказів у транснаціональних атаках; правові колізії в питаннях юрисдикції та процедурної взаємодії [1, с. 393–394; 3, с. 374–375].

Перспективи вдосконалення пов’язані з:

- гармонізацією української правової бази з положеннями Директиви ЄС NIS2 та Будапештської конвенції;

- створенням Національної телекомунікаційної платформи кібербезпеки для оперативного обміну інформацією та індикаторами компрометації;
- підвищенням кадрового потенціалу через постійну професійну підготовку;
- впровадженням сучасних технологій (Big Data, штучний інтелект);
- розвитком партнерства з приватним сектором та посиленням міжнародної співпраці через мережі Інтерполу та Європолу [1, с. 402–403].

Отже, кібербезпека є невід'ємним елементом інформаційно-аналітичного забезпечення підрозділів кримінальної поліції. Вона забезпечує захист інформаційних ресурсів, оперативне реагування на загрози, збір цифрових доказів та ефективну протидію кіберзлочинності в умовах гібридної війни. Аналіз нормативної бази, ролі Департаменту кіберполіції та практичних аспектів свідчить про необхідність системного підходу до її розвитку. Вирішення виявлених проблем шляхом кадрового, технічного та нормативного вдосконалення сприятиме підвищенню стійкості кримінальної поліції до кіберзагроз і зміцненню національної безпеки України.

Список використаних джерел:

1. Василенко В. М. Національна кібербезпека в умовах диджиталізації суспільства: роль поліції в захисті критичної інфраструктури. *Науковий вісник. 2025.* С. 392–403.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Офіційний вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Мамедова Е. А. Кібербезпека патрульної поліції: підходи до визначення поняття науковцями та практиками. *Науковий вісник. 2023*. С. 374–377.

4. Кіберполіція. Кібербезпека України. Legal Aid Wiki. URL: https://legalaid.wiki/index.php/Кіберполіція._Кібербезпека_України

ТЕХНОЛОГІЧНА ЕВОЛЮЦІЯ ТА СТРАТЕГІЧНА ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ DELTA

Проскурня Є. Є.
старший викладач кафедри тактико-спеціальної та спеціальної фізичної підготовки факультету підготовки фахівців для підрозділів превентивної діяльності Національної поліції України
Одеський державний університет внутрішніх справ

Сучасний театр воєнних дій зазнав фундаментальної трансформації, перейшовши від традиційних кінетичних зіткнень до високотехнологічної мережево-центричної війни, де інформаційна перевага є визначальним фактором успіху. У центрі цієї цифрової революції знаходиться система ситуаційної обізнаності DELTA – унікальна розробка Сил оборони України, яка інтегрує передові рішення в галузі штучного інтелекту (ШІ) для автоматизованого розпізнавання техніки, координації підрозділів та скорочення циклу ураження цілей. Платформа DELTA, створена Центром інновацій та розвитку оборонних технологій Міністерства оборони України, представляє собою хмарне рішення, що відповідає стандартам НАТО та забезпечує повний контроль над бойовим простором у режимі реального часу [1].

Основним драйвером аналітичної потужності DELTA є інтеграція спеціалізованої ШІ-платформи Avengers, яка виконує завдання з автоматичного виявлення та класифікації ворожих об’єктів за допомогою алгоритмів комп'ютерного зору. Платформа Avengers, розроблена Центром інновацій Міноборони, є унікальною у світі за обсягом відеоданих з ворожою технікою. Центр інновацій продовжує навчати ШІ-модель платформи Avengers на нових даних. Це дозволяє удосконалювати якість розпізнавання різноманітної ворожої техніки, навіть у складних умовах, наприклад танків, прихованих в лісових масивах, або БМП, що рухаються ґрунтовими дорогами [2].

Впровадження платформи Avengers в екосистему DELTA стало відповіддю на колосальне зростання обсягів відеоданих, які фізично не здатні опрацювати людські оператори. За оцінками

фахівців, система DELTA забезпечує понад 150 тисяч паралельних переглядів відеотрансляцій, що вимагає автоматизації аналізу для виявлення значущих об’єктів [3].

Платформа Avengers базується на моделях глибокого навчання, які пройшли тренування на найбільшому у світі наборі даних про ворожу військову техніку, що був розмічений вручну. Це дозволяє системі розпізнавати техніку з високою швидкістю та точністю навіть у складних умовах навколишнього середовища. Платформа Avengers використовує комп'ютерний зір для розпізнавання та класифікації 70% ворожих транспортних засобів та обладнання на відео з дронів та камер спостереження — всього за 2,2 секунди.

ШІ-алгоритми Avengers здатні ідентифікувати широкий спектр об'єктів: від основних бойових танків (ОБТ) до артилерійських систем та логістичного транспорту. Особлива увага приділяється здатності розрізняти техніку в умовах низької контрастності, наявності маскування або складного рельєфу, наприклад, танки в лісових масивах або БМП на ґрунтових дорогах.

Завдяки ШІ-платформі оператори можуть приймати рішення швидше та ефективніше, а ризик помилок через втому зменшується. Така інтеграція вже успішно працює в стрімінговому модулі VEZHA бойової системи DELTA. Нова версія мобільного застосунку Vezha інтегрована з модулем планування застосування безпілотників Mission Control та дозволяє уникати конфлікту частот FPV-дронів. Vezha розповсюджується винятково через Mobile Device Management – тобто через військовий аналог App Store або Play Market.

Інтеграція ШІ безпосередньо в стрімінговий модуль VEZHA дозволяє операторам дронів отримувати підказки в режимі реального часу. Це вирішує проблему «втоми оператора», коли після тривалого спостереження за екраном око замилюється, і боєць може пропустити замасковану ціль [4]. ШІ діє як невтомний асистент, що маркує підозрілі об'єкти, дозволяючи людині зосередитися на прийнятті рішень щодо пріоритетності цілей та способу їх ураження. Система не просто «бачить» об'єкт, вона миттєво передає його координати в загальну мережу DELTA, де вони стають доступними для артилерії або операторів ударних БпЛА.

Ефективність розпізнавання техніки в DELTA залежить від безперервного потоку якісних даних. Крім Avengers, існують

інші критично важливі системи, що наповнюють загальний інтелект екосистеми.

Система ОСНІ відіграє роль гігантського сховища та аналізатора відеоданих. Вона об'єднує потоки від понад 15 000 екіпажів дронів, що працюють на передовій. За час повномасштабного вторгнення система зібрала близько 2 мільйонів годин відео (що еквівалентно 228 рокам безперервного перегляду). Цей колосальний обсяг даних є фундаментом для навчання нейромереж. Щодня система поповнюється 5-6 терабайтами нових даних, що робить українську базу знань про сучасну війну найбільш актуальною у світі.

Одним із найскладніших завдань для ШІ на українському полі бою є ідентифікація техніки в умовах, коли обидві сторони використовують подібні радянські зразки (наприклад, Т-72 або БМП-2). У таких випадках критичного значення набуває розпізнавання специфічного маркування [5].

ШІ-моделі Avengers навчаються розпізнавати символи вторгнення («Z», «V», «O»), які наносяться білою фарбою на російську техніку. Хоча ці знаки спочатку призначалися для внутрішньої координації ворога та запобігання фратріциду (дружньому вогню) між російськими підрозділами, для української системи DELTA вони стали ідентифікаторами цілей.

Для запобігання «дружньому вогню» по власних дронах та техніці в екосистемі DELTA впроваджено протокол UA DRONE ID. Це рішення забезпечує розпізнавання за принципом «свій-чужий» у цифровому просторі. Завдяки інтеграції цього протоколу, оператори в системі DELTA бачать не лише ворожі цілі, підсвічені ШІ, а й положення власних безпілотників та наземних засобів, що значно підвищує рівень безпеки та координації [6].

Будучи основою цифрового управління військами, DELTA є пріоритетною ціллю для російських спецслужб. Безпека системи базується на хмарній архітектурі, що відповідає найвищим стандартам захисту даних.

За 2024 рік Центр реагування на кіберінциденти зафіксував 38 000 інцидентів, спрямованих проти інфраструктури Сил оборони, що знаходяться під його захистом. На початку 2025 року інтенсивність атак збереглася на рівні близько 2000 інцидентів на місяць [7].

Система успішно витримала численні спроби фішингу та впровадження шкідливого ПЗ. Завдяки використанню моделей

машинного навчання для аналізу трафіку, DELTA автоматично блокує підозрілу активність, забезпечуючи безперервний доступ до розвідданих для бойових підрозділів.

Список використаних джерел:

1. Що таке система DELTA і як вона задає тренди для країн НАТО?: вебсайт. Міністерство оборони України. 2024. URL: https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi (дата звернення: 02.03.2026).

2. Українські військові виявляють 12 тисяч цілей щотижня завдяки штучному інтелекту — Катерина Черногоренко : вебсайт. Міністерство оборони України. 2024. URL: https://mod.gov.ua/news/ukrayinski-vijskovi-viyavlyayut-12-tisyach-czilej-shhotizhnya-zavdyaki-shtuchnomu-intelektu-katerina-chernogorenko (дата звернення: 02.03.2026).

3. Систему DELTA впроваджують на всіх рівнях Сил оборони: Шмигаль підписав наказ: вебсайт. Укрінформ. 2024. URL: https://www.ukrinform.ua/rubric-ato/4022859-sistemu-delta-vprovadzuut-na-vsih-rivnah-sil-oboroni-smigal-pidpisav-nakaz.html (дата звернення: 02.03.2026).

4. Ukraine uses AI tools to identify Russian equipment : website. The New Voice of Ukraine. 2024. URL: https://english.nv.ua/nation/ukraine-uses-ai-tools-to-identify-russian-equipment-50453137.html (дата звернення: 02.03.2026).

5. Britzky E. Here's what those mysterious white 'Z' markings on Russian military equipment may mean: website. Task & Purpose. 2022. URL: https://taskandpurpose.com/news/russian-military-equipment-white-markings/ (дата звернення: 02.03.2026).

6. Центр інновацій та розвитку оборонних технологій Міністерства оборони України : офіційний вебсайт. URL: https://cidtd.lobbyx.army/ (дата звернення: 02.03.2026).

7. Що треба знати про розробників DELTA. Детальний ґайд про підрозділ : вебсайт. DOU. 2023. URL: https://dou.ua/lenta/articles/delta-team-and-work/ (дата звернення: 02.03.2026).

СУЧАСНІ МОДЕЛІ КІБЕРСТІЙКОСТІ: ЗМІСТ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ

Свиридюк Наталія Петрівна
доктор юридичних наук, професор
Одеський державний університет внутрішніх справ

Проблематика забезпечення кіберстійкості набуває особливої актуальності в умовах стрімкої цифровізації суспільних відносин, зростання масштабів транснаціональної кіберзлочинності та ускладнення архітектури критичної інформаційної інфраструктури. Сучасні кіберінциденти характеризуються високим рівнем латентності, транскордонністю, складністю правової атрибуції та значним деструктивним потенціалом, що зумовлює необхідність формування комплексних міжнародно-правових механізмів забезпечення кібербезпеки та кіберстійкості.

Особливого значення у цих умовах набуває кримінальний аналіз кіберінцидентів, який відіграє системоутворюючу роль як інструмент виявлення закономірностей кіберзлочинної діяльності, встановлення взаємозв'язків між суб'єктами атак, прогнозування кіберзагроз та формування доказової бази. Його еволюція від допоміжного елементу цифрової криміналістики до самостійної аналітичної функції кібербезпеки супроводжується активним впровадженням OSINT-підходів та елементів кіберрозвідки.

У сучасній міжнародній практиці сформувалися різні моделі забезпечення кіберстійкості, що поєднують правові, інституційні, організаційні та технологічні механізми реагування на кіберзагрози. Попри різноманітність підходів (наприклад, підходів США, Європейського Союзу, Великої Британії та НАТО), їх спільною тенденцією є поступова інтеграція кримінально-аналітичних функцій у системи управління кіберризиками та реагування на інциденти. Водночас у сучасній доктрині кіберправа відсутній уніфікований підхід до співвідношення регуляторних, оборонних та кримінально-процесуальних механізмів кібербезпеки, що ускладнює адаптацію ефективних моделей у державах, які функціонують в умовах гібридної війни.

У цьому контексті особливого значення набуває питання нормативного закріплення базових міжнародно-правових механізмів

протидії кіберзлочинності, які формують основу для координації зусиль держав у сфері розслідування кіберінцидентів та забезпечення кримінально-правової відповідальності. Саме таким ключовим інструментом виступає Будапештська Конвенція про кіберзлочинність (Convention on Cybercrime) [1], яка заклала основу міжнародного співробітництва у сфері розслідування комп'ютерних злочинів, збирання електронних доказів та координації діяльності правоохоронних органів. Разом з тим, однією з ключових проблем міжнародного кіберправа залишається складність правової атрибуції кібератак, що суттєво ускладнює застосування механізмів міжнародно-правової відповідальності держав та притягнення винних осіб до кримінальної відповідальності.

Ефективність зазначених міжнародно-правових механізмів значною мірою визначається не лише їх нормативним змістом, але й практичними інструментами імплементації, зокрема рівнем міжнародної координації, обміну електронними доказами та організації спільного реагування на кіберінциденти. Саме тому аналіз міжнародної договірної бази доцільно доповнити дослідженням національних та наднаціональних моделей кіберстійкості, у межах яких зазначені підходи набувають практичного інституційного втілення. У цьому контексті особливий інтерес становлять сучасні моделі кіберстійкості, серед яких однією з найбільш розвинених є **американська модель**.

Американська модель кіберстійкості вирізняється високим рівнем нормативної деталізації та ризик-орієнтованим підходом до управління кібербезпекою. Ключову роль відіграє Агентство кібербезпеки та захисту інфраструктури (Cybersecurity and Infrastructure Security Agency – CISA) [2], яке координує реагування на кіберінциденти, тоді як Національний інститут стандартів і технологій США (National Institute of Standards and Technology – NIST) [3] формує методологічну основу управління ризиками. Важливим елементом є централізований механізм повідомлення про кіберінциденти, що забезпечує ефективність кримінального аналізу щодо оперативного формування доказової бази та аналітики кіберінцидентів.

Водночас у міжнародній практиці сформувався альтернативний підхід, орієнтований не стільки на централізацію управління ризиками, скільки на нормативну уніфікацію та гармонізацію

регуляторних вимог у межах наднаціональних правових систем. Найбільш репрезентативним прикладом такого підходу виступає Європейська модель.

Модель Європейського Союзу базується на принципах нормативної гармонізації, превентивного регулювання та забезпечення єдиного рівня кібербезпеки. Інституційну координацію забезпечує Агентство Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity – ENISA) [4], а нормативну основу – акти ЄС у сфері управління кіберризиками та захисту цифрової інфраструктури. Європейський підхід орієнтований на формування єдиного правового простору обігу електронних доказів та міждержавного обміну інформацією щодо кіберінцидентів. Разом з тим, європейська модель демонструє складну багаторівневу регуляторну структуру, що певною мірою впливає на оперативність реагування на динамічні кіберзагрози. Це зумовлює актуальність альтернативних підходів, які поєднують регуляторну гнучкість із високим рівнем взаємодії між державним та приватним секторами кібербезпеки. Одним із найбільш показових прикладів такої моделі є підхід Великої Британії.

Модель Великої Британії має гібридний характер, поєднуючи державне регулювання та тісну взаємодію з приватним сектором. Основним інституційним елементом є Національний центр кібербезпеки (National Cyber Security Centre – NCSC) [5], який виконує функції координації, аналітики та методичної підтримки. Особливістю британського підходу є орієнтація на ризикорієнтовану модель управління кіберзагрозами, а також активне залучення бізнесу до процесів кіберзахисту. Це забезпечує гнучкість реагування та швидку адаптацію до нових типів загроз. Значну увагу британська модель приділяє механізмам державно-приватного партнерства та оперативному обміну кіберрозвідувальною інформацією. У той час модель Великої Британії все ж залишається національною системою кіберстійкості. Натомість на наднаціональному рівні дедалі більшого значення набувають механізми колективної кібероборони, які передбачають координацію зусиль держав у межах спільних безпекових структур. Найбільш інституційно розвиненою моделлю такого типу є підхід Організації Північноатлантичного договору (НАТО).

Модель НАТО ґрунтується на принципі колективної кібероборони та міждержавної координації. Її особливістю є інтеграція кіберпростору у систему колективної безпеки Альянсу, що трансформує кіберінциденти із суто технічних подій у елемент сучасних гібридних конфліктів. У системі колективної кібероборони ключову роль відіграє Кооперативний центр передового досвіду з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence– CCDCOE) [6]. У цьому контексті кримінальний аналіз кіберінцидентів набуває значення стратегічного безпекового інструменту.

Проведений порівняльно-правовий аналіз свідчить, що сучасні моделі кіберстійкості еволюціонують у напрямі інтеграції кримінального аналізу кіберінцидентів у систему управління кіберризиками. Водночас рівень такої інтеграції суттєво відрізняється залежно від моделі – від централізованої (США) до нормативно-гармонізованої (ЄС) та гібридної (Велика Британія, НАТО).

Досвід зазначених міжнародних моделей має особливе значення для України, система кібербезпеки якої функціонує в умовах постійного гібридного та кібервпливу. Україна займає особливе місце, оскільки функціонування її системи кібербезпеки відбувається в умовах повномасштабної гібридної війни, що поєднує кібератаки, інформаційно-психологічні операції, елементи кіберрозвідки та системний вплив на критичну інфраструктуру держави.

Практичний досвід України у сфері протидії масштабним кібератакам та захисту критичної інфраструктури формує новий підхід до забезпечення кіберстійкості в умовах гібридної війни. У цих умовах кримінальний аналіз кіберінцидентів поступово інтегрується у систему кібероборони та національної безпеки.

На відміну від США та держав Європейського Союзу, українська модель кіберстійкості все ще характеризується фрагментарністю нормативно-правового регулювання та недостатнім рівнем інституційної координації. Особливого значення для України набуває імплементація міжнародних стандартів NIST, ISO та NIS2, здатної забезпечити адаптивність системи кіберзахисту в умовах постійної трансформації кіберзагроз.

Водночас Україна має унікальний практичний досвід функціонування в умовах постійних кібер- та гібридних атак, що формує новий тип кіберстійкості, заснований не лише на нормативних

моделях, а й на реальній практиці протидії масштабним кібероперація-ям. Умови повномасштабної гібридної війни фактично перетворили Україну на простір апробації сучасних механізмів кібероборони, цифрової криміналістики та кримінального аналізу кіберінцидентів. Це створює підґрунтя для трансформації України з реципієнта міжнародних стандартів у активного учасника формування нових підходів до забезпечення міжнародної кібербезпеки.

Таким чином, сучасна система міжнародної кіберстійкості поступово трансформується у комплексний механізм управління цифровими ризиками, що поєднує правові, безпекові, кримінально-процесуальні та технологічні інструменти протидії кіберзагрозам. У цьому процесі особливого значення набуває кримінальний аналіз кіберінцидентів як елемент забезпечення цифрової безпеки та міжнародної координації у сфері протидії транснаціональній кіберзлочинності. Практичний досвід України в умовах гібридної війни формує підґрунтя для подальшого розвитку міжнародних підходів до кібероборони, цифрової криміналістики та захисту критичної інфраструктури.

Список використаних джерел:

1. Council of Europe. *Convention on Cybercrime* (Budapest Convention, ETS No. 185). URL: https://www.coe.int/ en/web/ cybercrime/the-budapest-convention

2. Cybersecurity and Infrastructure Security Agency (CISA). Official Website. URL: https://www.cisa.gov

3. National Institute of Standards and Technology (NIST). URL: https://www.nist.gov

4. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu

5. National Cyber Security Centre. URL: https://www.ncsc.gov.uk

6. Cooperative Cyber Defence Centre of Excellence (CCDCOE). NATO. URL: https://ccdcoe.org

ОСНОВИ ПОБУДОВИ ТА ПРИЗНАЧЕННЯ СИСТЕМИ «ВІРАЖ-ПЛАНШЕТ»

Сіфоров Олександр Іванович
кандидат технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ

Сучасна еволюція засобів повітряного нападу характеризується переходом до мережецентричних стратегій, масованим застосуванням безпілотних систем та критичним скороченням часу, необхідного для прийняття управлінських рішень. У цьому контексті автоматизована система (далі – АС) «Віраж-планшет» постає як фундаментальний елемент національної системи протиповітряної оборони України, забезпечуючи інтеграцію різнорідних джерел інформації в єдиний контур управління. Система «Віраж-планшет» за своїм призначенням є спеціалізованим програмно-апаратним комплексом, орієнтованим на автоматизацію процесів збору, обробки, відображення та аналізу інформації про повітряну та надводну обстановку.

Основним концептуальним завданням системи є підтримка прийняття рішень командирами частин і підрозділів Збройних Сил України, зокрема Радіотехнічних військ, Зенітних ракетних військ та авіації Повітряних Сил. В умовах інтенсивного бойового застосування система дозволяє мінімізувати когнітивне навантаження на оператора шляхом автоматичного узагальнення даних, що надходять від КП радіотехнічних батальйонів, окремих радіолокаційних рот та взаємодіючих підрозділів інших видів збройних сил. Функціональна архітектура системи забезпечує не лише відображення поточної ситуації, а й глибоку аналітику траєкторій, розрахунок рубежів перехоплення та видачу цілевказання вогневим засобам [1].

Важливим аспектом є уніфікація та стандартизація складових системи, що дозволяє інтегрувати її в загальну автоматизовану систему управління «Дніпро». Це створює умови для безперебійного обміну даними між різними рівнями командування, від тактичного планшета окремої мобільної групи до стратегічних командних центрів. Таким чином, «Віраж-планшет» виступає

сполучною ланкою, що перетворює розрізнені радіолокаційні відмітки на структуровану інформаційну модель бойового простору.

Програмне забезпечення системи «Віраж-планшет» розроблене як комплекс спеціальних програмних засобів (СПЗ), що встановлюються на автоматизованих робочих місцях (АРМ), об'єднаних у локальні та глобальні мережі обміну даними. Склад апаратно-програмного комплексу передбачає чіткий розподіл на загальносистемне та спеціальне програмне забезпечення, що гарантує стабільність роботи в умовах радіоелектронної протидії та кіберзагроз.

Центральним елементом СПЗ є програмний модуль АРМ сервера обробки і відображення повітряної (надводної) обстановки, відомий як АРМ-ОВПО або «електронний планшет». Цей модуль виконує роль інтелектуального хаба, де здійснюється злиття даних (data fusion) від декількох РЛС та інших сенсорів. Програмне забезпечення підтримує роботу з геоінформаційними системами (ГІС), що дозволяє накладати вектори цілей на високоточні цифрові карти та супутникові знімки.

Обмін даними в системі «Віраж-планшет» базується на стандартах сімейства TCP/IP, що забезпечує сумісність із сучасним мережевим обладнанням. Локальні мережі будуються відповідно до специфікацій IEEE 802.3z (1000Base-SX/LX), що гарантує пропускну здатність на рівні Gigabit Ethernet. Для фізичного рівня передачі використовуються волоконно-оптичні лінії зв'язку (ВОЛЗ) та мідна вита пара, а для мобільних сегментів — цифрові радіостанції Motorola.

Тактико-технічні характеристики системи «Віраж-планшет» визначаються її здатністю обробляти складні динамічні об'єкти в реальному часі. Система забезпечує автоматизацію зняття радіолокаційної інформації через аналого-цифрові перетворювачі, що дозволяє інтегрувати навіть застарілі зразки РЛС у сучасну цифрову мережу.

Функціонал системи дозволяє автоматично розгортати зони ураження паралельно курсу цілі, що критично важливо для мобільних вогневих груп. Оператор бачить на планшеті не лише позначку цілі, а й прогнозований вектор її руху. Коли ціль входить у розраховану зону, система видає сповіщення про перехід до «готовності №1». Це значно підвищує ефективність ППО, особливо при реалізації тактики «засідок». Для забезпечення точності

орієнтування система використовує GPS-модулі, які в реальному часі оновлюють координати вогневих засобів. Це дозволяє підрозділам ППО вести бойову роботу під час маневру, зберігаючи при цьому актуальність цілевказання, отриманого від віддалених РЛС.

Геопросторова обізнаність є основою функціонування «Віраж-планшет». Система оперує великими масивами картографічних даних, забезпечуючи прив'язку повітряної обстановки до фізичного рельєфу місцевості.

Зона ураження ПЗРК є складною об'ємною фігурою. Відповідно, дальність до дальньої та ближньої межі зони ураження не мають постійних значень. На основі дальності до дальньої та ближньої межі зони ураження з урахуванням часу польоту ракети розраховується дальня та ближня межі зони пуску ракет, а також рубіж переведення підрозділів в бойову готовність № 1. Ці розрахунки важко виконувати вручну. Для забезпечення ситуаційної обізнаності командирів та бойових обслуг система "Віраж-Планшет" автоматизує ці розрахунки з урахуванням рельєфу місцевості та місцевих предметів, що можуть зменшувати зону ураження на малих висотах [2].

На робочих місцях операторів використовується багатошарове представлення інформації. Нижні шари включають цифрові карти місцевості або супутникові знімки високої роздільної здатності. Це дозволяє командирам аналізувати «мертві зони» радіолокаційного покриття, зумовлені рельєфом, та оптимально розташовувати підрозділи. Система підтримує роботу з координатами в сучасних стандартах (наприклад, WGS-84), що забезпечує сумісність із західними системами навігації та цілевказання.

Особлива увага приділяється геодезичній прив'язці цілей. Точність визначення координат залежить від розташування об'єкта відносно бази сенсорів.

В умовах сучасної війни «Віраж-планшет» став ключовим інструментом протидії безпілотним літальним апаратам. Проблема виявлення малорозмірних та низькошвидкісних БПЛА, таких як «Shahed-136», полягає в їхній малій ЕПР, що робить їх майже невидимими для традиційних РЛС на фоні перешкод від землі.

Інноваційним підходом стала інтеграція системи «Віраж» з мережею пасивних акустичних сенсорів, відомою як «Sky Fortress». Ця система використовує понад 14000 мікрофонних вузлів,

розгорнутих по всій території країни. Кожен вузол складається з мікрофона та обчислювального блоку (початково на базі смартфонів, згодом — на базі спеціалізованого заліза Gen 3), встановлених на щоглах висотою близько 2 метрів. Акустичні дані передаються до центрального вузла «Віраж», де алгоритми машинного навчання ідентифікують звукові сигнатури ворожих об'єктів[3].

Мобільні вогневі групи, озброєні кулеметними установками, критично залежать від цілевказання системи «Віраж-планшет». Оскільки такі установки зазвичай не мають власних радарів чи тепловізорів, планшет з поточною повітряною обстановкою є єдиним засобом, що дозволяє їм завчасно підготуватися до зустрічі з ціллю та відкрити вогонь у потрібному секторі

Автоматизована система «Віраж-планшет» довела свою високу ефективність як гнучкий, масштабований та економічно вигідний інструмент управління протиповітряною обороною. Її здатність до інтеграції різнорідних даних — від потужних РЛС до тисяч дешевих акустичних датчиків — створює унікальний «інформаційний купол», здатний протистояти сучасним загрозам, включаючи масовані атаки роїв дронів.

Перспективи розвитку системи вбачаються у подальшому впровадженні алгоритмів штучного інтелекту для автоматичного розпізнавання цілей за акустичним та радіолокаційним профілем, а також у розвитку інтерфейсів з використанням технологій доповненої реальності та систем орієнтування голови для скорочення часу реакції оператора. Враховуючи досвід застосування, «Віраж-планшет» може стати основою для створення стандартів NATO в сегменті децентралізованих систем SHORAD/C-UAS.

Список використаних джерел:

1. Методичні рекомендації використання спеціалізованого програмного забезпечення «Віраж-планшет» під час підготовки бойових обслуг підрозділів зенітних ракетних військ Повітряних Сил Збройних Сил України. 2024. 44 с. URL: https://sprotyvg7.com.ua/wp-content/uploads/2024/11/%D0% 9C% D0%95 %D0% A2%D0%9E%D0%94%D0%A0%D0%95%D0%9A%D0%9E%D0 %9C%D0%95%D0%9D%D0%94%D0%90%D0%A6%D0%86%D0 %87-%D0%B2%D0%86%D0%A0%D0%90%D0%96-

%D0%9F%D0%9B%D0%90%D0%9D%D0%A8%D0%95%D0%A2.pdf (дата звернення: 03.03.2026).

2. Моделювання переносного зенітного ракетного комплексу «Piorun» у спеціальному програмному забезпеченні «Віраж-РД» / С. І. Бурковський та ін. Системи озброєння і військова техніка. 2023. № 3 (75). С. 39–52. DOI: https://doi.org/10.30748/soivt.2023.75.05.

3. Ukraine's "Sky Fortress". Warp 9. URL: https://www.warp9.io/ukraine-sky-fortress (дата звернення: 03.03.2026).

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПІДРОЗДІЛАХ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Терлецький Анатолій Володимирович
доктор філософії, викладач кафедри
адміністративно-правових дисциплін
Одеського державного університету внутрішніх справ

Кримінальна поліція як складова частина Національної поліції України, що ставить своїм завданням протидію злочинності, охорону прав і свобод людини, інтересів суспільства і держави, а також забезпечення публічної безпеки і порядку, відповідно до чинного законодавства України, в межах та задля виконання покладених на неї повноважень, має право на використання необхідної для цього інформації.

Щодо можливості використання інформації Закон України «Про Національну поліцію» визначає [1]:

- ст. 23: поліцейський, за письмовим запитом, може одержувати від державних органів, органів місцевого самоврядування, юридичних осіб державної форми власності інформацію, необхідну для виконання завдань та повноважень поліції;

- ст. 25: поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених законом. Поліція в рамках інформаційно-аналітичної діяльності: 1) формує реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2)

користується реєстрами та базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; 3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Крім того, поліція може створювати бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону, та інформаційно-аналітичні системи (у тому числі міжвідомчі), необхідні для виконання покладених на неї повноважень;

- ст. 27: поліція має безпосередній оперативний (у тому числі автоматизований) доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних» [2]. Інформація про доступ до реєстру та бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про особу, яка отримала доступ, та про обсяг даних, доступ до яких було отримано.

Разом з тим, ст. 18 Закону України «Про Національну поліцію» зобов'язує поліцейського зберігати інформацію з обмеженим доступом, яка стала йому відома у зв'язку з виконанням службових обов'язків, а ст. 28 визначає відповідальність за протиправне використання інформаційних ресурсів. Поліція має вживати всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації [1].

Саме наявність юридичної відповідальності співробітників поліції, у тому числі працівників підрозділів кримінальної поліції, за протиправне використання інформаційних ресурсів є одним з проявів забезпечення інформаційної безпеки під час виконання покладених на поліцію повноважень, адже встановлення відповідальності за вчинення протиправного діяння має попереджувальну та стримувальну функцію щодо вчинення подібних діянь як самою особою, так і іншими особами в майбутньому.

Проте, не лише наявністю індивідуальної відповідальності окремого співробітника має забезпечуватись інформаційна безпека і певному підрозділі кримінальної поліції.

Інформаційна безпека в підрозділах кримінальної поліції, крім того, забезпечується наявністю спеціального обладнання та приміщень, де має зберігатися документація зі службовою інформацією.

Слід зазначити, що відповідно наказу Національної поліції України від 12 жовтня 2018 року № 945 (у редакції наказу Національної поліції України від 01 вересня 2023 року № 810) певні відомості у сфері здійснення оперативно-розшукової діяльності та досудового розслідування, застосування оперативно-технічних заходів, відомості у сфері протидії тероризму та екстремістським проявам, боротьби з окремими видами злочинів відносяться до відомостей, що становлять службову інформацію в системі Національної поліції України [3].

При роботі з такою інформацією, поліцейські, у тому числі, працівники підрозділів кримінальної поліції, мають дотримуватись вимог Типової інструкції про порядок ведення, обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що місять службову інформацію, затвердженої постановою Кабінету Міністрів України від 19 жовтня 2016 року № 736 [4].

Так, зазначеною Інструкцією визначається порядок приймання та реєстрації документів зі службовою інформацією, їх надсилання та користування, друкування та перегляд, формування виконаних документів у справи, а також забезпечення збереженості таких документів.

Слід зазначити, що робота з документами зі службовою інформацією має проводитися в окремо виділених і належним чином обладнаних службових приміщеннях з дотриманням вимог, які унеможливлюють ознайомлення із змістом таких документів сторонніх осіб. Допуск працівників до роботи з такими документами здійснюється лише на підставі списку, складеного посадовою особою, відповідальною за роботу із службовою інформацією, і затвердженого відповідним керівником підрозділу.

Документи, що містять інформацію «Для службового користування» в обов'язковому порядку мають зберігаються у шафах,

сейфах, що розташовані у службових приміщеннях або сховищах архіву. Такі шафи, сейфи, службові приміщення, сховища архіву повинні надійно замикатися і опечатуватися металевими печатками, порядок виготовлення та використання яких визначається керівником установи. Слід зауважити, що зберігання таких документів здійснюється працівниками, які безпосередньо отримали їх під розписку, у спосіб, який унеможливлює доступ до них сторонніх осіб.

Крім того, документи, що становлять службову інформацію, не дозволяється виносити за межі установи, крім випадків передачі документів на виконання у структурні підрозділи, що розташовуються поза межами основного приміщення установи, та у разі виникнення необхідності в їх узгодженні, підписанні в установах, розташованих у межах одного населеного пункту. Винесення такого документа за межі установи здійснюється на підставі резолюції керівника установи (його заступника) або керівника структурного підрозділу, в якому такий документ (його проект) підготовлено. При цьому документ повинен бути вкладений у конверт або упакований у такий спосіб, щоб виключити можливість його прочитання [4].

Отже, забезпечення інформаційної безпеки в поліції в цілому та підрозділах кримінальної поліції зокрема забезпечується чітким та безумовним виконанням та дотриманням чинного законодавства України, що регулює зазначене питання, а також власною самоорганізацією, відповідальністю та контролем під час виконання покладених на поліцію обов'язків.

Список використаних джерел:

1. Про Національну поліцію : Закон України від 02.07.2015 року № 580-VIII. Дата оновлення: 12.04.2026. URL: https://zakon.rada.gov.ua/laws/show/580-19?find=1&text#Text.

2. Про захист персональних даних : Закон України від 01.06.2010 року № 2297-VI. Дата оновлення: 14.06.2025. URL: https://zakon.rada. gov.ua/laws/show/2297-17#Text.

3. Про внесення змін до Переліку відомостей, що становлять службову інформацію в системі Національної поліції України : Наказ Національної поліції України від 01.09.2023 року № 810. URL: https://zakon.rada.gov.ua/rada/show/v0810887-23#Text.

4. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших

матеріальних носіїв інформації, що містять службову інформацію: Постанова Кабінету Міністрів України від 19.10.2016 року № 736. Дата оновлення: 25.08.2023. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text.

ПРОТИДІЯ DEEPFAKE-ТЕХНОЛОГІЯМ: ЗАГРОЗА ДЕЗІНФОРМАЦІЇ ТА МЕТОДИ ВЕРИФІКАЦІЇ КОНТЕНТУ

Томас Ростислав Русланович
курсант І курсу ННІ № 4-25-101 Кб, рядовий поліції
Харківського національного університету внутрішніх справ
Науковий керівник: ***Кіріка Діана Володимирівна***
кандидатка юридичних наук, доцентка,
доцентка кафедри адміністративної діяльності ННІ №3
Харківського національного університету внутрішніх справ

Сьогодні вміти відрізнити фейкове відео чи аудіо від справжнього - це не просто «корисна фішка», а питання власної безпеки. Сучасні нейромережеві технології досягли такого рівня розвитку, що здатні створювати надзвичайно реалістичні підроблені аудіо- та відеоматеріали, які часто складно відрізнити від автентичних. Технологія діпфейків перестала бути експериментальним або розважальним явищем, вона активно використовується як інструмент інформаційних маніпуляцій, шахрайства та дискредитації. За допомогою діпфейків здійснюється поширення неправдивої інформації, фінансове ошуканство, а також вплив на суспільну думку.

Метою дослідження є комплексне вивчення механізмів створення діпфейків та розробка обґрунтованого підходу до їх виявлення шляхом застосування технічних засобів верифікації та розвитку медіаграмотності. У межах дослідження передбачається класифікація видів синтетичного контенту та способів його поширення; аналіз програмних засобів детекції на основі виявлення біометричних аномалій і цифрових артефактів; оцінювання ефективності законодавчих ініціатив щодо регулювання технологій штучного інтелекту. Огляд літератури та існуючих досліджень демонструє перехід наукової спільноти від простого вивчення

алгоритмів GAN (Generative Adversarial Networks) до розробки систем «цифрового водяного знаку» та блокчейн-протоколів для підтвердження походження медіафайлів. Структура роботи вибудувана від розбору технічної природи маніпуляцій до формування практичних рекомендацій щодо впровадження систем автоматизованого моніторингу інформаційного простору, що дозволить мінімізувати вплив дезінформації на суспільні та державні інститути.

Deepfake-технології концептуалізуються, як об'єкт суворого правового регулювання через їхній потенціал впливу на суспільну безпеку та фундаментальні права громадян. EU AI Act визначає діпфейк, як результат функціонування систем штучного інтелекту, що генерують або маніпулюють контентом (зображеннями, аудіо- чи відеоматеріалами), створюючи високий ступінь схожості з реальними особами, об'єктами або подіями. Ключовою юридичною ознакою такого контенту є його здатність вводити пересічного спостерігача в оману, створюючи ілюзію автентичності там, де подія або образ є штучно сконструйованими.

Технологічний фундамент створення діпфейків, згідно з аналітичним підходом регулятора, базується на передових методах машинного та глибокого навчання (Deep Learning). Ці системи здатні аналізувати величезні масиви біометричних та візуальних даних для синтезування голосу, міміки та рухів, що майже не відрізняються від природних. Закон класифікує такі системи як інструменти, що потребують підвищеної прозорості: постачальники зобов'язані забезпечити маркування згенерованого контенту у машинозчитуваному форматі. Це дозволяє ідентифікувати штучне походження медіафайлів на етапі їх поширення, що є критично важливим для протидії маніпуляціям у цифровому середовищі.

Сфери застосування Deepfake-технологій, охоплюють широкий спектр суспільних відносин. У сфері політики та медіа діпфейки розглядаються як загроза демократичним процесам, що вимагає негайного розкриття інформації про їхнє походження для запобігання дезінформації. У рекламі та бізнесі ШІ допомагає створювати крутий персоналізований контент, але закон тут суворий: треба чітко показувати, де реальна зйомка, а де - графіка. Для творчості, мемів чи сатири правила трохи м’якші, щоб не обмежувати задум автора. Головне, щоб такі відео не ганьбили людей і не видавали брехню за правду. В EU AI Act (це європейський

закон про штучний інтелект) прямо кажуть: маркувати діпфейки - це не просто формальність. Це потрібно, щоб люди розуміли, що перед ними, і не давали себе обдурити. Тільки так можна зберегти довіру до технологій та захистити приватність кожного з нас у цифровому світі[1].

Діпфейки - це вже не просто технологічна новинка, а серйозна загроза для нашої приватності та цифрового «я». Експерти NIST кажуть прямо: через такі підробки люди взагалі перестають вірити будь-якій інформації. На рівні держави це б'є по виборах і демократії, бо фейками легко дискредитувати політиків і маніпулювати думкою суспільства. А в звичайному житті та бізнесі це призводить до «інформаційного нігілізму» - стану, коли ніхто не вірить нікому. Це тягне за собою реальні збитки: від обвалів на біржах через вкинуте фейкове відео до руйнування репутації великих компаній.

У NIST також виділяють конкретні схеми шахрайства. Наприклад, «діпфейк-фішинг», коли хакери підробляють голос або обличчя боса, щоб виманити гроші чи отримати доступ до секретних даних. Тому зараз кожна компанія має прораховувати такі ризики й бути готовою, що будь-який дзвінок чи відео може виявитися професійною підробкою. Такі випадки демонструють перехід від традиційних методів соціальної інженерії до високотехнологічних маніпуляцій, які потребують впровадження нових механізмів управління ідентифікацією (Identity Management).

Особлива увага приділяється психологічному впливу на аудиторію, що визначається як «шкода, пов’язана з приватністю» (privacy-related harm). У NIST кажуть прямо: діпфейки настільки реалістичні, що наш мозок спочатку реагує емоційно, а вже потім включає логіку. Через це люди живуть у постійній тривозі, бо розуміють - будь-хто може вкрасти їхнє обличчя чи голос і використати це для брудних маніпуляцій, а захиститися від цього майже неможливо. Ще одна небезпечна штука - так званий «парадокс брехуна». Коли фейків стає занадто багато, справжні злочинці можуть просто заявити, що реальний доказ проти них - це теж діпфейк. Це створює повний хаос, де ніхто вже не знає, чому вірити. Висновок NIST такий: просто технічних програм для розпізнавання підробок уже замало. Потрібно повністю міняти підхід до безпеки даних на всіх етапах — від їх створення до зберігання,

щоб повернути людям хоч якийсь контроль над своєю цифровою особистістю[2].

Методи верифікації мультимедійного контенту концептуалізуються, як багаторівнева архітектура захисту інформаційного суверенітету. У межах цієї парадигми традиційні методи верифікації, такі як фактична перевірка (fact-checking) та судова медіаекспертиза, розглядаються як критично важливий інтелектуальний рівень аналізу. Попри автоматизацію, роль людини-експерта залишається визначальною у виявленні контекстуальних аномалій та логічних невідповідностей, які часто ігноруються алгоритмами, але є характерними для синтетичного контенту. Експертний аналіз артефактів освітлення, тіней та фізики рухів дозволяє верифікувати автентичність на основі невідповідності цифрового сигналу законам реального фізичного світу. Паралельно з традиційними підходами, ITU-T AMAS фокусується на розробці та впровадженні передових технологічних рішень для виявлення Deepfake.

Науковий аналіз спрямований на детектування біологічних та цифрових сигнатур ШІ, зокрема через аналіз мікроколивань шкіри (фотоплетизмографія) та виявлення невідповідностей у фазах артикуляції (lip-sync errors). Особливе місце у звітах посідає концепція «цифрового ланцюга походження» (provenance), яка передбачає використання криптографічних підписів та метаданих для фіксації історії створення та редагування медіафайлу. Це дозволяє трансформувати процес верифікації з пасивного пошуку підробок у активну систему підтвердження цілісності контенту з моменту його генерації камерою або програмним забезпеченням.

Стратегічним вектором діяльності ITU є розвиток міжнародних стандартів і рекомендацій для медіа та журналістики. У науковому дискурсі AMAS наголошується, що без глобальної стандартизації метаданих та протоколів прозорості журналістика не зможе ефективно протидіяти масштабним кампаніям дезінформації. Рекомендації ITU включають впровадження єдиних технічних стандартів для маркування ШІ-генерованого контенту та створення інтероперабельних платформ для обміну даними про верифіковані джерела. ITU-T AMAS стверджує, що лише через інтеграцію технологічних інструментів детектування у суворі етичні та технічні стандарти медіавиробництва можливо забезпечити

сталість «екосистеми довіри» в умовах тотальної експансії генеративного штучного інтелекту[3].

Отже, здатність розпізнавати фальсифікований цифровий контент набуває особливого значення та стає важливою складовою інформаційної безпеки особистості. В умовах постійного інформаційного протистояння цифрова грамотність і дотримання принципів цифрової гігієни є необхідними навичками для кожного. Недостатній рівень критичного сприйняття інформації та невміння виявляти маніпулятивний контент можуть призвести до негативних наслідків як для окремих осіб, так і для суспільства та держави загалом.

Список використаних джерел:

1. EU AI Act (Article 50): Transparency Requirements for Deepfakes. URL: https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/ (дата звернення: 16.05.2026)
2. NIST Privacy Framework 1.1 (Final Release Q4 2025). URL: https://www.nist.gov/privacy-framework (дата звернення: 15.05.2026)
3. ITU-T AMAS (AI and Multimedia Authenticity Standards). URL: https://aiforgood.itu.int/multimedia-authenticity/reports/ (дата звернення: 16.05.2026)

КІБЕРБЕЗПЕКА ТА ВИКЛИКИ КОНФІДЕНЦІЙНОСТІ В СИСТЕМАХ DRONE ID

Удренас Галина Іванівна
доцент кафедри тактико-спеціальної та спеціальної фізичної підготовки факультету підготовки фахівців для підрозділів превентивної поліції Національної поліції України Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Системи Drone ID (Remote ID) — це фактично «цифрові номерні знаки» для безпілотників. Хоча вони розроблені для підвищення безпеки повітряного простору та ідентифікації порушників, їхнє впровадження відкриває серйозну «скриньку Пандори» щодо кібербезпеки та приватності.

Впровадження Drone ID супроводжується значними ризиками у сфері інформаційної безпеки, оскільки більшість сучасних протоколів трансляції розроблялися з пріоритетом на відкритість та простоту, а не на захищеність.

Системи DroneID передають дані (ID оператора, координати дрона, точку зльоту, швидкість) через відкриті канали, такі як Bluetooth Legacy, Bluetooth 5.x або Wi-Fi NAN (Neighbor Awareness Networking).

Дослідження безпеки дронів лідера ринку DJI (який займає близько 94% світового споживчого сегменту) виявили, що пропрієтарний протокол Drone ID передає дані в нешифрованому вигляді [1]. Це дозволяє пасивним зловмисникам за допомогою дешевого обладнання (SDR) перехоплювати інформацію про місцезнаходження не лише дрона, а й пілота ("home point").

Використання SDR (Software Defined Radio), це найпотужніший метод. Пристрої на кшталт HackRF One або RTL-SDR дозволяють сканувати ефір та «слухає» частоти 2.4 ГГц. Спеціальне ПЗ (наприклад, на базі GNU Radio) виокремлює пакети даних, що відповідають стандарту ASTM F3411 (міжнародний стандарт Remote ID). Це дозволяє бачите не просто «шум», а координати GPS, серійний номер та висоту дрона в реальному часі на мапі.

Ще один з способів не законого втручання, це сніффінг через смартфони та ESP32. Застосунки типу Drone Scanner використовують вбудований Bluetooth/Wi-Fi чіп телефону для пасивного прослуховування пакетів DroneID.

ESP32/Arduino це маленький чіп за $5 можна прошити як сканер, який буде вібрувати або надсилати сповіщення в Telegram, щойно в радіусі 500-1000 метрів з'явиться дрон. Багато сучасних систем (наприклад, DJI Aeroscope) працюють саме за цим принципом, але з набагато потужнішими антенами, що дозволяє «бачити» пілота за 10-50 км.

Такі вразливості створюють ризики для фізичної безпеки легітимних операторів та комерційної таємниці компаній. До критичних вразливостей у прошивках сучасних БПС, можна віднести можливість:

— зловмисникам отримати привілейований (root) доступ до системи управління;

— дистанційно вимкнути або підмінити трансляцію Remote ID;

— здійснити атаку типу "відмова в обслуговуванні" (DoS), спричинивши падіння апарата в польоті;

— використовувати підроблені серійні номери для маскування зловмисної діяльності.

Спроби впровадження шифрування часто стикаються з технічними обмеженнями. Наприклад, аналіз схеми шифрування FMX у деяких робототехнічних системах показав використання статичних ключів, що повторюються на всіх пристроях серії, та застарілих алгоритмів (Blowfish-ECB), що робить такий захист номінальним. Більш того, відкрита архітектура ADS-B та RID робить їх вразливими до спуфінгу — трансляції хибних координат, що може призвести до зіткнень у повітрі або дезорієнтації систем управління трафіком.

Для балансу між безпекою та приватністю в сфері поліцейської діяльності пропонуємо такі підходи:

— Заміна постійного ID на тимчасові токени, які змінюються кожні кілька годин. Мова йде про динамічні ідентифікатори;

— Шифрування координат оператора так, щоб їх могли розшифрувати лише державні органи;

— Використання технології блокчейну, тобто верифікації справжності повідомлень та запобігання спуфінгу.

DroneID — це компроміс. Для регуляторів це інструмент порядку, для користувачів — потенційна діра в безпеці. У військових умовах (як ми бачимо в Україні) використання стандартних протоколів Drone ID часто є смертельно небезпечним, що змушує пілотів програмно або фізично відключати ці модулі.

Список використаних джерел:

1. Drone Security and the Mysterious Case of DJI’s DroneID. URL https://www.ndsssymposium. org/wpcontent/uploads/ 2023 /02/ndss2023_f217_paper.pdf

СЕКЦІЯ 3.
ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

ПРОБЛЕМИ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Астапова Діана Максимівна
курсант 202 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Науковий керівник: ***Собко Ганна Миколаївна***
професор кафедри кримінального права та кримінології ОДУВС д.ю.н., професор

Проблеми кваліфікації кіберзлочинів, що вчиняються проти основ національної безпеки України, на сучасному етапі розвитку державності набувають особливої гостроти через трансформацію традиційних методів підривної діяльності у цифрову площину. Стрімкий розвиток інформаційно-комунікаційних технологій протягом останніх десятиліть докорінно змінив ландшафт загроз, оскільки активна інтеграція комп'ютерних систем у всі сфери державного управління робить їх вразливою ціллю для злочинних посягань. Динаміка розвитку технологій часто випереджає законодавчу реакцію, що створює певні прогалини у правовому регулюванні та ускладнює процес притягнення винних осіб до відповідальності [1, с. 63]. Така тенденція зумовлена розмиванням меж між фізичним та віртуальним протистоянням, у якому кібератаки еволюціонували з інструментів промислового шпигунства до рівня повноцінної зброї масового дестабілізуючого впливу на державні інститути. Особливої гостроти ця проблема набула в умовах повномасштабного вторгнення та дії воєнного стану. Сьогодні кібератаки є невід'ємною складовою гібридної агресії, спрямованою на дестабілізацію конституційного ладу та

територіальної цілісності України. Центральною проблемою правозастосування є визначення об'єкта посягання, де суспільні відносини щодо забезпечення зовнішньої та внутрішньої безпеки держави, її конституційного ладу та територіальної цілісності переплітаються з технічними аспектами функціонування комп'ютерних систем. З огляду на положення Стратегії кібербезпеки України, актуалізується потреба у чіткому розмежуванні актів кібертероризму, кібердиверсій та державної зради, що вчиняються з використанням інформаційно-комунікаційних технологій, семе тому кваліфікація дій за статтями розділу І Особливої частини Кримінального кодексу України у поєднанні з використанням кіберзасобів потребує ретельного аналізу суб'єктивної сторони та специфіки способу вчинення діяння. Зокрема, державна зрада у формі надання іноземній державі чи організації допомоги в проведенні підривної діяльності проти України сьогодні часто виражається у проведенні масованих хакерських атак на об'єкти критичної інфраструктури або у зборі конфіденційної інформації через несанкціонований доступ до державних реєстрів [2, с. 99]. При цьому виникає складна правова колізія щодо відмежування шпигунства від державної зради, а також необхідність чіткого розмежування цих складів від загально кримінальних злочинів у сфері використання ЕОМ. Не менш складною є кваліфікація посягань на територіальну цілісність, вчинених через соціальні мережі та веб-ресурси, де ключовою проблемою стає встановлення моменту закінчення злочину та розмежування публічних закликів від приватної думки, що неможливо без проведення комплексних лінгвістичних та ІТ-експертиз [3, с. 455-456]. Особливу небезпеку становить кібердиверсія, яка передбачає втручання в роботу автоматизованих систем управління з метою ослаблення держави, що за своїми наслідками може бути еквівалентним фізичному знищенню стратегічних об'єктів. Проте встановлення прямого причинно-наслідкового зв'язку між програмним кодом та матеріальними наслідками є значним викликом для слідства. Специфіка досліджуваної проблеми полягає у невідповідності традиційного інструментарію кримінального права динамічній природі цифрових доказів, що вимагає переосмислення класичних ознак складу злочину в контексті високої анонімності та транскордонності кіберзлочинців. Важливою перешкодою для ефективної

кваліфікації є транснаціональний характер таких злочинів, оскільки організатори атак найчастіше перебувають поза межами української юрисдикції, використовуючи засоби анонімізації для приховування цифрових слідів [4, с. 44]. Це вимагає від правоохоронних органів не лише глибоких знань кримінального права, а й володіння методиками виявлення специфічних електронних доказів у криміналістичному аспекті [5, с. 39]. Безпрецедентне зростання кількості кіберінцидентів на об'єкти критичної інфраструктури протягом 2022–2026 років підтверджує необхідність негайної модернізації системи кримінально-правової кваліфікації та адаптації законодавства шляхом криміналізації нових видів цифрових загроз, які наразі не відображені в диспозиціях статей КК України, проте становлять реальну небезпеку для національних інтересів. Такий підхід забезпечить ефективну протидію гібридним загрозам через усунення прогалин у правовому регулюванні новітніх методів підривної діяльності. Ефективна протидія таким посяганням можлива лише за умови системного підходу, який включає вдосконалення законодавчих конструкцій, підвищення технічної компетенції суб'єктів розслідування та розширення міжнародного співробітництва у сфері колективної кібербезпеки. Вирішення правових колізій та встановлення чітких критеріїв кваліфікації за ознаками мети та наслідків є першочерговим завданням для забезпечення стабільності національної безпеки в умовах гібридної агресії. В умовах повномасштабної агресії рф кіберпростір став повноцінним доменом ведення бойових дій, де цифрові атаки за своєю руйнівною силою можуть прирівнюватися до конвенційного озброєння. Особлива актуальність дослідження зумовлена тим, що чинний Кримінальний кодекс України потребує оперативного адаптування до тактики «гібридної війни», де межа між кримінальним хакерством та державною зрадою стає дедалі тоншою. Ефективна кваліфікація таких діянь сьогодні є не просто юридичним питанням, а критичним елементом забезпечення національної стійкості та невідворотності покарання для осіб, що сприяють ворогу в цифровому полі. Вирішення правових колізій та впровадження спеціалізованих методик доказування дозволить правоохоронній системі діяти на випередження, захищаючи конституційний лад та територіальну цілісність держави. Таким чином, системне реформування підходів до кримінально-правової

оцінки кіберзагроз є стратегічним пріоритетом для зміцнення національної безпеки України на сучасному етапі.

Список використаних джерел:

1. Козій А., Марченко Т., Шевченко В. Актуальні проблеми протидії кіберзлочинності в Україні // Theoretical foundations of state and law : collective monograph / Bondar V., Kuzmenko I., Rudnichenko S., Dumanskyi R. etc. Boston : Primedia eLaunch, 2022. С. 59–65. URL: https://isg-konf.com/wp-content/uploads/ 2022/04/ Monograph/Doi/Legal/ISG.2022.MONO.LEGAL.1.2.3.pdf

2. Проблеми кваліфікації злочинів проти основ національної безпеки України : методичні поради і завдання. Харків : Національний юридичний університет імені Ярослава Мудрого, 2019. Електронне видання. URL: https://library.nlu.edu.ua/ POLN_ TEXT/POSIBNIKI_2019/MPiZ_214.pdf

3. Погорецький М. М., Клименко С. В. Проблеми криміналізації кіберзлочинів в Україні. Вісник кримінального судочинства. 2026. № 1. С. 447–459. DOI: https://doi.org/10.59835/2413-5372.2026.1/447-459 URL: https://vkslaw.com.ua/index. php/ journal/article/view/919/795

4. Самойленко О., Цехан Д. Транснаціональні кіберзлочини: навчально-методичний посібник для здобувачів вищої освіти [Електронне видання]. Одеса : Фенікс, 2024. 136 с. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/275e67bb-4664-4404-a7e9-5b7d8241e7a5/content

5. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект : навчально-методичний посібник. Одеса : Національний університет «Одеська юридична академія», 2020. 133 с. URL: https://dspace.onua.edu.ua/server/ api/core/bitstreams/ c5fd2 1d6-f96b-4531-ad0c-da2272b64aab/content

ВИКОРИСТАННЯ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ ДЛЯ ВДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Бойко Андрій Володимирович
доктор юридичних наук, професор кафедри
адміністративно-правових дисциплін,
Одеського державного університету внутрішніх справ

Сучасні тенденції розвитку злочинності характеризуються зростанням рівня її організованості, транснаціонального характеру та активним використанням цифрових технологій. За таких умов підвищується значення кримінального аналізу як інструменту інформаційно-аналітичного забезпечення правоохоронної діяльності. Ефективність кримінального аналізу значною мірою залежить від здатності аналітиків обробляти великі масиви різнорідних даних, виявляти приховані зв'язки між подіями та особами, а також прогнозувати можливі сценарії розвитку криміногенної ситуації. У зв'язку з цим особливої актуальності набуває використання методів системного аналізу, які дозволяють розглядати злочинність та діяльність правоохоронних органів як складні динамічні системи [1].

Системний аналіз являє собою сукупність методологічних підходів, спрямованих на дослідження складних об'єктів шляхом вивчення їх структури, функцій, взаємозв'язків між елементами та впливу зовнішнього середовища. Використання системного підходу в кримінальному аналізі дає можливість перейти від дослідження окремих фактів до комплексного вивчення кримінальних явищ. При цьому злочинна діяльність розглядається як система, що складається з взаємопов'язаних суб'єктів, ресурсів, каналів комунікації, фінансових потоків та інших елементів. Такий підхід сприяє більш глибокому розумінню механізмів функціонування злочинних мереж та підвищує якість управлінських рішень у сфері протидії злочинності [1].

Одним із перспективних напрямів застосування системного аналізу є побудова моделей кримінальних процесів та мережевих структур злочинних угруповань. Методи графового аналізу дозволяють виявляти ключових учасників злочинних груп,

визначати характер зв'язків між ними та оцінювати стійкість кримінальних мереж до зовнішнього впливу. Крім того, використання моделей системної динаміки забезпечує можливість прогнозування змін криміногенної ситуації залежно від різних управлінських впливів і зовнішніх факторів. Це створює передумови для переходу від реактивної до проактивної моделі діяльності правоохоронних органів.

Особливого значення методи системного аналізу набувають у процесі обробки цифрової інформації, що використовується під час розслідування кримінальних правопорушень. Сучасні дослідження демонструють ефективність інтеграції інструментів штучного інтелекту, обробки природної мови та цифрової криміналістики для аналізу доказової інформації. Використання інтелектуальних систем дозволяє автоматизувати класифікацію даних, встановлення зв'язків між доказами та їх співвіднесення з нормами кримінального законодавства, що значно підвищує швидкість і якість аналітичної роботи [2].

В умовах цифрової трансформації правоохоронної діяльності важливим напрямом розвитку кримінального аналізу є створення інтегрованих інформаційно-аналітичних систем, здатних забезпечувати збір, накопичення, обробку та візуалізацію даних із різних джерел. Застосування методів системного аналізу під час проєктування таких систем сприяє формуванню єдиного інформаційного середовища для підтримки прийняття рішень. У результаті забезпечується більш ефективне використання наявних інформаційних ресурсів, знижується ризик втрати важливої інформації та підвищується оперативність реагування на кримінальні загрози [1; 2].

Таким чином, використання методів системного аналізу є перспективним напрямом удосконалення кримінального аналізу в діяльності правоохоронних органів України. Системний підхід забезпечує комплексне дослідження кримінальних явищ, сприяє виявленню закономірностей розвитку злочинності, підвищує якість прогнозування та ефективність управлінських рішень. Подальший розвиток методології кримінального аналізу доцільно пов'язувати з інтеграцією методів системного аналізу, технологій штучного інтелекту та сучасних інформаційно-аналітичних платформ, що відповідає актуальним тенденціям цифровізації правоохоронної діяльності.

Список використаних джерел:

1. Ковальова О. В., Батрак К. О. International Legal Principles of Information Support of Law Enforcement Activities in Ukraine. Ukrainian Polyceistics: Theory, Legislation, Practice. 2026. № 1. С. 17–22. DOI: 10.32782/2709-9261-2026-1-17-22.

2. Фединишин Т., Партика О. Генерація з доповненням на основі пошуку для судово-правового аналізу: інтеграція Кримінального кодексу України з доказами з мобільних пристроїв. Кібербезпека: освіта, наука, техніка. 2026. Т. 4. № 32. С. 478–488. DOI: 10.28925/2663-4023.2026.32.1196.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ НАРКОЗЛОЧИННОСТІ

Давидкін Влас Олександрович
курсант 202 взводу Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Форос Ганна Володимирівна
завідувачка кафедри кримінального аналізу та інформаційних технологій, к.ю.н., доцент ОДУВС

У сучасних умовах розвитку українського суспільства особливої актуальності набуває проблема протидії організованій злочинності, зокрема злочинам у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів. Наркобізнес є одним із найбільш прибуткових видів злочинної діяльності, що приваблює організовані злочинні угруповання та сприяє формуванню стійких кримінальних структур. Організована наркозлочинність становить серйозну загрозу національній безпеці держави, оскільки пов’язана з отриманням значних незаконних прибутків, розвитком транснаціональних кримінальних зв’язків, корупційними проявами та негативним впливом на соціальну безпеку суспільства [1, с. 447].

Науковці зазначають, що організована злочинність є складним соціально-правовим явищем, яке характеризується наявністю стійких злочинних об'єднань, чіткою ієрархічною структурою, розподілом ролей між учасниками та плануванням злочинної діяльності. У межах таких угруповань існує система внутрішніх зв'язків та дисципліни, що забезпечує координацію протиправної діяльності та отримання стабільних незаконних прибутків [1, с. 446]. Одним із ключових напрямів діяльності організованих злочинних груп є незаконний обіг наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів.

Організована наркозлочинність охоплює комплекс протиправних дій, пов'язаних із виробництвом, зберіганням, транспортуванням і збутом наркотичних засобів. Дослідники зазначають, що злочини у сфері незаконного обігу наркотиків характеризуються високим рівнем латентності, оскільки вони часто вчиняються без очевидних потерпілих, із використанням різноманітних засобів конспірації та сучасних технологій комунікації [2, с. 95]. Крім того, розвиток цифрових технологій значно ускладнив процес виявлення та документування таких злочинів, оскільки злочинці активно використовують мережу Інтернет, електронні платіжні системи та інші сучасні засоби зв'язку.

У зв'язку з цим важливого значення набуває інформаційно-аналітичне забезпечення діяльності правоохоронних органів. У науковій та спеціальній літературі зустрічаються такі поняття, як «інформаційно- аналітичне забезпечення», «інформаційно- аналітична робота». Ми вважаємо, що інформаційно-аналітичне забезпечення є поняттям більш ширшим та важливішим для управління складними соціальними системами. Інформаційно-аналітичне забезпечення – це сукупність технологій, методів збору та обробки інформації, що характеризує об'єкт управлінського впливу (соціальні, політичні, економічні та інші процеси), специфічних прийомів їхньої діагностики, аналізу та синтезу, а також оцінки наслідків прийняття різних варіантів політичних рішень. Так нашу думку, систему інформаційного-аналітичного забезпечення можна визначити як взаємозалежну та відповідним чином сформовану сукупність організаційних, організаційно- правових, інформаційних, методичних, програмно- технологічних компонентів, що забезпечує необхідну якість прийнятих управлінських

рішень за рахунок раціонального використання інформаційних ресурсів та інформаційних технологій [3, с. 193] .

Головною категорією інформаційно- аналітичного забезпечення є інформація, за від-сутності якої неможливо правильно і цілеспрямовано реалізовувати управлінський процес. Згідно ст. 1 Закону України «Про інформацію», інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Сучасні умови розвитку інформаційного суспільства сприяють активному використанню відкритих джерел інформації у діяльності правоохоронних органів. Методи OSINT дозволяють отримувати важливі відомості з відкритих інформаційних ресурсів, зокрема соціальних мереж, електронних платіжних сервісів та інших цифрових платформ. Аналіз таких даних дає можливість встановлювати канали збуту наркотичних засобів, виявляти зв'язки між учасниками злочинних угруповань та документувати їх протиправну діяльність.

Важливим елементом інформаційно-аналітичного забезпечення є також використання спеціалізованих інформаційних систем та баз даних, що функціонують у правоохоронних органах. Використання таких систем дозволяє накопичувати значні масиви інформації та здійснювати їх комплексний аналіз, що значно підвищує ефективність протидії організованій злочинності.

Таким чином, інформаційно-аналітичне забезпечення відіграє важливу роль у діяльності Національної поліції України у сфері протидії організованій наркозлочинності. Використання сучасних аналітичних методів, інформаційних технологій та можливостей відкритих джерел інформації дозволяє підвищити ефективність виявлення, документування та припинення діяльності організованих злочинних угруповань, що займаються незаконним обігом наркотичних засобів.

Список використаних джерел:

1. Джужа О. М., Василевич В. В., Чернєй В. В., Чернявський С. С. Кримінологія : підручник. Київ : Національна академія внутрішніх справ, 2020. 612 с.

2. Мигаленко П. С., Пчолкін В. Д. Криміналістична характеристика злочинів, пов'язаних із незаконним обігом наркотичних засобів, психотропних речовин або їх аналогів. Актуальні

проблеми сучасної науки в дослідженнях молодих учених. 2021. С. 95–100.

3. Мельнікова О.О., Форос Г.В. Особливості використання інформаційно-аналітичного забезпечення оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми. Правова держава, 2021. № 42. С. 189-196

АНАЛІТИЧНІ ПРОДУКТИ КРИМІНАЛЬНОГО АНАЛІЗУ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Драч Владислав Максимович
курсант 202 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України
Науковий керівник: ***Калугін Володимир Юрійович***
Професор кафедри кримінального аналізу
та інформаційних технологій, к.ю.н., доцент

У сучасних умовах розвитку правоохоронної діяльності кримінальний аналіз виступає одним із ключових інструментів підвищення ефективності оперативно-розшукової діяльності. Особливе значення у цьому процесі мають аналітичні продукти, які формуються на основі обробки та узагальнення інформації про злочинну діяльність. До таких продуктів належать аналітичні довідки, кримінальні карти, схеми зв'язків, профілі злочинців, прогностичні звіти та інші матеріали, що дозволяють виявляти закономірності та тенденції розвитку злочинності [1, с. 307].

Аналітичні продукти кримінального аналізу становлять ключовий результат інтелектуально-аналітичної діяльності у сфері протидії злочинності та відіграють визначальну роль у забезпеченні ефективного функціонування правоохоронних органів. [2, с. 32] У сучасних умовах зростання обсягів інформації, ускладнення криміногенної ситуації та активного використання злочинними угрупованнями новітніх технологій, саме якісно підготовлені аналітичні продукти дозволяють трансформувати розрізнені

дані у цілісні знання, необхідні для прийняття обґрунтованих управлінських і процесуальних рішень.

Під аналітичними продуктами кримінального аналізу доцільно розуміти систематизовані результати обробки інформації, представлені у формі документів, візуалізацій, моделей або прогнозів, які відображають суттєві характеристики злочинної діяльності, її структуру, тенденції та взаємозв'язки. Їх створення базується на використанні комплексу методів, зокрема статистичного аналізу, аналізу зв'язків, геоінформаційного аналізу, контент-аналізу та методів прогнозування.

Аналітичні продукти кримінального аналізу забезпечують перехід від реактивної моделі діяльності правоохоронних органів до проактивної, що передбачає попередження злочинів ще на етапі їх підготовки. Використання аналітичних продуктів дозволяє значно підвищити ефективність прийняття управлінських рішень, оскільки вони базуються на системному аналізі інформації та враховують взаємозв'язки між різними елементами злочинної діяльності [3, с. 18].

Важливою складовою аналітичних продуктів є візуалізація даних, яка дозволяє більш ефективно сприймати інформацію та виявляти приховані зв'язки між об'єктами аналізу. Використання графічних моделей, карт зв'язків та інших інструментів візуалізації сприяє підвищенню якості аналітичної роботи та забезпечує більш ефективне використання отриманих результатів у практичній діяльності.

У сучасних умовах особливого значення набуває використання цифрових технологій у процесі створення аналітичних продуктів. Зокрема, застосування спеціалізованого програмного забезпечення дозволяє обробляти великі обсяги даних, автоматизувати аналітичні процеси та підвищити точність отриманих результатів. Крім того, важливим джерелом інформації є відкриті джерела (OSINT), які дозволяють отримувати актуальні дані про осіб, події та об'єкти без порушення законодавства.

Разом із тим, ефективність використання аналітичних продуктів залежить від рівня підготовки працівників, які здійснюють їх розробку та застосування. Недостатній рівень аналітичної компетентності може призводити до помилок у висновках та неефективного використання отриманої інформації. У зв'язку з цим особливого

значення набуває підготовка фахівців у сфері кримінального аналізу, здатних працювати з сучасними інформаційними системами та застосовувати аналітичні методи у практичній діяльності.

Таким чином, аналітичні продукти кримінального аналізу є важливим інструментом підвищення ефективності оперативно-розшукової діяльності. Їх використання дозволяє забезпечити більш якісне планування оперативних заходів, підвищити рівень розкриття злочинів та сприяти переходу до проактивної моделі діяльності правоохоронних органів.

Список використаних джерел:

1. Марков М.М. Використання інформаційно-аналітичних можливостей у протидії злочинності. Науковий вісник Національної академії внутрішніх справ. 2018. № 4 (109) С. 305-312

2. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх 2021. 288 с.

3. Пядишев В.Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. Актуальні питання юридичної науки. 2024. № 1. Т. 2. С. 403–412.

4. Варенко, В., Кушнарьов, В.. Цифрові інструменти візуалізації інформації в аналітичній діяльності. Український журнал з бібліотекознавства та інформаційних наук, (2025) № 15, С. 10–22

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОГНОЗУВАННІ ТА ПОПЕРЕДЖЕННІ ЗЛОЧИННОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

Іллящук Денис Георгійович
кандидат юридичних наук, доцент кафедри кримінально-правових дисциплін, Одеського державного університету внутрішніх справ

Сучасний етап розвитку суспільства характеризується стрімким поширенням цифрових технологій, які істотно впливають на всі сфери суспільного життя, зокрема й на криміногенну ситуацію. Цифрова трансформація сприяє появі нових форм злочинної діяльності, розширенню можливостей для вчинення кіберзлочинів, використанню злочинцями анонімних комунікаційних

платформ, криптовалют та засобів штучного інтелекту. У таких умовах традиційні підходи до виявлення та розслідування кримінальних правопорушень потребують суттєвого вдосконалення. Одним із найбільш перспективних інструментів забезпечення ефективної правоохоронної діяльності стає кримінальний аналіз, який дозволяє здійснювати системне дослідження криміногенної обстановки, виявляти закономірності злочинної поведінки та формувати обґрунтовані прогнози щодо розвитку злочинності.

Цифровізація правоохоронної діяльності створює нові можливості для накопичення, обробки та аналізу значних масивів інформації. Використання сучасних інформаційно-аналітичних систем дає змогу інтегрувати дані з різних джерел, встановлювати приховані взаємозв'язки між подіями, особами та об'єктами, а також оперативно реагувати на зміни криміногенної ситуації. Як зазначається в сучасних наукових дослідженнях, цифрова трансформація правоохоронних органів є важливою передумовою підвищення ефективності боротьби зі злочинністю, проте водночас потребує належного нормативно-правового забезпечення, розвитку цифрових компетентностей персоналу та впровадження сучасних механізмів інформаційної безпеки [1].

Особливого значення кримінальний аналіз набуває у сфері прогнозування злочинності. Прогностична функція кримінального аналізу полягає у виявленні тенденцій розвитку кримінальних явищ на основі статистичних даних, результатів моніторингу оперативної обстановки та використання математичних моделей. Сучасні методи аналізу даних, зокрема технології машинного навчання, дозволяють визначати закономірності злочинної активності, прогнозувати можливі місця та час вчинення кримінальних правопорушень, а також оцінювати ризики виникнення нових загроз. Використання таких підходів сприяє переходу від реагування на вже вчинені злочини до їхнього попередження шляхом своєчасного виявлення криміногенних факторів.

Важливою складовою кримінального аналізу в умовах цифрової трансформації є робота з цифровими доказами та інформацією, що формується в електронному середовищі. Розвиток цифрових технологій призводить до постійного зростання обсягів електронних даних, які можуть містити відомості про підготовку, вчинення або приховування злочинів. У зв'язку з цим

підвищується значення аналітичних інструментів, здатних здійснювати автоматизовану обробку великих масивів даних, виявляти підозрілі закономірності та підтримувати прийняття управлінських рішень. Водночас поширення технологій штучного інтелекту та автоматизованих систем аналізу інформації актуалізує питання забезпечення законності, прозорості та захисту прав людини під час використання таких інструментів [1].

Кримінальний аналіз виступає важливим елементом сучасної системи попередження злочинності. Його результати можуть використовуватися для планування профілактичних заходів, оптимального розподілу сил і засобів правоохоронних органів, визначення пріоритетних напрямів оперативно-службової діяльності та формування державної політики у сфері безпеки. Умови цифрової трансформації суспільства зумовлюють необхідність подальшого розвитку аналітичних підходів, інтеграції сучасних інформаційних технологій та впровадження інноваційних методів прогнозування кримінальних ризиків.

Таким чином, кримінальний аналіз є одним із ключових інструментів забезпечення ефективної протидії злочинності в умовах цифрової трансформації суспільства. Його використання сприяє підвищенню обґрунтованості управлінських рішень, розвитку прогностичних можливостей правоохоронних органів та зміцненню системи запобігання кримінальним правопорушенням. Подальше вдосконалення методології кримінального аналізу, розширення можливостей використання цифрових технологій та забезпечення належного правового регулювання цих процесів є необхідними умовами підвищення ефективності правоохоронної діяльності в Україні.

Список використаних джерел:

1. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання // Вісник Кримінологічної асоціації України. 2026. Т. 32, № 2. С. 945–958. DOI: 10.32631/vca.2024.2.74.

ОРГАНІЗАЦІЙНІ АСПЕКТИ СТВОРЕННЯ СПЕЦІАЛІЗОВАНИХ АНАЛІТИЧНИХ ПІДРОЗДІЛІВ У СТРУКТУРІ ПРАВООХОРОННИХ ОРГАНІВ

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету внутрішніх справ

Сучасний розвиток злочинності, її організований, транснаціональний та технологічно ускладнений характер зумовлює необхідність модернізації системи правоохоронної діяльності. Традиційні форми реагування на кримінальні правопорушення дедалі частіше виявляються недостатньо ефективними в умовах швидкої зміни криміногенної ситуації, збільшення обсягів інформації та використання злочинцями новітніх цифрових технологій. У зв'язку з цим особливої актуальності набуває створення спеціалізованих аналітичних підрозділів у структурі правоохоронних органів, діяльність яких спрямована на інформаційно-аналітичне забезпечення прийняття управлінських і процесуальних рішень.

Організаційна складова застосування кримінального аналізу має визначальне значення, оскільки навіть найсучасніші аналітичні методики не можуть бути результативними без належної структури управління, кадрового потенціалу, технологічного забезпечення та координації між суб'єктами правоохоронної діяльності.

Значний внесок у розвиток теоретичних засад зробили вітчизняні та зарубіжні науковці, які розглядали питання intelligence-led policing, аналітичного забезпечення розслідувань, використання великих масивів даних у правоохоронній сфері. Водночас питання саме організаційного впровадження кримінального аналізу в українських реаліях потребують подальшого комплексного дослідження.[1]

Одним із першочергових організаційних аспектів є створення спеціалізованих аналітичних підрозділів у структурі правоохоронних органів.

Спеціалізовані аналітичні підрозділи доцільно розглядати як структурні елементи правоохоронної системи, основним

призначенням яких є збір, накопичення, систематизація, обробка та інтерпретація відомостей, що мають значення для запобігання, виявлення, припинення та розслідування кримінальних правопорушень. Це надзвичайно важливо для будь-якої діяльності, адже якщо є можливість спрогнозувати перебіг тих чи інших явищ, то з'являється можливість прийняти адекватне управлінське рішення, спираючись на аналітику як прогностичну складову процесу прийняття рішення. [2] Саме тому аналітика – одна із загальних функцій управління економічними, політичними і безпековими системами, значимість якої не схильна до впливу часу і навряд чи може бути переоцінена.

Необхідність створення аналітичних підрозділів зумовлена низкою факторів. По-перше, значно зросли обсяги інформації, яка надходить до правоохоронних органів із різних джерел: оперативних обліків, реєстрів, камер відеоспостереження, відкритих джерел, повідомлень громадян, міжнародних інформаційних каналів. Без належної аналітичної обробки ці масиви даних не можуть бути повноцінно використані. По-друге, сучасна злочинність характеризується високим рівнем мобільності, конспірації та використанням фінансових і цифрових схем, що потребує застосування складних методів аналізу зв'язків, поведінкових моделей та прогнозування. По-третє, ефективне управління правоохоронними силами потребує переходу від реактивної моделі діяльності до превентивної, заснованої на випереджувальному виявленні загроз. [3]

Організаційна побудова таких підрозділів має враховувати рівень правоохоронного органу та його функціональне призначення. На центральному рівні доцільним є функціонування аналітичних центрів, що координують регіональні структури, формують методологію аналізу, здійснюють міжвідомчу взаємодію та готують загальнодержавні оцінки криміногенної ситуації. На регіональному рівні аналітичні підрозділи повинні забезпечувати аналіз локальної злочинності, специфічних ризиків території, взаємодію з органами місцевого самоврядування та координацію територіальних підрозділів.

Особливе значення має кадрове забезпечення аналітичних підрозділів. Навички інформаційно-аналітичної роботи потрібні не лише працівникам інформаційно-аналітичних підрозділів, а й усім суб'єктам ОРД, які виконують інформаційно-розшукову

функцію. [4] Працівники повинні володіти знаннями у сфері кримінології, статистики, інформаційних технологій, геоінформаційних систем, методів візуалізації даних, правового регулювання захисту інформації. Крім професійної підготовки, важливими є аналітичне мислення, уважність до деталей, здатність працювати з великими обсягами даних та формулювати практично орієнтовані висновки. У зв'язку з цим актуальним є впровадження спеціальних освітніх програм і системи постійного підвищення кваліфікації аналітичного персоналу.

Невід'ємною умовою функціонування аналітичних підрозділів є належне технічне оснащення. Йдеться про використання сучасних інформаційно-аналітичних платформ, програм для аналізу зв'язків, картографування злочинності, автоматизованої обробки статистичних показників, роботи з відкритими джерелами та цифровими доказами. Інтеграція таких систем дозволяє значно скоротити час обробки інформації та підвищити точність аналітичних висновків.

Разом із тим створення спеціалізованих аналітичних підрозділів супроводжується певними труднощами. Серед них слід виокремити недостатнє нормативно-правове врегулювання статусу аналітиків, обмежений доступ до окремих інформаційних ресурсів, нестачу кваліфікованих кадрів, відсутність єдиних стандартів аналітичної діяльності та іноді недооцінку ролі аналітичної роботи керівним складом. Подолання зазначених проблем потребує комплексного підходу та системної державної політики.

Створення спеціалізованих аналітичних підрозділів у структурі правоохоронних органів є необхідною умовою підвищення ефективності протидії злочинності в сучасних умовах. Такі підрозділи забезпечують науково обґрунтоване прийняття рішень, сприяють раціональному використанню ресурсів, підвищують рівень превенції та результативність розслідувань. Подальший розвиток аналітичного напряму має стати важливим елементом реформування правоохоронної системи України відповідно до європейських стандартів безпеки.

Отже, кримінальний аналіз є важливим елементом сучасної правоохоронної діяльності, що забезпечує науково обґрунтоване прийняття управлінських рішень, прогнозування загроз та раціональний розподіл ресурсів. Його результативність безпосередньо залежить

від належної організації роботи, яка включає створення спеціалізованих підрозділів, підготовку кваліфікованих кадрів, розвиток інформаційно-аналітичної інфраструктури, міжвідомчу взаємодію та правове регулювання. Подальше удосконалення організаційних засад застосування кримінального аналізу в Україні має стати одним із пріоритетів реформування правоохоронної системи.

Список використаних джерел:

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. Київ: «ВАІТЕ», 2024. 444 с.

2. Гончарук О.М. Основні компоненти забезпечення ефективної діяльності підрозділів кримінального аналізу Національної поліції України. Науковий вісник Ужгородського Національного Університету, 2025. С.355- 363

3. Пядишев В.Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. Актуальні питання юридичної науки. Право і суспільство № 1 / 2024. Т. 2. С. 403-412

4. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: ЛьвДУВС, 2017. 244 с.

ЩОДО ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ЯК СЦЕЦИФІЧНОГО ВИДУ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Корнієнко Максим Вікторович
доктор юридичних наук, професор,
полковник поліції, перший проректор
Одеського державного університету внутрішніх справ

Відповідно до наказу МВС України від 20.10.2017 року № 870, який затверджує Положення про автоматичну інформаційну систему оперативного призначення єдиної інформаційної системи МВС, кримінальний аналіз – це специфічний вид інформаційно-аналітичної діяльності в оперативно-розшуковій діяльності, що

спрямований на встановлення та припущення взаємозв'язків між інформацією (відомостями, даними) про злочинну діяльність та потенційно з нею пов'язаною інформацією, отриманою з інших джерел, її оцінювання, інтерпретацію та прогнозування розвитку досліджуваних подій, ситуацій і фактів з метою їх використання під час здійснення оперативно-розшукової діяльності, розроблення тактичних і стратегічних заходів з протидії злочинності [1].

Здійснення кримінального аналізу як і будь-якого іншого виду діяльності підрозділів Національної поліції України має відбуватись відповідно до норм чинного законодавства України.

Так, відповідно до ст. 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави (ст. 3 Конституції України) [2].

Закон України «Про Національну поліцію» від 02.07.2015 року № 580-VIII, який визначає правові засади організації та діяльності Національної поліції України, статус поліцейських, а також порядок проходження служби в Національній поліції України, статтею 3 закріплює те, що у своїй діяльності поліція керується Конституцією України, міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України, цим та іншими законами України, актами Президента України та постановами Верховної Ради України, прийнятими відповідно до Конституції та законів України, актами Кабінету Міністрів України, а також виданими відповідно до них актами Міністерства внутрішніх справ України, іншими нормативно-правовими актами [3].

Під час виконання своїх завдань поліція забезпечує дотримання прав і свобод людини, гарантованих Конституцією та законами України, а також міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України, і сприяє їх реалізації (ст. 7) [3].

Поліція діє виключно на підставі, у межах повноважень та у спосіб, що визначені Конституцією та законами України. Поліцейському заборонено виконувати злочинні чи явно незаконні розпорядження та накази. Накази, розпорядження та доручення вищих органів, керівників, посадових та службових осіб, службова,

політична, економічна або інша доцільність не можуть бути підставою для порушення поліцейським Конституції та законів України (ст. 8) [3].

Крім того, ст. 25 Закону України «Про Національну поліцію» визначає повноваження поліції у сфері інформаційно-аналітичного забезпечення. Зокрема, поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених законом. Поліція в рамках інформаційно-аналітичної діяльності: 1) формує реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується реєстрами та базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; 3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями тощо. Крім того, поліція може створювати власні реєстри та бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону, та інформаційно-аналітичні системи (у тому числі міжвідомчі), необхідні для виконання покладених на неї повноважень [3].

Враховуючи, що кримінальний аналіз є складовим елементом оперативно-розшуковій діяльності, то для прийняття рішення щодо його проведення необхідна наявність таких підстав (ст. 6 Закону України «Про оперативно-розшукову діяльність») [4]: наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів; запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках, а також осіб, яким надається дозвіл на перебування без супроводу в контрольованих та стерильних зонах, зонах обмеженого доступу, що охороняються, та критичних частинах таких зон аеропортів; необхідність перевірки осіб у зв'язку з призначенням на посади в розвідувальних органах України або залученням до конфіденційного співробітництва з

такими органами, доступом осіб до розвідувальної таємниці; наявність узагальнених матеріалів центрального органу виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, отриманих в установленому законом порядку, а також випадки, передбачені ст. 17 Закону України «Про розвідку» [5].

Відсутність вищеперерахованих підстав є забороною для проведення оперативно-розшукових заходів, у тому числі, й кримінального аналізу як специфічного виду інформаційно-аналітичної діяльності підрозділів Національної поліції України [4].

Дослідження та аналіз правової регламентації здійснення кримінального аналізу підрозділами Національної поліції України є необхідним та вкрай актуальним, адже діяльність органів державної влади, у тому числі, Національної поліції, яка, відповідно до Закону України «Про Національну поліцію», є центральним органом виконавчої влади, що служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, має відбуватись виключно в межах чинного законодавства України та на підставі положень, закріплених нормативно-правовими актами України.

Список використаних джерел:

1. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС : Наказ МВС України від 20.10.2017 року № 870. Дата оновлення: 15.02.2024. URL: https://zakon.rada.gov.ua/laws/show/z1433-17#Text (дата звернення: 25.04.2026).

2. Конституція України : Закон України від 28.06.1996 року № 254к/96-ВР. Дата оновлення: 01.01.2020. URL: https://zakon.rada.gov.ua/ laws/show/254% D0%BA/96-%D0%B2%D1%80#n4178 (дата звернення: 25.04.2026).

3. Про Національну поліцію : Закон України від 02.07.2015 року № 580-VIII. Дата оновлення: 12.04.2026. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 25.04.2026).

4. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 року № 2135-XII. Дата оновлення: 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 25.04.2026).

5. Про розвідку : Закон України від 17.09.2020 року № 912-IX. Дата оновлення: 15.01.2026. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 25.04.2026).

ПЕРСПЕКТИВИ ТА ВИКЛИКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Кіреєва Ольга Сергіївна
кандидат психологічних наук, доцент
доцент кафедри спеціальних дисциплін факультету правоохоронної діяльності Національної академії Державної прикордонної служби України імені Богдана Хмельницького

Динамічний розвиток інформаційних технологій, глобальна цифровізація суспільних процесів та стрімке зростання обсягів даних зумовлюють необхідність трансформації підходів до кримінального аналізу. У цьому контексті технології штучного інтелекту постають не лише як допоміжний інструмент, а як стратегічний ресурс, здатний істотно підвищити ефективність оперативно-розшукової діяльності, у тому числі підрозділів Державної прикордонної служби України. В умовах воєнного стану, транскордонної злочинності та гібридних загроз значення інтелектуальних аналітичних систем для прикордонної безпеки суттєво зростає [1].

Аналітичний потенціал штучного інтелекту полягає у здатності алгоритмів машинного навчання здійснювати обробку, класифікацію та інтерпретацію великих масивів неструктурованої інформації (Big Data) у режимі, близькому до реального часу [2]. Для аналітичних підрозділів Державної прикордонної служби України це означає можливість інтеграції даних з різних джерел: баз перетину кордону, відеоспостереження, оперативної інформації та відкритих джерел. На відміну від традиційних методів аналізу, такі системи здатні виявляти складні нелінійні зв'язки, приховані закономірності та ризикові профілі осіб або транспортних потоків. Це відкриває можливості для побудови прогностичних моделей, зокрема щодо незаконної міграції, контрабанди та діяльності диверсійних груп.

Технологічний аспект інтеграції штучного інтелекту охоплює широкий спектр інструментів: системи комп'ютерного зору для розпізнавання об'єктів і осіб на пунктах пропуску, алгоритми обробки природної мови (NLP) для аналізу повідомлень у мережі, а також рішення у сфері предиктивної аналітики. Для Державної прикордонної служби України особливого значення набувають автоматизовані системи аналізу ризиків, які активно впроваджуються в країнах ЄС (наприклад, у діяльності Frontex). Поєднання можливостей штучного інтелекту з технологіями відкритої розвідки (OSINT) дозволяє ефективно виявляти та документувати транскордонні злочини, включаючи торгівлю людьми, незаконне переміщення зброї та кіберзлочини [2]. Автоматизація збору та первинної обробки інформації з відкритих джерел значно підвищує швидкість реагування прикордонних підрозділів.

Разом із тим, впровадження технологій штучного інтелекту супроводжується низкою суттєвих правових і етичних викликів. Передусім це стосується визначення процесуального статусу аналітичних висновків, сформованих із використанням алгоритмів, та можливості їх використання як доказів у кримінальному провадженні. Для Державної прикордонної служби України це питання є критично важливим у контексті документування правопорушень на державному кордоні [3].

Відповідно до підходів Європейського Союзу, зокрема положень Акту про штучний інтелект (EU AI Act), необхідно забезпечити баланс між безпекою та дотриманням прав людини, включаючи захист персональних даних та недискримінаційність алгоритмів[4]. Також актуальною є імплементація принципів «пояснюваного штучного інтелекту» (Explainable AI), що дозволяє забезпечити прозорість рішень, прийнятих автоматизованими системами.

Організаційний вимір впровадження штучного інтелекту нерозривно пов'язаний із підготовкою кадрів для аналітичних підрозділів Державної прикордонної служби України. Сучасні офіцери-аналітики повинні володіти компетентностями у сфері обробки даних, цифрової аналітики та роботи з інтелектуальними системами. Відповідно до рекомендацій міжнародних організацій, таких як Europol та INTERPOL, ключовим є розвиток міжвідомчої взаємодії, обміну даними та стандартизації аналітичних процесів [5]. Освітні програми мають бути адаптовані до

сучасних викликів та включати практичні кейси використання штучного інтелекту аналітиками у прикордонній сфері.

Окремим викликом є постійна еволюція інструментів, які використовують правопорушники, зокрема у сфері кіберзлочинності та транскордонних правопорушень. Використання даркнету, шифрованих каналів зв'язку та технологій анонімізації потребує від прикордонних підрозділів постійного вдосконалення аналітичних інструментів і впровадження сучасних технологій штучного інтелекту [2].

Підсумовуючи, слід зазначити, що ефективне впровадження технологій штучного інтелекту у кримінальний аналіз у системі Державної прикордонної служби України можливе лише за умови комплексного підходу, який поєднує технологічні інновації, міжнародні стандарти, нормативно-правове забезпечення та системну підготовку персоналу. Такий підхід відповідає сучасним європейським практикам і створює передумови для формування ефективної системи прикордонної безпеки України.

Список використаних джерел:

1. Купрієнко Д. А., Кіреєва О. С. Використання можливостей OSINT і штучного інтелекту для забезпечення стабілізаційних заходів прикордонного загону на деокупованій території прикордонних районів України. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України* : матеріали міжвідом. наук.-практ. конф. (Київ, 1 листоп. 2024 р.). Київ, 2024. С. 115-117.

2. Когут Ю. І. Штучний інтелект і безпека : практичний посібник / за ред. А. С. Довгополого. Київ : Консалтингова компанія «СІДКОН» ; ВД «Дакор», 2024. 294 с.

3. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах ДПСУ / О. С. Кіреєва, Ю.В. Крутік, О. М. Махлай, А. С. Треус. Хмельницький : Вид-во НАДПСУ, 2022. 360 с.

4. AI Act enters into force. Directorate-General for Communication. URL: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.

5. Коваленко Р. С., Кисельов А. О. Сучасні можливості технології OSINT у кримінальному аналізі в умовах воєнного стану. *Міжнародна та національна безпека: теоретичні і прикладні*

аспекти : матеріали VIII Міжнар. наук.-практ. конф. (м. Дніпро, 15 бер. 2024 р.). Дніпро : ДДУВС, 2024. Ч. ІІ. С. 85-87.

КОНЦЕПТУАЛЬНІ ЗАСАДИ УПРОВАДЖЕННЯ МЕТОДОЛОГІЇ ІОСТА-Україна

Користін Олександр Євгенійович
доктор юридичних наук, професор,
заслужений діяч науки і техніки України
Департамент кіберполіції НПУ
Інститут дослідження кібервійни

Розробка методології «ІОСТА Україна» є стратегічно важливим кроком для забезпечення національної безпеки, що зумовлений комплексом безпекових, правових та інтеграційних чинників. Актуальність цієї роботи насамперед полягає у необхідності переходу від реактивної моделі протидії до проактивного стратегічного аналізу, адже в умовах гібридної війни та постійної еволюції кіберзагроз здатність держави передбачати вектори атак, а не лише фіксувати їхні наслідки, стає визначальним фактором національної стійкості у кіберпросторі.

У сучасному ландшафті кіберзлочинність перестала бути виключно технічною загрозою, а, насамперед, масштабним чинником соціальної дестабілізації. Організована злочинність в Інтернеті безпосередньо загрожує правам, гідності та фінансовій безпеці кожного громадянина. Методологія «ІОСТА Україна» забезпечує системний моніторинг загроз, що спрямовані проти вразливих категорій населення, дозволяючи державі своєчасно впроваджувати превентивні механізми захисту. Це дозволяє мінімізувати «гуманітарні наслідки» кіберзлочинності, що є критично важливим для збереження суспільної довіри до державних інституцій.

В умовах кібервійни кіберзлочинні мережі часто використовуються як «проксі-актори» для проведення деструктивних операцій, що мають на меті не лише викрадення коштів, а й підрив функціонування держави. Стійкість суспільства залежить від здатності держави виявляти та нейтралізувати ці мережі на етапі їхнього формування, запобігаючи використанню кіберзлочинності як

інструменту гібридної агресії. Методологія створює умови для консолідації зусиль усього державного апарату, перетворюючи розрізнені дані в єдину систему «інтелектуального щита», що гарантує захист прав людини та національних інтересів у кіберпросторі.

Впровадження методології Європолу IOCTA забезпечує єдність аналітичного підходу з європейськими правоохоронними структурами, створюючи спільну мову для міжнародної взаємодії, що є невід'ємною складовою євроінтеграційних процесів та адаптації українського законодавства до стандартів ЄС.

Проте пряме запозичення іноземних інструментів без належної адаптації є неефективним, тому методологія «IOCTA Україна» вимагає критичного врахування українських правових реалій, соціокультурних особливостей та специфіки безпекових наслідків воєнного стану. Реалізація такого підходу мінімізує суб'єктивізм в управлінських рішеннях, оскільки завдяки використанню верифікованих даних, комплексного аналізу ризиків та експертної валідації керівництво отримує обґрунтовану базу для стратегічного спрямування зусиль протидії кіберзлочинності.

Впровадження «IOCTA Україна» – це не лише зміна аналітичного інструментарію, а інституційний перехід до нової якості безпеки, де кожна виявлена загроза, кожен знешкоджений «енейблер» – це крок до зміцнення загальної стійкості українського суспільства перед обличчям глобальних цифрових викликів, що дозволяє формувати обґрунтовану державну політику та зміцнювати загальну кіберстійкість держави в умовах високої невизначеності.

Сучасний стан кіберзлочинності характеризується безпрецедентним рівнем професіоналізації та технологічної адаптивності злочинних угруповань. Аналіз звітів IOCTA (включаючи видання 2026 року) демонструє еволюцію кіберзагроз, де використання наскрізного шифрування, мереж проксі-серверів та генеративного штучного інтелекту стає фундаментом для безмежного масштабування злочинної діяльності. Модель «Кіберзлочинність як послуга» трансформувалася у високотехнологічні екосистеми, де злочинці успішно приховують свою інфраструктуру від технічного моніторингу. Кіберзлочинці дедалі частіше використовують методи соціальної інженерії, основні тренди охоплюють автоматизоване створення високоякісного фішингового контенту за

допомогою LLM, використання нейромереж для створення Deepfake-маніпуляцій та складні схеми обходу фінансового моніторингу через децентралізовані криптоактиви, що робить традиційні системи верифікації особистості вразливими.

На тлі такої еволюції перед правоохоронними органами постають критичні завдання, що вимагають негайного перегляду операційних стратегій. Ключовим вектором діяльності стає перехід до випереджувального аналізу, який базується на таких пріоритетах:

- *технологічна інтероперабельність та аналітика*: посилення здатності правоохоронних органів працювати з великими масивами даних, інтегруючи інструменти блокчейн-форензики, автоматизованого аналізу загроз у реальному часі та дешифрування інфраструктурних потоків;
- *стратегічна нейтралізація «енейблерів»*: системне виявлення та руйнування технічної інфраструктури, що живить злочинність – зокрема хостинг-провайдерів, які ігнорують зловживання, та проксі-сервісів, що забезпечують анонімність зловмисників;
- *міжнародна інтероперабельність*: в умовах транскордонного характеру кіберзлочинів та складності приховування (шифрування), оперативний обмін даними з Європолом/Інтерполом та CERT-EU стає не просто бажаним, а обов'язковим та критично важливим для ідентифікації спільних патернів атак;
- *комплексна превенція та захист ланцюгів постачання*: комплексна превенція реалізується через спільні зусилля державного та приватного секторів, спрямовані на захист автоматизованих ланцюгів постачання програмного забезпечення та підвищення цифрової грамотності населення як фундаментальних бар'єрів для реалізації злочинних схем.

Фактично, сучасні завдання правоохоронних органів полягають у подоланні технологічного розриву між державою та злочинним світом, який ще більше поглибився через розповсюдження доступного ШІ. Ефективність протидії сьогодні вимірюється здатністю інституцій швидко адаптувати свої методи під динамічну зміну тактик зловмисників, які активно використовують шифрування та автоматизацію. Інтеграція ризик-орієнтованого підходу в щоденну роботу правоохоронних та регуляторних органів України дозволить забезпечити перехід до науково обґрунтованої моделі безпеки, здатної мінімізувати вплив кіберзлочинності на суспільство та

національну безпеку в кіберпросторі, загалом, в умовах цифровізації, що постійно трансформується.

Аналіз регламентних документів Ради Європейського Союзу, зокрема «SOCTA Customer Requirements» (12267/15), свідчить про системну трансформацію методології оцінки загроз організованої злочинності, яка була імплементована у звіті SOCTA 2017 року. Цей етап ознаменував перехід від суто описового аналізу кримінальної ситуації до повноцінного ризик-орієнтованого інструментарію, що відповідає сучасним вимогам до правоохоронної діяльності. Це стало ключовим чинником переорієнтації всієї європейської правоохоронної архітектури на предиктивну оцінку ризиків. Оскільки SOCTA визначає загальну стратегічну рамку протидії організованій злочинності, вона задає параметри, за якими здійснюється вимірювання ризиків: від аналізу суб'єктів та їхніх ресурсів до оцінки наслідків для безпекового середовища ЄС.

Зміна методологічного підходу ґрунтувалася на деталізації функціональних вимог до аналітичного продукту, де головним завданням стала не лише фіксація фактів злочинності, а прогнозування ризиків через оцінку вразливостей та спроможностей злочинних мереж. Визначення «Customer Requirements» для циклу SOCTA 2017 року дозволило синхронізувати зусилля держав-членів ЄС та Європолу, забезпечивши єдиний стандарт збору даних. Це дозволило правоохоронним органам чіткіше диференціювати загрози за рівнем їхнього впливу на безпекове середовище ЄС, перетворюючи розрізнену інформацію на структуровану базу для прийняття стратегічних рішень.

Фактично, поліпшення методології 2017 року закріпило принцип інтеграції розвідувальних даних у ризиковий профіль кожного злочинного сегмента. Упроваджений підхід надав змогу оцінювати злочинність не як набір ізольованих інцидентів, а як динамічну систему, де ризик визначається взаємодією між суб'єктами злочину, використовуваними ними інструментами («енейблерами») та слабкими місцями в системі захисту. Така переорієнтація на оцінку ризиків стала фундаментом для подальшої спеціалізації аналітичних звітів, забезпечивши високий рівень предиктивності, що є критично важливим для актуалізації оперативного фокусу органів правопорядку.

Взаємозв'язок між SOCTA та IOCTA відображає ієрархічну інтеграцію загальнокримінологічного аналізу та галузевої кібер-експертизи. SOCTA виступає фундаментом, що забезпечує стратегічне бачення стану організованої злочинності в Європейському Союзі, ідентифікуючи ключові злочинні структури та їхній вплив на безпеку. Своєю чергою, IOCTA є продуктом галузевої спеціалізації, що деталізує кіберпросторову складову загроз, виявлених у межах SOCTA, перетворюючи загальний кримінологічний зріз на глибокий технічний аналіз.

Реалізація такого галузевого підходу дозволяє правоохоронним органам долати розрив між класичними методами розслідування та динамічним розвитком цифрових злочинних технологій. Використання IOCTA забезпечує фокусування на специфічних «енейблерах» кіберзлочинності, таких як криптографічна анонімізація, мережева інфраструктура та автоматизовані інструменти впливу, які в загальному аналізі SOCTA можуть залишатися на другому плані через свою технологічну складність. Таким чином, IOCTA поглиблює методологію SOCTA, адаптуючи параметри оцінки ймовірності та наслідків до специфіки віртуального середовища, де фізичні кордони втрачають значення, а швидкість вчинення злочинів зростає експоненціально.

Фактично, галузева спеціалізація через IOCTA дозволяє правоохоронним органам не лише фіксувати прояви злочинності, а й оцінювати стійкість цифрових екосистем до атак, що є критично важливим для превентивного ризик-менеджменту. Взаємодоповнюваність цих інструментів створює єдину аналітичну систему, де SOCTA задає стратегічний контекст, а IOCTA надає необхідний технічний та операційний інструментарій для оцінювання ризиків у кіберсфері. Такий інтегрований підхід забезпечує відповідність національних стратегій безпеки сучасним стандартам європейської правоохоронної архітектури, уможливлюючи ефективну протидію викликам, що постійно трансформуються.

Аналіз звітів Europol IOCTA за період 2016–2026 років дозволяє зробити висновок про використання оцінки ризиків як базового методологічного інструментарію. Цей підхід передбачає чітку ідентифікацію, глибокий аналіз та пріоритезацію загроз на основі інтеграції розвідувальних даних, отриманих від держав-членів ЄС, приватного сектору та міжнародних партнерів.

Звіти IOCTA не є виключно статистичними збірниками; вони являють собою результати комплексного аналізу, де кожна ключова сфера – від атак на інформаційні системи до фінансового шахрайства та сексуальної експлуатації дітей – оцінюється крізь призму масштабу, суспільного впливу та операційних спроможностей злочинних угруповань. Методологія звітів демонструє еволюцію від описового підходу до глибокої предиктивної аналітики, де ризик-орієнтований підхід дозволяє виокремлювати ключові чинники («енейблери»): анонімізація, використання криптоактивів, розвиток тіньової інфраструктури, а також технологічні «мультиплікатори» загроз: генеративний штучний інтелект, наскрізне шифрування та багаторівневі мережі проксі-серверів, що кардинально розширюють можливості злочинних екосистем, дозволяючи їм ефективно приховувати свою інфраструктуру та автоматизувати злочинні процеси.

Фактичний стан використання оцінки ризиків у межах IOCTA свідчить про її функцію як фундаментальної парадигми для стратегічного управління безпекою. Виявлені ризики безпосередньо впливають на визначення пріоритетів правоохоронної діяльності в межах циклу EMPACT, забезпечуючи прийняття обґрунтованих рішень на рівні керівництва. Застосування канонічної моделі оцінки, що поєднує ймовірність реалізації загрози та тяжкість її наслідків, створює умови для порівняння рівнів загроз у часі та просторі.

Впровадження ризик-орієнтованого підходу в методологію «IOCTA Україна» знаменує фундаментальний перехід від реактивної фіксації інцидентів до предиктивного управління національною системою кібербезпеки. В основі цієї моделі лежить встановлення чіткого функціонального зв'язку між потенційними загрозами, вразливістю інфраструктури та реальною спроможністю системи до ефективної відповіді. Такий підхід дозволяє замість безсистемної протидії всім викликам одночасно зосередити обмежені інтелектуальні та фінансові ресурси держави на найбільш критичних зонах, де ймовірність атак та масштаби їхніх наслідків становлять найвищу загрозу для національних інтересів.

Завдяки динамічному прогнозуванню та сценарному моделюванню методологія отримує спроможність не лише ідентифікувати поточні аномалії, а й випереджати розвиток кіберзлочинності, виходячи з глибокого розуміння нових технологічних

викликів. Більше того, цей підхід дає змогу об'єктивно виміряти ефективність міжвідомчої координації та виявити системні прогалини в захисті ланцюгів постачання, які часто стають критичними точками входу для організованих злочинних угруповань.

Фактично, ризик-орієнтована модель перетворює «ІОСТА Україна» на дієвий інструмент стратегічного менеджменту, де будь-які управлінські рішення – від модернізації технічного інструментарію до оптимізації регуляторної бази – ґрунтуються на доведеній аналітичним шляхом необхідності мінімізації конкретних високих ризиків. У підсумку це забезпечує цілісну превенцію та зміцнює загальну кіберстійкість держави, формуючи прозорий і зрозумілий алгоритм дій для захисту суспільства в умовах перманентної кібервійни.

ОБМЕЖЕННЯ ІНФОРМАЦІЙНИХ ПРАВ І СВОБОД ЛЮДИНИ В УМОВАХ ВОЄННОГО СТАНУ

Кухтюк Юлія Віталіївна
курсант 202 взводу навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної поліції
Національної поліції України
*Науковий керівник**: Собко Ганна Миколаївна***
доктор юридичних наук, професор,
професор кафедри кримінального права та кримінології
Одеського державного університету внутрішніх справ

Проблематика обмеження прав і свобод людини посідає центральне місце в сучасній юридичній науці та практиці публічного адміністрування, оскільки безпосередньо впливає на рівень демократичності та правової зрілості суспільства. Конституція України проголошує людину, її життя і здоров'я, честь і гідність, недоторканність та безпеку найвищою соціальною цінністю, а діяльність держави спрямована на утвердження та забезпечення прав і свобод. Водночас право не є абсолютним у своїй природі, адже в умовах загроз національній безпеці, громадському порядку чи здоров'ю населення постає необхідність юридично обґрунтованого їх обмеження, що є загальновизнаної світової практикою, передбаченою

міжнародними правовими актами — насамперед Конвенцією про захист прав людини і основоположних свобод.

Актуальність дослідження зумовлена сучасними трансформаціями, які переживає Українська держава в умовах воєнного стану, масштабних викликів безпеці та необхідності оперативного реагування на загрози терористичного, інформаційного та військового характеру. У таких умовах забезпечення балансу між захистом прав людини та інтересами держави набуває особливо важливого значення. Від правомірності, пропорційності та обґрунтованості обмежень залежить рівень довіри суспільства до державної влади, стабільність правопорядку та ефективність реалізації демократичних цінностей у правовій системі України.

У сучасних умовах тема обмеження прав і свобод людини потребує всебічного вивчення крізь призму безпекових викликів, трансформації державної політики та потреби дотримання принципу верховенства права. Наукове осмислення механізмів обмеження прав у період воєнного та повоєнного відновлення має ключове значення для формування ефективної моделі правового захисту особи й одночасно гарантування стабільності державної системи. Як справедливо зазначає О. С. Лотюк, повоєнний період може супроводжуватися низкою кризових явищ, що створюють загрозу національній безпеці та можуть обумовлювати необхідність тимчасового збереження конституційних обмежень прав і свобод громадян, але лише за умови їх відповідності міжнародним стандартам, пропорційності та обмеженості у часі [1, с.13].

Особливої уваги потребує питання недопущення використання обмежень у політичних цілях або як засобу тиску на громадянське суспільство та інститути демократії. Виважене застосування правових інструментів має передбачати чіткі гарантії проти зловживань, контроль з боку парламенту, судову перевірку правомірності рішень та прозорість процедур впровадження обмежень. У цьому контексті повоєнна модель відновлення суспільства і держави повинна базуватися на розумінні, що конституційні права і свободи залишаються фундаментом демократичного розвитку, а будь-які обмеження мають бути винятковими та юридично обґрунтованими.

У контексті поглибленого аналізу обмеження прав і свобод людини в умовах війни важливо підкреслити, що правомірність

таких обмежень не може оцінюватися виключно з позиції доцільності чи державної необхідності. Не менш значущим є їх відповідність стандартам демократичного суспільства та дотримання балансу між інтересами державної безпеки і невід'ємними правами людини. Адже навіть у найскладніших умовах воєнного протистояння держава зобов'язана залишатися правовою та орієнтувати свою політику на захист людської гідності, недопущення свавілля і зловживань владою. Як наголошує М. М. Коба, ефективність та прийнятність обмежувальних заходів безпосередньо залежить від їх законності, пропорційності і тимчасового характеру, а недотримання цих вимог здатне спричинити суспільне несприйняття й утрату довіри до інститутів влади [2, с. 13].

На нашу думку, воєнний стан та об'єктивні потреби оборони держави не повинні слугувати підставою для довготривалого розширення владних повноважень та трансформації держави в авторитарну. Після завершення воєнних дій украй важливо забезпечити поступове повернення до повноцінного функціонування конституційного механізму захисту прав людини, відновлення демократичних інститутів та посилення контролю громадянського суспільства. Лише за таких умов обмеження, застосовані під час війни, будуть сприйматися як необхідні та правомірні, а не як засоби політичного контролю чи маніпуляції.

У науковій літературі зазначається, що запровадження правового режиму воєнного стану об'єктивно зумовлює необхідність тимчасового обмеження окремих прав і свобод громадян, що пов'язано з потребою забезпечення оборони держави, громадської безпеки та стабільності функціонування органів публічної влади. Дослідники підкреслюють, що такі обмеження повинні ґрунтуватися на принципах законності, пропорційності, необхідності та мінімального втручання, тобто застосовуватися лише у випадках, коли іншими засобами неможливо досягти захисту національних інтересів і безпеки. Тимчасовий характер обмежень, їх чітка нормативна регламентація та наявність механізмів правового контролю розглядаються як ключові гарантії недопущення зловживання владними повноваженнями [3, с.17].

OSINT (Open Source Intelligence) у контексті обмеження прав і свобод людини виступає як сучасний інструмент збору, аналізу та використання інформації з відкритих джерел (соціальні мережі,

медіа, реєстри, супутникові знімки тощо) з метою забезпечення національної безпеки, протидії злочинності та документування правопорушень. Застосування OSINT в умовах воєнного стану дозволяє державним органам, зокрема правоохоронним, оперативно отримувати значущу інформацію без втручання у приватне життя особи в традиційному розумінні, що частково мінімізує необхідність жорстких обмежень прав. Водночас використання відкритих даних може створювати ризики непрямого втручання у право на приватність, особливо у випадках масового моніторингу або профайлінгу осіб. У зв'язку з цим застосування OSINT має ґрунтуватися на принципах законності, пропорційності та цільового використання інформації, а також супроводжуватися належним правовим регулюванням і контролем, щоб уникнути зловживань та забезпечити баланс між інтересами державної безпеки і правами людини.

Важливою передумовою ефективності обмеження прав і свобод людини в умовах воєнного стану є чітка формалізація меж втручання держави у приватну сферу особи та постійний інституційний контроль за дотриманням принципу пропорційності. Обмеження не повинні перетворюватися на інструмент управлінського тиску чи механізм легітимізації надмірної централізації влади. Значущим залишається забезпечення прозорості прийняття рішень, регулярна звітність суб'єктів владних повноважень та залучення інститутів громадянського суспільства до моніторингу запроваджених обмежень. Тільки за умов зваженого нормативного регулювання та ефективного демократичного контролю обмеження прав і свобод можуть відповідати принципам правової держави.

Системний аналіз обмежень прав і свобод людини в умовах воєнного стану демонструє, що їх запровадження є правомірним лише за суворого дотримання міжнародних і конституційних стандартів. Обмеження мають бути чітко окресленими, тимчасовими та обґрунтованими реальною потребою захисту держави та суспільства. Рекомендовано удосконалити механізми парламентського і судового контролю, запровадити відкриті механізми звітування органів влади щодо прийнятих рішень, а також посилити роль громадянського суспільства у моніторингу правозастосування. Важливо забезпечити післявоєнний етап поступової деконцентрації обмежень і повернення до повного обсягу конституційних прав як показника демократичної стійкості держави.

Список використаних джерел:

1. Лотюк О.С. Конституційні засади обмеження прав та свобод людини і громадянина у повоєнний період. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 2. С. 9-15.
2. Коба М.М. Обмеження прав і свобод людини в умовах війни: загальнотеоретичний аналіз. *Juris Europensis Scientia*. 2024. Вип. 4. С.8-14.
3. Кубаєнко А., Крижановська О., Курганський О. Сучасні практики поліцейської діяльності: навчально-методичний посібник. Нац. ун-т «Одеська юридична академія». Одеса: Юридична література, 2024. 144 с.
4. Главацька А. О., Ангельська О. В., Опірський І. Р. Дослідження технології використання OSINT // Матеріали науково-практичної конференції. 2024.

ДЕЯКІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Савенко Дмитро Олександрович
старший інспектор 5-го відділу 3-го управління
Департаменту кіберполіції Національної поліції України
Ісмайлов Карен Юрійович
кандидат юридичних наук, доцент,
начальник 5-го відділу 3-го управління
Департаменту кіберполіції Національної поліції України

Актуальність дослідження визначається тим, що на сьогоднішній день першочерговим обов'язком держави, особливо в умовах воєнного стану, залишається забезпечення безпеки її громадян. Спектр загроз національній безпеці стає все більш складним та різноманітним. Тероризм, кібератаки, нетрадиційні атаки із застосуванням хімічної, ядерної або біологічної зброї, а також масштабні аварії або природні катаклізми - будь-що може поставити під загрозу безпеку громадян, завдавши серйозної шкоди інтересам та економічному добробуту країни [1, с. 21]. В умовах стрімкого розвитку інформаційних технологій виникла принципово нова категорія загроз:

дезінформаційні кампанії, розповсюдження фейкових новин та інформаційно-психологічні операції (ІПСО).

Метою дослідження є аналіз технічних можливостей сучасних OSINT-інструментів на основі штучного інтелекту в контексті виявлення фейкових новин та протидії дезінформаційним кампаніям, а також визначення особливостей їх практичного застосування в умовах гібридної війни в контексті російсько-українського збройного конфлікту.

Особливої гостроти ця проблематика набуває після початку повномасштабного вторгнення росії у 2022 році, де країна-агресор системно використовує інформаційно-психологічні операції як повноцінний інструмент ведення гібридної війни, що застосовується паралельно з традиційними бойовими діями. Основною метою таких операцій є дестабілізація внутрішньополітичної ситуації в Україні, психологічний тиск на населення та провокування соціальних конфліктів.

За таких умов дослідження технічних засобів виявлення та нейтралізації дезінформаційних загроз, зокрема OSINT-інструментів на основі штучного інтелекту, набуває не лише наукового, а й практичного значення для забезпечення інформаційної безпеки держави.

Основні загрози, які несуть інформаційно-психологічні операції в умовах воєнного конфлікту: розпалення конфлікту та поглиблення напруження, маніпуляція суспільною думкою, розповсюдження дезінформації, підрив моралі та деморалізація військових та населення, психологічний тиск та зміна стратегій ведення війни, посилення стереотипів та ворожнечі, порушення міжнародного співтовариства [2, с. 9].

З початку XXI століття в умовах технологічного прогресу Інтернет давно вже міцно увійшов у життя людей, а для деяких осіб – це єдиний спосіб самовираження та пошуку друзів або заработка. Завдяки створенню Інтернету, кожна людина може приєднатися до величезних і практично невичерпних джерел інформації [3, с. 132]. Саме тому розвідка з відкритих джерел грає дуже важливу роль в сучасному світі.

Роль OSINT в кібербезпеці є комплексною. Для приватної особи OSINT – це спосіб побачити себе очима зовнішнього світу, а також для захисту особистої ідентичності в Інтернеті [4, с. 49]. Для держави - це механізм, який одночасно виступає як інструмент для збору розвідувальної інформації, так і для протидії вище

зазначеним діям з боку іншого суб'єкту (країна-агресор, тощо), особливо в контексті поширення дезінформації, фейків та ІПСО.

За умов стрімкого розвитку інформаційних технологій розвідка з відкритих джерел залишається одним із найбільш перспективних та багатосторонніх інструментів у сфері кібербезпеки. Інформація отримана за допомогою розвідки з відкритих джерелах може одночасно використовуватись як інструмент протидії загрозам національній безпеці України, так і як інструмент для їх розповсюдження, наприклад: розповсюдження інформації про об'єкти критичної інфраструктури, військові об'єкти та інші чутливі підприємства [5, с. 169]. В контексті поширення фейкових новин та дезінформації OSINT-інструменти також можуть використовуватися як з метою розповсюдження такої інформації, так і для протидії проти неї.

Як було зазначено раніше, особливу загрозу національній безпеці становить розповсюдження дезінформації (системна, цілеспрямована діяльність із поширення хибних або маніпулятивних відомостей з метою досягнення конкретного політичного, військового чи соціального ефекту) та фейків (конкретна одиниця неправдивого контенту: сфабрикована новина, підроблене зображення, вирване з контексту відео, тощо), що в свою чергу може сприяти зміні соціальних настроїв та спонуканню населення країни до певних діянь. Тобто, збір відкритої інформації, включно з аналізом соціальних мереж, супутникових знімків, повідомлень у ЗМІ та даних із різних онлайн-ресурсів, є важливим елементом боротьби проти дезінформації [6, с. 283].

У світі, де відкриті джерела інформації є основними джерелами комунікації, використання OSINT технологій для збору даних створює не лише можливості, але й серйозні загрози [7, с. 242]. Саме тому слід приділити особливу увагу взаємодії OSINT з технологіями штучного інтелекту (ШІ) у боротьбі з дезінформацією. Сучасні рішення на основі ШІ, такі як автоматизовані системи перевірки фактів, виявлення контенту типу «deepfake» на основі нейронних мереж та алгоритми кластеризації скоординованих інформаційних кампаній, значно посилюють аналітичний потенціал OSINT [8, с. 111]. Інтеграція розвідки з відкритих джерел та машинного навчання створює нову парадигму боротьби з гібридними інформаційними загрозами, що у свою чергу вимагає відповідної правової кодифікації у національному законодавстві та міжнародних угодах, які стосуються кіберпростору.

Станом на сьогодні існує достатньо велика кількість ШІ-інструментів, які доцільно використовувати під час перевірки новин та протидії дезінформації як працівникам державних структур, так і приватним підприємствам:

Назва	**Технічні можливості OSINT-інструменту**
Hive AI	Детектор згенерованого ШІ-контенту (зображення, текст, відео). Використовує ансамблі CNN, класифікує ймовірність AI-генерації у відсотках. API-доступ, пакетна обробка. Окремі моделі для DALL-E, Midjourney, Stable Diffusion.
Decopy AI	Реверсний пошук зображень + детектор AI-генерації. Пошук за візуальним fingerprint-ом через перцептивний хешинг. Виявляє часткові копії та маніпуляції (обрізка, накладення фільтрів).
TinEye	Реверсний пошук зображень на базі власного індексу (60+ млрд зображень). Використовує image fingerprinting, а не метадані. Відстежує хронологію появи зображення в мережі — дозволяє знайти оригінальне джерело.
InVID-WeVerify	Браузерний плагін для верифікації відео та зображень. Розбиває відео на keyframe-и, запускає реверсний пошук по кожному. Аналізує метадані, геолокацію, контекст публікації. Інтегровано з YouTube Data API.
Deepware scanner	Спеціалізований детектор deepfake-відео. Аналізує артефакти на рівні облич (blending boundaries, temporal inconsistencies). На вході — URL або файл, на виході — score ймовірності маніпуляції.
AI voice detector	Бінарний (score-based) класифікатор синтезованої мови. Аналізує спектральні характеристики, просодику, артефакти TTS-моделей. Деякі версії розрізняють конкретні TTS-движки.
Let`s Data	No-code платформа для збору та аналізу публічних даних (соцмережі, веб). Парсинг без API, побудова датасетів, базова аналітика + інтеграція з BI-інструментами. Орієнтована на OSINT-журналістику.
Pangram	Детектор AI-тексту з фокусом на провенанс контенту. Використовує watermarking-сигнали та статистичний аналіз розподілу токенів. Позиціонується для медіа та академічного середовища.

Таб. Порівняння технічних можливостей OSINT інструментів на основі ШІ

одночас, формування належного інформаційно-безпекового середовища для здійснення OSINT-діяльності супроводжується низкою суттєвих організаційно-технічних та правових проблем. Водночас відсутність уніфікованих стандартів і методичних рекомендацій щодо побудови подібної інфраструктури призводить до фрагментарності підходів та підвищує ризики інформаційної безпеки [9, с. 156].

Таким чином, проведений аналіз дозволяє сформулювати наступні висновки: по-перше, розвідка з відкритих джерел в поєднанні з інструментами штучного інтелекту сформувала якісно новий рівень верифікації інформації: автоматизовані детектори (Hive AI, Deepware Scanner, AI Voice Detector) дозволяють виявляти згенерований або маніпульований контент у режимі реального часу, що раніше вимагало значних людських ресурсів та часових витрат.

По-друге, повномасштабне вторгнення росії в лютому 2022 року стало каталізатором масштабного впровадження OSINT-інструментів: їх використання вийшло за межі академічного та журналістського середовища та поширилося на рівень державних структур та збройних сил. Це підтверджує, що OSINT-інструментарій перестав бути допоміжним і набув статусу самостійного елемента системи національної безпеки.

По-третє, жоден з розглянутих інструментів не є універсальним: кожен із них орієнтований на конкретну модальність контенту (текст, зображення, відео, аудіо), що обумовлює необхідність їх комплексного використання в рамках єдиної верифікаційної методології.

По-четверте, чинне законодавство України не містить спеціальних норм, що регулюють застосування OSINT-інструментів на основі ШІ у сфері протидії дезінформації, що створює правову невизначеність щодо допустимості зібраних доказів та відповідальності суб'єктів розвідувальної діяльності. Усунення цієї прогалини є необхідною умовою для інституціоналізації OSINT-практик на державному рівні.

Список використаних джерел:

1. Користін О.Є., Демедюк С.В. OSINT Open Source Intelligence. Теорія та методологія : монографія. Київ : 7БЦ, 2025. 304 с.

2. Ісмайлов К.Ю. Роль інформаційно-психологічних операцій в сьогоденні: проблематика, виклики та заходи захисту.

Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика: матеріали Міжнародної науково-практичної конференції (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. С. 8-10.

3. Ісмайлов К.Ю. Інтернет як сучасний фактор розповсюдження дискримінаційних виявів. *Порівняльно-аналітичне право.* 2017. № 3. С. 131-133.

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

5. Івкова В.С., Опірський І.Р. OSINT-технології як загроза кібербезпеці держави. *КІБЕРБЕЗПЕКА: освіта, наука, техніка*. 2025. Т. 3, № 27. С. 165-179.

6. Величко Т.О. Протидія російській інформаційній агресії за допомогою OSINT. *Оперативно-бойова діяльність сил сектору безпеки і оборони в умовах воєнного стану* : Матеріали Всеукр. науково-практ. конф. представників сектору безпеки і оборони України, наук. та науково-пед. працівників, здобувачів освіти та інших зацікавл. осіб, м. Київ, 24 жовтня 2024 р. Київ, 2024. С. 283-284.

7. Савенко Д.О., Ісмайлов К.Ю. OSINT та соціальні мережі: загрози та можливості для молодіжних комунікацій. *«Sociological and psychological models of youth communication»*: VII Міжнародна науково-практична конференція, Copenhagen, 18-21 February 2025. С. 242-246.

8. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.

9. Ісмайлов К.Ю. Деякі особливості нормативного регулювання діяльності правоохоронців у мережі інтернет в Україні. *Актуальні питання діяльності Національної поліції як суб'єкту протидії організованій злочинності* : матеріали Всеукраїнської науково-практичної конференції (м. Кропивницький, 02 квітня 2026 року). Кропивницький, 2026. С. 154-157.

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ АНАЛІТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Скупінська Олена Вадимівна
аспірант кафедри адміністративно-правових дисциплін,
Одеський державний університет внутрішніх справ

Сучасний етап розвитку правоохоронної діяльності характеризується активним впровадженням аналітичних інформаційних систем, які забезпечують збір, обробку, аналіз та візуалізацію значних масивів даних з метою підтримки управлінських рішень і підвищення ефективності протидії злочинності. Використання таких систем дозволяє здійснювати кримінальний аналіз, прогнозування криміногенних процесів, виявлення взаємозв'язків між подіями та особами, а також своєчасне реагування на загрози громадській безпеці. У зв'язку з цим особливого значення набуває належне правове регулювання використання аналітичних інформаційних систем у діяльності правоохоронних органів України, що має забезпечувати баланс між потребами безпеки держави та дотриманням прав і свобод людини [1].

Правові засади функціонування аналітичних інформаційних систем формуються комплексом нормативно-правових актів, серед яких важливе місце займають Конституція України, Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про Національну поліцію», а також підзаконні нормативні акти, що регламентують порядок створення та використання інформаційно-комунікаційних ресурсів у секторі безпеки та оборони. Нормативне регулювання повинно забезпечувати законність отримання, обробки та зберігання інформації, визначати повноваження суб'єктів доступу до інформаційних ресурсів і встановлювати механізми контролю за використанням інформації в правоохоронній діяльності [2].

Особливу актуальність питання правового регулювання набуває в умовах цифрової трансформації правоохоронної системи та інтеграції сучасних технологій штучного інтелекту до аналітичних платформ. Сучасні інформаційні системи здатні автоматизувати процеси аналізу великих даних, формувати прогностичні моделі та виявляти приховані закономірності у кримінальних подіях. Водночас застосування алгоритмів автоматизованого

аналізу породжує низку правових викликів, пов'язаних із забезпеченням прозорості прийняття рішень, недопущенням дискримінації, захистом персональних даних та визначенням відповідальності за помилки алгоритмів. Тому законодавче забезпечення використання таких технологій має враховувати не лише технічні аспекти їх функціонування, але й вимоги щодо дотримання фундаментальних прав людини [2].

Важливим напрямом удосконалення правового регулювання є визначення єдиних стандартів інформаційної безпеки для аналітичних систем правоохоронних органів. Зростання кількості кібератак на державні інформаційні ресурси потребує створення ефективних механізмів захисту інформації, що обробляється в аналітичних системах. Відповідно до сучасних наукових підходів інформаційно-аналітичне забезпечення правоохоронної діяльності повинно базуватися на принципах конфіденційності, цілісності та доступності даних, а також передбачати застосування комплексних організаційно-правових заходів щодо захисту інформаційних ресурсів [1].

Перспективи розвитку правового регулювання використання аналітичних інформаційних систем у діяльності правоохоронних органів України пов'язані з гармонізацією національного законодавства з європейськими стандартами у сфері захисту персональних даних та цифрового врядування. У контексті євроінтеграційних процесів особливого значення набуває впровадження принципів підзвітності, прозорості та контролю за діяльністю інформаційних систем, що використовуються для прийняття управлінських та процесуальних рішень. Належне нормативне забезпечення використання аналітичних технологій сприятиме підвищенню ефективності правоохоронної діяльності, зміцненню довіри суспільства до правоохоронних органів та забезпеченню належного рівня захисту прав людини в умовах цифровізації суспільних відносин.

Список використаних джерел:

1. Демчук Т. І. Інформаційно-аналітичні та організаційні методи правоохоронної діяльності. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2025. Вип. 90. Ч. 5. С. 430–436. DOI: 10.24144/2307-3322.2025.90.5.57.

2. Мациборська О. М. Проблеми впровадження в діяльність правоохоронних органів інформаційних систем на базі штучного інтелекту. *Аналітично-порівняльне правознавство.* 2026. № 1. С. 92–97. DOI: 10.24144/2788-6018.2026.01.3.14.

СЕКЦІЯ 4.
OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ

ВИЯВЛЕННЯ ТА ДОКУМЕНТУВАННЯ КІБЕРЗЛОЧИНІВ ІЗ ВИКОРИСТАННЯМ КРИПТОВАЛЮТ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Барба Вячеслав Євгенович
доктор філософії, викладач кафедри
адміністративно-правових дисциплін,
Одеський державний університет внутрішніх справ

Стрімкий розвиток цифрових технологій та поширення криптовалют зумовили появу нових форм злочинної діяльності у кіберпросторі. Віртуальні активи дедалі частіше використовуються як інструмент вчинення кримінальних правопорушень, пов'язаних із шахрайством, вимаганням, відмиванням доходів, отриманих злочинним шляхом, незаконним обігом товарів і послуг у дарknеті, а також фінансуванням інших протиправних дій. Особливістю таких злочинів є поєднання традиційних кримінальних механізмів із сучасними цифровими технологіями, що значно ускладнює процес їх виявлення, документування та доказування. Науковці відзначають, що поширення віртуальних активів трансформувало характер сучасної злочинності та створило нові виклики для правоохоронних органів щодо організації ефективного розслідування кримінальних правопорушень [1].

Однією з головних проблем виявлення кіберзлочинів із використанням криптовалют є високий рівень анонімності або псевдонімності транзакцій. Хоча більшість операцій у блокчейн-мережах є публічними, встановлення реальної особи, яка контролює криптовалютний гаманець, потребує застосування спеціальних аналітичних інструментів та комплексних слідчих заходів. Злочинці активно використовують сервіси мікшування транзакцій, децентралізовані фінансові платформи, а також криптовалюти з підвищеним рівнем конфіденційності, що ускладнює процес

простеження руху коштів. У результаті виникають суттєві труднощі з ідентифікацією суб'єктів злочинної діяльності та встановленням причинно-наслідкового зв'язку між цифровими активами й конкретними кримінальними правопорушеннями [1].

Важливе значення у протидії таким правопорушенням має належне документування цифрових доказів. Криптовалютні транзакції залишають цифрові сліди у блокчейні, які можуть використовуватися як джерело доказової інформації під час кримінального провадження. Однак специфіка цифрових доказів потребує дотримання особливих процедур їх фіксації, збереження та процесуального оформлення. Втрата цілісності даних, помилки під час вилучення цифрової інформації або недотримання процесуальних вимог можуть поставити під сумнів допустимість таких доказів у суді. У сучасних дослідженнях наголошується, що ефективне документування кіберзлочинів повинно базуватися на використанні криміналістичних методів виявлення та фіксації цифрових слідів, які забезпечують належний рівень достовірності та доказової сили отриманої інформації [2].

Складність документування злочинів із використанням криптовалют також обумовлена їх транснаціональним характером. Учасники протиправної діяльності можуть перебувати в різних країнах, використовувати іноземні криптовалютні біржі та сервіси, а зберігання цифрових даних нерідко здійснюється на серверах, розташованих за межами юрисдикції держави, яка проводить розслідування. За таких умов особливого значення набуває міжнародне співробітництво правоохоронних органів, гармонізація законодавства у сфері віртуальних активів та вдосконалення механізмів обміну інформацією між компетентними органами різних держав. Відсутність уніфікованих підходів до правового регулювання криптовалют ускладнює як процес розслідування, так і подальше притягнення винних осіб до відповідальності [1].

Перспективним напрямом підвищення ефективності виявлення кіберзлочинів є використання спеціалізованих систем блокчейн-аналітики та інтелектуальних технологій обробки даних. Сучасні програмні засоби дозволяють здійснювати автоматизований аналіз великих масивів транзакційної інформації, виявляти підозрілі фінансові операції, встановлювати зв'язки між криптовалютними адресами та формувати аналітичні моделі злочинної

активності. Дослідники зазначають, що впровадження технологій штучного інтелекту та методів інтелектуального аналізу даних значно розширює можливості виявлення фінансових злочинів у цифровому середовищі та сприяє підвищенню результативності правоохоронної діяльності [1].

Не менш важливим напрямом розвитку є вдосконалення нормативно-правового забезпечення діяльності правоохоронних органів у сфері розслідування злочинів, пов'язаних із використанням криптовалют. Формування єдиних методичних рекомендацій щодо роботи з цифровими доказами, підготовка фахівців з блокчейн-аналітики та запровадження сучасних криміналістичних методик сприятимуть підвищенню якості документування таких правопорушень. Водночас необхідним є подальше наукове дослідження механізмів використання віртуальних активів у злочинній діяльності та розроблення ефективних моделей їх криміналістичного аналізу.

Отже, використання криптовалют у злочинній діяльності створює нові виклики для системи кримінальної юстиції та правоохоронних органів. Анонімність транзакцій, транснаціональний характер злочинів і складність роботи з цифровими доказами потребують комплексного підходу до їх виявлення та документування. Подальший розвиток блокчейн-аналітики, удосконалення криміналістичних методик, розширення міжнародного співробітництва та адаптація законодавства до сучасних цифрових реалій становлять основні перспективні напрями підвищення ефективності протидії кіберзлочинам із використанням криптовалют.

Список використаних джерел

1. Саєнко В. В. Аналіз стану наукового дослідження проблем розслідування кримінальних правопорушень, пов'язаних з використанням віртуальних активів // Аналітично-порівняльне правознавство. – 2025. – № 4. – С. 280–294. – DOI: 10.24144/2788-6018.2025.04.3.41.

2. Крижановський А. С., Кравець В. С. Про криміналістичні методи виявлення та фіксації цифрових слідів від кіберзлочинів // Науковий вісник Ужгородського національного університету. Серія: Право. – 2026. – Вип. 93. – С. 84–90. – DOI: 10.24144/2307-3322.2026.93.5.13.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ДЖЕРЕЛО ДОКАЗОВОЇ ІНФОРМАЦІЇ ПРИ ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ OSINT

Болгар Олег Васильович
доктор юридичних наук, доцент, професор кафедри адміністративно-правових дисциплін
Одеського державного університету внутрішніх справ.

Повномасштабна збройна агресія Російської Федерації проти України зумовила суттєве зростання ролі цифрових технологій у процесі документування воєнних злочинів. Соціальні мережі стали не лише засобом комунікації та поширення інформації, а й важливим джерелом доказових даних для правоохоронних органів, міжнародних слідчих місій, правозахисних організацій та незалежних дослідників. Щоденно користувачі публікують фото-, відео- та текстові матеріали, які можуть містити відомості про обставини вчинення воєнних злочинів, місце події, час її здійснення, причетних осіб та наслідки протиправних дій. У цих умовах особливого значення набувають методи відкритої розвідки (OSINT), що дозволяють здійснювати пошук, збір, перевірку та аналіз інформації з відкритих джерел для подальшого використання у процесі документування міжнародних злочинів [1].

Соціальні мережі Facebook, X (Twitter), Instagram, TikTok, Telegram та YouTube сьогодні формують значний масив цифрових даних, які можуть бути використані як потенційні джерела доказової інформації. Завдяки наявності метаданих, геолокаційних ознак, візуальних орієнтирів та часових маркерів дослідники мають можливість встановлювати місце та час подій, ідентифікувати учасників конфлікту, а також відтворювати хронологію окремих епізодів воєнних злочинів. Практика документування подій у Бучі, Маріуполі, Краматорську та інших населених пунктах України засвідчила, що матеріали із соціальних мереж нерідко стають важливим джерелом відомостей для подальшого проведення слідчих дій та міжнародних розслідувань. Дослідники відзначають, що саме поєднання журналістських розслідувань, правозахисної діяльності та OSINT-технологій сформувало нову модель документування воєнних злочинів у цифровому середовищі [2].

Однією з головних переваг OSINT є можливість оперативного отримання інформації без безпосереднього доступу до місця події. У багатьох випадках проведення традиційних слідчих дій у районах активних бойових дій є неможливим або пов'язане зі значними ризиками для життя та здоров'я слідчих, експертів і свідків. За таких умов відкриті джерела інформації дозволяють отримувати первинні відомості про потенційні порушення міжнародного гуманітарного права та здійснювати їх попередню перевірку. Важливим є також те, що цифрові матеріали можуть бути збережені та проаналізовані незалежно від часу їх створення, що розширює можливості ретроспективного дослідження подій та встановлення нових фактів у вже відкритих кримінальних провадженнях [1].

Водночас використання соціальних мереж як джерела доказової інформації супроводжується низкою суттєвих обмежень. Насамперед це стосується проблеми достовірності цифрового контенту. Поширення дезінформації, використання маніпулятивних матеріалів, монтаж відеозаписів, застосування технологій штучного інтелекту для створення deepfake-контенту та навмисне викривлення фактів істотно ускладнюють процес перевірки інформації. У зв'язку з цим матеріали із соціальних мереж не можуть автоматично розглядатися як достовірні докази без проведення процедури верифікації. Ефективне застосування OSINT передбачає використання методів геолокації, хронолокації, аналізу метаданих, порівняння інформації з різних незалежних джерел та перевірки цифрових слідів на предмет їх автентичності [2].

Ще одним суттєвим обмеженням є питання процесуальної допустимості інформації, отриманої з відкритих джерел. Для використання таких матеріалів у кримінальному провадженні необхідно забезпечити належну фіксацію джерела походження інформації, збереження її цілісності та дотримання вимог кримінального процесуального законодавства щодо збору й оформлення доказів. Особливу складність становить швидкоплинний характер цифрового контенту, оскільки повідомлення можуть бути видалені користувачами, обмежені для перегляду або змінені після їх первинної публікації. Саме тому важливого значення набуває створення спеціалізованих цифрових архівів та систем довготривалого збереження електронних доказів [1].

Перспективним напрямом розвитку OSINT є інтеграція технологій штучного інтелекту та автоматизованого аналізу великих масивів даних. Використання сучасних алгоритмів дозволяє швидко виявляти релевантний контент серед мільйонів публікацій, здійснювати класифікацію матеріалів, встановлювати взаємозв'язки між окремими подіями та формувати аналітичні моделі для підтримки розслідувань. Поряд із цим важливим завданням залишається розроблення єдиних міжнародних стандартів використання відкритих джерел інформації під час документування воєнних злочинів та забезпечення їх належної доказової сили в національних і міжнародних судових інстанціях [2].

Отже, соціальні мережі стали одним із найважливіших джерел доказової інформації у процесі документування воєнних злочинів в умовах сучасних збройних конфліктів. Застосування OSINT-технологій відкриває широкі можливості для збору, аналізу та верифікації цифрових даних, однак ефективність їх використання значною мірою залежить від забезпечення достовірності інформації, дотримання процесуальних вимог та впровадження сучасних технологічних рішень. Подальший розвиток методології OSINT та вдосконалення механізмів роботи з цифровими доказами сприятимуть підвищенню ефективності документування воєнних злочинів і забезпеченню невідворотності відповідальності винних осіб.

Список використаних джерел:

1. Костюченко О. О., Шевцов А. В. Використання відкритих джерел інформації (OSINT) при розслідуванні злочинів проти людяності. Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. 2025. № 2(130). С. 46–51. DOI: 10.17721/1728-2195/2025/2.130-7.

2. Мірошниченко С. В. OSINT як поле конвергенції журналістики та правозахисної діяльності: досвід документування воєнних злочинів в Україні // Наукові записки Інституту журналістики. 2026. Т. 88, № 1. С. 89–101. DOI: 10.17721/2522-1272.2026.88.7.

РОЛЬ OSINT У ЗАБЕЗПЕЧЕННІ ПУБЛІЧНОЇ БЕЗПЕКИ І ПОРЯДКУ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Волошанівська Тетяна Володимирівна
доктор юридичних наук, доцент, доцент кафедри кримінально-правових дисциплін
Одеського державного університету внутрішніх справ.

Відповідно до Закону України «Про Національну поліцію України» від 02.07.2015 року № 580-VIII, Національна поліція України (поліція) – це центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку (ст. 1) [1].

Завданнями поліції є (ст. 2):

1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства і держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [1].

Поняття публічної безпеки і порядку у чинному законодавстві України відсутні, проте Закон України «Про національну безпеку України» від 21.06.2018 року № 2469-VIII закріплює визначення таких понять, як: національна безпека, державна безпека, а також громадська безпека і порядок [2].

Національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

Державна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру;

Громадська безпека і порядок – захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і

громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз [2].

Аналізуючи визначення громадської безпеки і порядку, можна стверджувати, що поняття публічної безпеки і порядку більшою мірою є тотожним із визначенням громадської безпеки і порядку.

Слід зазначити, що у виконанні завдань поліції, зокрема, забезпеченні публічної безпеки і порядку, поліцейським підрозділам нашої держави допомагає розвідка на основі відкритих джерел або OSINT.

Ключові напрями застосування OSINT для забезпечення публічної безпеки і порядку є [3, с. 431-437; 4, с. 282-284]:

- моніторинг масових заходів і протестів: аналіз публікацій, хештегів та геоміток у соціальних мережах допомагає прогнозувати кількість учасників мітингів, оцінювати радикалізацію настроїв та виявляти координаторів потенційних безладів;

- запобігання загрозам і кримінальним правопорушенням: своєчасний збір даних дозволяє виявляти приховані суспільно-небезпечні процеси, діяльність радикальних угруповань та підготовку до порушень громадського порядку;

- ідентифікація правопорушників: використання інструментів розпізнавання облич, аналіз фото- та відеоматеріалів з відкритих джерел дають змогу встановлювати особи зловмисників, які вчинили хуліганство чи інші кримінальні правопорушення проти громадського порядку чи моральності;

- протидія дезінформації та паніці: моніторинг інфопростору допомагає виявляти ворожі ІПСО (інформаційно-психологічні операції), фейки та чутки, які штучно дестабілізують ситуацію серед цивільного населення;

- оцінка інфраструктурних ризиків: збір даних про надзвичайні ситуації, руйнування чи аварії через повідомлення очевидців допомагає поліції та екстреним службам швидше скерувати сили туди, де безпека громадян під загрозою.

Список використаних джерел:

1. Про Національну поліцію : Закон України від 02.07.2015 року № 580-VIII. Дата оновлення: 12.04.2026. URL:

https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 28.04.2026).

2. Про національну безпеку України : Закон України від 21.06.2018 року № 2469-VIII. Дата оновлення: 24.01.2026. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 28.04.2026).

3. Рибка Д. OSINT у забезпеченні національної безпеки. *Науковий вісник Ужгородського національного університету*. Серія ПРАВО. 2025. Вип. 91: Ч. 4. С. 431-437. DOI https://doi.org/10.24144/2307-3322.2025.91.4.59

4. Мірошніченко І. О., Ланде Д. В. Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів. *Системи та технології кібернетичної безпеки* : матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. С. 282-284.

OSINT-ТЕХНОЛОГИЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ

Домніцак Володимир Володимирович
Завідувач науково-дослідної лабораторії з актуальних питань кримінального аналізу, кандидат юридичних наук, доцент

Повномасштабна збройна агресія Російської Федерації проти України зумовила необхідність активного використання сучасних цифрових технологій для фіксації та документування воєнних злочинів. У сучасних умовах особливого значення набувають OSINT-технології (Open Source Intelligence), тобто методи збору та аналізу інформації з відкритих джерел. Використання відкритих даних дозволяє правоохоронним органам, міжнародним організаціям, журналістам та громадським ініціативам оперативно отримувати інформацію про факти порушення міжнародного гуманітарного права.

OSINT-технології сьогодні активно застосовуються для документування обстрілів цивільної інфраструктури, встановлення місця та часу вчинення воєнних злочинів, ідентифікації

військових підрозділів та окремих осіб, причетних до злочинної діяльності. Значення відкритої розвідки суттєво зросло у зв'язку з розвитком цифрових платформ, соціальних мереж, супутникових систем та онлайн-сервісів.

Використання OSINT дозволяє не лише швидко збирати інформацію, але й формувати доказову базу для міжнародних судових інституцій, зокрема Міжнародного кримінального суду. У зв'язку з цим дослідження теоретичних та практичних аспектів застосування OSINT-технологій у документуванні воєнних злочинів є актуальним напрямом сучасної юридичної науки.

Поняття та сутність OSINT-технологій

Термін OSINT (Open Source Intelligence) означає отримання та аналітичну обробку інформації з відкритих джерел [1, с. 45]. До таких джерел належать соціальні мережі, електронні засоби масової інформації, супутникові знімки, відкриті бази даних, геолокаційні сервіси, відеохостинги, форуми та інші інтернет-ресурси.

У сучасному світі OSINT став важливим інструментом діяльності правоохоронних органів, спеціальних служб, військової розвідки та журналістських розслідувань. Особливістю відкритої розвідки є те, що інформація збирається виключно з легальних та доступних джерел без використання спеціальних негласних методів.

Науковці зазначають, що OSINT є ефективним засобом інформаційно-аналітичного забезпечення безпеки держави, оскільки дозволяє швидко реагувати на кризові ситуації та виявляти загрози [2, с. 117]. Крім того, відкриті джерела часто містять значний обсяг даних, які можуть бути використані як допоміжні докази під час кримінальних проваджень.

Основними етапами OSINT-дослідження є:

- збір інформації;
- перевірка достовірності даних;
- аналіз отриманої інформації;
- встановлення взаємозв'язків;
- формування аналітичних висновків.

У практичній діяльності використовуються різні інструменти OSINT-аналізу. Найбільш поширеними є системи геолокації, аналізу метаданих, моніторингу соціальних мереж та супутникового спостереження. Такі інструменти дозволяють встановлювати

місце зйомки відео чи фотографії, визначати час події, ідентифікувати осіб та транспортні засоби.

Особливого значення OSINT набув після початку широкомасштабної війни в Україні, коли відкриті джерела стали одним із головних інструментів документування злочинів проти цивільного населення.

Нормативно-правове забезпечення документування воєнних злочинів

Документування воєнних злочинів здійснюється на основі норм міжнародного гуманітарного права та національного законодавства України. Основними міжнародними актами у цій сфері є Женевські конвенції 1949 року, Додаткові протоколи до них, Римський статут Міжнародного кримінального суду та інші міжнародно-правові документи.

Відповідно до Римського статуту Міжнародного кримінального суду воєнними злочинами визнаються серйозні порушення законів та звичаїв війни, що спричиняють тяжкі наслідки для цивільного населення [3]. До таких злочинів належать умисні вбивства, катування, депортація цивільних осіб, обстріли цивільних об'єктів та застосування заборонених методів ведення війни.

Національне законодавство України також містить норми щодо відповідальності за воєнні злочини. Зокрема, стаття 438 Кримінального кодексу України передбачає відповідальність за порушення законів та звичаїв війни [4]. У сучасних умовах правоохоронні органи України активно здійснюють фіксацію злочинів агресії та збір доказів для подальшого міжнародного судового переслідування.

Важливу роль у процесі документування відіграють міжнародні організації та правозахисні структури. Такі організації, як ООН, Amnesty International, Human Rights Watch та Bellingcat, активно використовують OSINT-технології для підтвердження фактів воєнних злочинів.

Використання відкритих джерел потребує дотримання процесуальних вимог щодо збирання та збереження доказів. Інформація повинна бути перевірена, задокументована та належним чином збережена для подальшого використання у кримінальному провадженні.

Практичне застосування OSINT у документуванні воєнних злочинів

Практика останніх років показала високу ефективність OSINT-технологій у процесі документування злочинів, пов'язаних зі збройною агресією проти України. Одним із найбільш поширених методів є аналіз фото- та відеоматеріалів, оприлюднених у соціальних мережах.

За допомогою геолокаційного аналізу дослідники можуть встановлювати точне місце вчинення злочину шляхом порівняння об'єктів на фото із супутниковими знімками та картографічними сервісами. Це дозволяє підтверджувати факти обстрілів житлових будинків, лікарень, шкіл та інших цивільних об'єктів.

Одним із відомих прикладів використання OSINT є документування подій у Бучі, Ірпені та Маріуполі. Супутникові знімки, відеоматеріали з безпілотників та дані соціальних мереж стали важливими доказами під час міжнародних розслідувань [5, с. 74].

OSINT-технології активно використовуються також для ідентифікації військовослужбовців та військових підрозділів. Аналіз акаунтів у соціальних мережах, фотографій, нашивок, номерів техніки та відкритих баз даних дозволяє встановлювати осіб, причетних до вчинення воєнних злочинів.

Крім того, відкриті джерела допомагають відстежувати переміщення військової техніки, визначати маршрути пересування підрозділів та аналізувати масштаби руйнувань. У багатьох випадках саме OSINT стає першим джерелом інформації про вчинення міжнародних злочинів.

Важливим напрямом є використання супутникових технологій. Компанії Maxar Technologies, Planet Labs та інші надають супутникові знімки високої якості, які дозволяють фіксувати наслідки бойових дій та руйнування цивільної інфраструктури.

Разом із перевагами існують і певні ризики використання відкритих джерел. Серед основних проблем можна виділити поширення фейкової інформації, можливість маніпуляцій цифровими матеріалами та складність перевірки достовірності окремих даних. Саме тому важливим є комплексний підхід до аналізу інформації та використання декількох незалежних джерел.

Перспективи розвитку OSINT-технологій

На сучасному етапі розвитку інформаційних технологій OSINT набуває дедалі більшого значення у сфері міжнародної

безпеки та правоохоронної діяльності. Подальший розвиток відкритої розвідки буде пов'язаний із використанням штучного інтелекту, автоматизованих систем аналізу даних та технологій Big Data.

Одним із перспективних напрямів є автоматизація аналізу цифрових матеріалів. Сучасні алгоритми вже здатні автоматично розпізнавати об'єкти на фото та відео, визначати геолокацію та аналізувати великі обсяги інформації у соціальних мережах.

Важливим напрямом розвитку є міжнародне співробітництво у сфері OSINT. Україна активно взаємодіє з міжнародними організаціями, журналістськими спільнотами та аналітичними центрами для обміну інформацією та координації роботи з документування воєнних злочинів.

На мою думку, у майбутньому OSINT стане одним із ключових елементів системи міжнародного правосуддя, оскільки відкриті джерела дозволяють швидко отримувати докази та забезпечувати прозорість розслідувань.

Водночас розвиток OSINT потребує належного правового регулювання та захисту персональних даних. Використання цифрових технологій повинно здійснюватися із дотриманням прав людини та міжнародних стандартів інформаційної безпеки.

Отже, OSINT-технології сьогодні є важливим інструментом документування воєнних злочинів та забезпечення міжнародного правосуддя. Використання відкритих джерел дозволяє оперативно збирати, перевіряти та аналізувати інформацію про порушення міжнародного гуманітарного права.

Практичне застосування OSINT підтверджує його високу ефективність у процесі фіксації злочинів агресії, ідентифікації осіб та збору доказів для міжнародних судових інституцій. Особливого значення відкриті джерела набули в умовах війни в Україні.

Разом із тим, ефективне використання OSINT потребує удосконалення правового регулювання, розвитку міжнародної співпраці та підготовки фахівців у сфері цифрової аналітики. Подальший розвиток інформаційних технологій сприятиме підвищенню ролі OSINT у сфері безпеки та правоохоронної діяльності.

Список використаних джерел:

1. Білоус В. В. OSINT у діяльності правоохоронних органів України. Київ : НАВС, 2022. 214 с. URL: https://www.naiau.kiev.ua/ (дата звернення: 17.05.2026).

2. Коваленко В. В. Використання відкритих джерел інформації у правоохоронній діяльності // Науковий вісник ДДУВС. 2023. № 2. С. 115–121. URL: https://visnik.dduvs.in.ua/ (дата звернення: 17.05.2026).

3. Римський статут Міжнародного кримінального суду від 17.07.1998. URL: https://zakon.rada.gov.ua/laws /show/995_ 588#Text (дата звернення: 17.05.2026).

4. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/ laws/show/ 2341-14#Text (дата звернення: 17.05.2026).

5. Шевчук О. О. Документування воєнних злочинів за допомогою цифрових технологій // Юридичний науковий електронний журнал. 2023. № 5. С. 72–78. URL: http://lsej.org.ua/5_2023/17.pdf (дата звернення: 17.05.2026).

6. Женевські конвенції про захист жертв війни від 12.08.1949. URL: https://zakon.rada.gov.ua/laws/show/ 995_151 #Text (дата звернення: 17.05.2026).

7. Amnesty International. Digital Verification Corps. URL: https://www.amnesty.org/en/digital-verification-corps/ (дата звернення: 17.05.2026).

8. Bellingcat. Open Source Investigations. URL: https://www.bellingcat.com/ (дата звернення: 17.05.2026).

9. Human Rights Watch. Ukraine: Apparent War Crimes in Russia-Controlled Areas. URL: https://www.hrw.org/ (дата звернення: 17.05.2026).

10. NATO Open Source Intelligence Handbook. Brussels, 2021. URL: https://www.nato.int/ (дата звернення: 17.05.2026).

11. Maxar Technologies. Satellite Imagery and Crisis Monitoring. URL: https://www.maxar.com/ (дата звернення: 17.05.2026).

12. Planet Labs. Global Daily Satellite Imagery. URL: https://www.planet.com/ (дата звернення: 17.05.2026).

13. Ratcliffe J. Intelligence-Led Policing. London : Routledge, 2016. 232 p.

14. Тіщенко В. В. Інформаційно-аналітичне забезпечення правоохоронної діяльності. Харків : Право, 2021. 286 с.

15. Europol Open Source Intelligence Report. URL: https://www.europol.europa.eu/ (дата звернення: 17.05.2026).

ВИКОРИСТАННЯ OSINT У РОЗКРИТТІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПЕРЕДБАЧЕНИХ СТ. 438 КК УКРАЇНИ

Кавунська Анна Олександрівна
кандидат юридичних наук, викладач кафедри
професійних та спеціальних дисциплін
Одеського державного університету внутрішніх справ

Відповідно до ст. 438 КК України воєнними злочинами визнається жорстоке поводження з військовополоненими або цивільним населенням, вигнання цивільного населення для примусових робіт, розграбування національних цінностей на окупованій території, застосування засобів ведення війни, заборонених міжнародним правом, незаконне переміщення або депортація дитини, невиправдана затримка репатріації дитини, вербування або використання дитини для участі у збройному конфлікті, воєнних (бойових) діях, інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також віддання наказу про вчинення таких дій [1].

Виходячи з класифікації кримінальних правопорушень, наданих у ст. 12 КК України, воєнні злочини є особливо тяжкими злочинами, а отже держава має вживати усіх можливих заходів та зусиль задля їх розкриття [1].

На сьогодні чинне кримінальне процесуальне законодавство України не містить поняття «розкриття злочинів», проте таке визначення міститься у Положенні про основи організації розкриття органами внутрішніх справ України злочинів загальнокримінальної спрямованості, затвердженого наказом МВС України від 30.04.2004 року № 458 (втратив чинність 11.02.2011 року) [2]. Отже, відповідно до зазначеного нормативно-правового акта, розкриття злочинів – це визначена законодавством і нормативно-правовими актами Міністерства внутрішніх справ України комплексна діяльність оперативних підрозділів, органів дізнання, досудового слідства, інших підрозділів органів внутрішніх справ, спрямована на встановлення наявності або відсутності суспільно небезпечного винного діяння, збирання доказів вини особи, яка

його вчинила, з метою притягнення її до кримінальної відповідальності та відшкодування збитків, завданих злочинною діяльністю, а також установлення та усунення причин і умов, що сприяють вчиненню злочинів [2].

Розкриття злочинів передбачає встановлення у ході проведення оперативно-розшукових заходів і слідчих дій обставин, що підлягають доказуванню в кримінальній справі: події злочину; вини особи, яка його вчинила; мотивів злочину; фактичних даних, що впливають на ступінь і характер відповідальності, характеризують таку особу; характеру й розміру шкоди, завданої злочином; інших обставин, що мають значення для правильного вирішення кримінальної справи [2].

Допомогою правоохоронним органам у розкритті злочинів, а особливо тих, що відповідно до чинного кримінального законодавства визнаються воєнними, можуть слугувати так звані OSINT-технології.

Слід зазначити, що чинне законодавство України не містить визначення дефініції OSINT, однак наявні її ознаки серед яких варто виділити такі: діяльність (тобто активні, усвідомлені дії, що свідчить про необхідність наявності мети діяльності); мета – отримання інформації, що цікава особі; характер діяльності включає в себе збір та аналіз інформації, формування висновків на підставі аналізу; відкриті джерела або відкрита інформація – об'єкт

відповідної діяльності (при цьому варто зазначити, що відповідні джерела характеризуються різними формами від класичних друкованих ЗМІ до електронних реєстрів) [3, с. 332].

Крім того, окремі науковці в галузі дослідження інформаційно-аналітичних технологій визначають, що OSINT це: діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору [4]; діяльність по отриманню розвідувальної інформації з відкритих джерел; розвідка на основі аналізу відкритих джерел інформації [5, с. 204]; діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору; розвідка на основі аналізу відкритих джерел інформації [6, с. 333].

На основі аналізу напрямів діяльності та застосування OSINT, така технологія може бути корисною у розслідуванні воєнних злочинів тим, що за допомогою OSINT можна визначити: геолокацію місця події (точне місце, де було зроблено фото або відео); час

події; осіб, що вчинили протиправні діяння; наявну техніку тощо. Крім того, аналізуючи супутникові знімки, можна встановити хронологію подій, що є обов'язковим для визначення складових об'єктивної сторони кримінального правопорушення, передбаченого ст. 438 КК України.

Список використаних джерел:

1. Кримінальний кодекс України : Закон України від 05.04.2001 року № 2341-III. Дата оновлення: 15.04.2026. URL: https://zakon.rada.gov.ua/laws/ show/2341-14#Text (дата звернення: 26.04.2026).

2. Про затвердження Положення про основи організації розкриття органами внутрішніх справ України злочинів загальнокримінальної спрямованості : Наказ МВС України від 30.04.2004 року № 458. Втрата чинності: 11.02.2011. URL: https://zakon.rada.gov.ua/laws/show/z0814-04#Text (дата звернення: 26.04.2026).

3. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії. Юридичний науковий електронний журнал. 2024. № 9. С. 332-335. DOI https://doi.org/10.32782/2524-0374/2024-9/78

4. Білобров А. В., Клімушин П. С. Використання технологій OSINT для отримання інформації. Протидія кіберзлочинності та торгівлі людьми : збірник матеріалів Міжнародної науково-практичної конференції (м. Харків, 27 травня 2020 року). С. 135-137.

5. Яровой Т. С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. Експерт: парадигми юридичних наук і державного управління. 2019. № 4(6). С. 201-208.

6. Мартинюк С. О. Характеристика принципів функціонування OSINT у сфері національної безпеки. Юридичний науковий електронний журнал. 2021. № 9. С. 332-334.

АВТОМАТИЗАЦІЯ ЗБОРУ ТА АНАЛІЗУ OSINT-ДАНИХ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Лемешко Юрій Олександрович
начальник управління кримінального аналізу
ГУНП в Харківській області
Серватовський Андрій Володимирович
заступник начальника відділу аналітичної роботи
управління кримінального аналізу
ГУНП в Харківській області

З початку повномасштабного вторгнення рф у 2022 році Харківська область стала однією з перших, що зазнала масштабної окупації: на піку бойових дій під контролем ворога перебувало до 32% території регіону.

У вересні 2022 року Збройні Сили України розпочали масштабний контрнаступ у Харківській та інших областях, внаслідок чого було звільнено значну частину регіону, станом на кінець 2022 року — 1,6% території області перебували під окупацією.

Після відновлення контролю над населеними пунктами правоохоронні органи та міжнародні спостерігачі розпочали фіксацію наслідків окупації. Робота на звільнених територіях дозволила задокументувати численні факти порушення норм міжнародного гуманітарного права, зокрема: катівні, масові поховання, вбивства мирних жителів, викрадення та депортації дітей, мародерство та інші грубі порушення міжнародного гуманітарного права, які не мають термінів давності. Проводились масштабні огляди вищезазначених місць вчинення злочинів під час яких виявлено та вилучено значні об’єми, різного роду документів підрозділів рф, як офіційних так і простих записів окремих командирів та військових.

Виявлені документи є одним з первинним джерел інформації для встановлення осіб, причетних до вчинення воєнних злочинів. Однак фрагментарність знайдених даних та їхній колосальний обсяг створили виклик для аналітичних, оперативних та слідчих підрозділів.

Особливістю воєнних злочинів є те, що стосовно подій злочинів, як правило, існує велика (надмірна) кількість доказів, які

прямо чи опосередковано підтверджують події злочину, а також інші обставини, що підлягають доказуванню. Водночас доказів, які прямо вказують (дають змогу ідентифікувати і довести вину) на виконавців чи організаторів злочину, може бути недостатньо. Крім того, необхідно вжити заходів для збереження і збору доказів, які можуть бути у потерпілих та свідків (фото-, відеоматеріали; речові докази) [1].

Документування в умовах активних бойових дій ускладняється, оскільки фізичний доступ до місць вчинення воєнних злочинів обтяжується низкою критичних загроз для життя персоналу та ризиком втрати матеріальних доказів [2].

З метою накопичення, систематизації та цифровізації доказів виникла необхідність у створенні спільного робочого простору, інтегрованої системи, яка поєднує в собі всі матеріали в одному цифровому середовищі, для аналітичних, оперативних та слідчих підрозділів.

Рішенням даного питання стала ініціатива створення системи SORC — розробленої місцевими харківськими програмістами за запитом слідчого управління для автоматизації вже існуючих процесів.

Модульна система SORC (System of Offence Registration and Criminal Investigations, Система обліку та розслідування кримінальних правопорушень) забезпечує повний цикл роботи: первинна реєстрація - накопичення даних – ідентифікація – формування доказової бази. Потенційними можливостями SORC є цифровізація, обробка, накопичення широкого спектру доказів та подальше аналітичне опрацювання отриманих відомостей. Найголовнішою перевагою, слід зазначити можливість використання цієї інформації у кримінальному провадженні незалежно від територіальності органу провадження та матеріальних носіїв, що пришвидшує повноту та якість роботи під час досудового розслідування. До того ж, завдяки значному об’єму накопиченої інформації (та постійне наповнення) у деяких кримінальних провадженнях, SORC може стати єдиним джерелом цінної інформації для доказування, оскільки оригінали або копії матеріалів доказування можуть бути пошкодженні або знищенні взагалі.

Як раніше зазначено, виявлені на деокупованих територіях речові докази та документи за своєю більшістю мають лише фрагменти необхідних даних. Отже інформація, матеріали потребують

значного доопрацювання, шляхом проведення комплексного аналітичного дослідження з використання безпосередньо у головній ролі OSINT-джерела та інструментарій.

У розслідуваннях щодо суб'єктів, які активно приховують інформацію, цифрові витоки даних та відомості з відкритих джерел стають основним замінником державних реєстрів. Сукупність цих даних з отриманими відомостями з деокупованих територій дозволяє деанонімізувати військових країни агресора.

Традиційні методи розвідки на основі відкритих джерел (OSINT) у «ручному» режимі вже не відповідають вимогам часу, щодо швидкості та глибини аналізу, враховуючі об'єми даних, що підлягає аналітичному опрацюванню.

Фінальний аналітичний профіль являється основним підтвердженням особи злочинця для органів прокуратури в процесі доказування. Обмежені можливості повної або часткової автоматизації збору даних змушують розставляти пріоритети між справами. Хоча висновок завжди залишається за аналітиком, ефективність його роботи прямо залежить від якості попередньо структурованої інформації. Ідеальна модель передбачає, що фахівець має працювати з уже наявним масивом даних, не витрачаючи критичний час на ручний пошук у розрізнених джерелах. Автоматизація вже напрацьованих методів та алгоритмів ручного пошуку основної інформації підвищить ефективність аналізу та зменшить витрати часу, що нерідко є критичним фактором.

Аналітиками для автоматизації пошуку та збору інформації вже напротязі декількох років активно та успішно використовується український програмний продукт Artellence BigDataPeople, який безперечно є вагомим інструментом для OSINT-розвідки.

Світовий ринок наразі пропонує значну кількість готових комерційних рішень та програмних продуктів, які функціонують згідно різних алгоритмів на основі штучного інтелекту у відкритій та закритій мережі. Головною цінністю таких рішень є автоматизація процесів та доступ до вже сформованих масивів даних, зібраних із найрізноманітніших джерел. Працівники підрозділу кримінального аналізу Харківщини тестували окремі програмні продукти, які в майбутньому можуть бути використані для автоматизації повторюваних робочих процесів:

- Bold – глибокий адаптивний інтелект для національної безпеки та корпоративних організацій, для приймання рішень, пов'язаних з ризиками та можливостями [3];
- Cognyte – аналітичне програмне забезпечення об'єднує, аналізує та візуалізує різнорідні набори даних у великих масштабах, щоб допомогти організаціям знаходити деталі та перетворювати дані на корисну інформацію, на основі якої вони можуть швидко діяти [4];
- Elephantastic – платформа OSINT-аналізу, яка збирає, упорядковує та структурує різноманітні дані з публічних джерел легкодоступними для пошуку, тим самим виявляючи ключові висновки зі складних даних [5];
- ESPY – набір модульних програм корпоративного рівня для підтримки розвідки та розслідувань, які пришвидшують діяльність завдяки синергії технологій, галузевих ноу-хау та експертизи в галузі розвідки [6];
- Penlink – рішень у сфері цифрової аналітики. Програмні рішення спрощують роботу зі складними даними, надаючи можливість швидко та ефективно приймати обґрунтовані рішення [7].

Кожен із представлених програмних продуктів має свої унікальні алгоритми та власні бази даних, що дозволяють здійснювати пошук і аналіз за різними типами вхідних параметрів. Застосування цих можливостей в діяльності правоохоронних органів значно скоротило б час обробки інформації та дозволило опрацьовувати значно більші обсяги даних порівняно з традиційними методами. Слід зазначити, що вказані технології вже перебувають на варті в органах безпеки багатьох країн. Зазначені програмні рішення, являються лише малою частиною представленого ринку та технологій, які постійно розвиваються.

Підсумовуючи, слід зазначити, що розвиток технологій робить ручну обробку великих масивів даних неконкурентною. У сучасних реаліях трансформації та гібридних загроз, швидкість прийняття рішень безпосередньо залежить від автоматизації аналітичних процесів. Використання інтелектуальних програмних продуктів дозволяє не лише скоротити часові витрати, а й виявити приховані зв'язки, які залишаються непомітними при звичному підході на який впливає низка факторів.

Попри ефективність готових комерційних рішень, їх впровадження обмежене високою вартістю та необхідністю постійного ліцензування. Раціональною альтернативою є детальне вивчення можливостей вже представлених програмних продуктів з практичної та технічної частини, для подальшої розробки власних аналогів, адаптованих до специфіки діяльності Національної поліції України та МВС в цілому.

Список використаних джерел:

1. Методичні рекомендації «Стандарти розслідування воєнних злочинів. Незаконне позбавлення волі та катування» (2023).
2. Global Rights Compliance. (2023). Basic Investigative Standards for International Crimes.
3. Bold Deep Adaptive Intelligence. URL: https://www.boldintel.com/about
4. Cognyte investigative analytics software. URL: https://www.cognyte.com/
5. Elephantastic OSINT investigation platform. URL: https://elephantastic.io/
6. ESPY Web Intelligence. URL: https://espy.is/
7. Penlink AI-powered digital intelligence and investigations. URL: https://www.penlink.com/

OSINT ЯК ІНСТРУМЕНТ ФОРМУВАННЯ ДОКАЗОВОЇ БАЗИ У МІЖНАРОДНОМУ ПРАВОСУДДІ ЩОДО ВОЄННИХ ЗЛОЧИНІВ

Лук'яненко Ілона Анатоліївна
Здобувачка вищої освіти 4 курсу,
Університет митної справи та фінансів, м. Дніпро
Науковий керівник: ***Батраченко Тетяна Сергіївна,*** *к.ю.н.,*
завідувач кафедри правоохоронної діяльності
Університет митної справи та фінансів, м. Дніпро

У сучасних умовах розвитку інформаційного суспільства відкриті джерела даних перетворилися на один із ключових ресурсів отримання інформації для правоохоронних органів. Використання OSINT (далі - Open Source Intelligence) у досудовому

розслідуванні зумовлене його доступністю, оперативністю та здатністю забезпечувати доказову базу без використання джерел інформації з обмеженим доступом. Саме тому аналіз відкритих джерел перетворився на невід'ємну складову досудового розслідування у межах кримінального провадження, дозволяючи встановлювати факти, ідентифікувати осіб та документувати події з високим рівнем достовірності.

Тривалий збройний конфлікт між російською федерацією та Україною, а також подальше повномасштабне вторгнення 24 лютого 2022 року істотно змінили мету використання OSINT-аналізу. Якщо раніше в Україні він застосовувався переважно для оперативного моніторингу та збору інформації, то від початку повномасштабної агресії його використання стало пріоритетним задля досягнення цілей доведення порушень міжнародного гуманітарного права з боку держави-агресора та формування доказової бази для притягнення винних у рамках міжнародного правосуддя.

Відтак, одним із важливих орієнтуючих документів, які визначають необхідні стандарти для знаходження, збирання, зберігання, перевірки та аналізу інформації із соціальних мереж та відкритих джерел, є Протокол Берклі. У пункті 8 цього протоколу зазначається, що інформація у відкритому доступі корисна для всіх розслідувань, але особливу роль вона відіграє у міжнародних кримінальних розслідуваннях та розслідуваннях у сфері порушення прав людини [1]. В продовження зазначеного, професорка Івон МакДермотт Різ, у рамках дискусії «InternationalLawTalks», ще у 2020 році наголосила на існуванні двох категорій інформації з відкритих джерел у розслідуванні міжнародних злочинів, а саме: перша - це контент, створений користувачами, зокрема матеріали, що виникають безпосередньо в умовах збройного конфлікту: відеозаписи, зроблені на мобільні телефони та поширені у соціальних мережах. Друга категорія - супутникові знімки, які забезпечують незалежну візуалізацію подій та територій, що часто недоступні для традиційних методів збору доказів [2].

Одним із найбільш резонансних прикладів підтвердження жорстокого поводження з українськими військовополоненими стало поширене у квітні 2023 року відео, на якому зафіксовано відрізання голови українському полоненому російським військовослужбовцем. Виходячи з деталей опублікованої інформації, вбачається, що одним

із перших це відео розмістив у своєму закритому телеграм-каналі лідер російської екстремістської організації «Мужское государство» Владислав Поздняков [3]. Зазначений випадок є показовим прикладом грубого порушення країною-агресором норм Женевських конвенцій та додаткових протоколів до них. Такі дії становлять серйозне порушення міжнародного гуманітарного права й мають важливе значення для оцінки подальших кроків світової спільноти у сфері притягнення винних до відповідальності та забезпечення належного захисту прав військовополонених.

Також, існує практика коли українські OSINT-експерти, здійснюючи всеосяжний моніторинг відкритої інформації, змогли встановити місце проживання російських військовослужбовців, їхнє походження, навчальні заклади та місця роботи, а також інші важливі відомості про осіб, причетних до вчинення воєнних злочинів. У низці випадків ідентифікація здійснювалася навіть за фотографіями, що зберігалися у мобільних телефонах, які російські військові залишили, терміново покидаючи з м. Буча [4, с. 816].

Але попри всі переваги використання OSINT, існує думка щодо негативного аспекту використання інформації з відкритих джерел що проявляється у значній кількісті дезінформації. Збирання, перевірка та оцінка цифрових даних, що можуть містити докази воєнних злочинів, вчинених під час збройної агресії проти України, становлять складний процес, який, як зазначають Тома М. Г. та Василова О. В., нагадує «лабіринт», з якого необхідно знайти вихід. Такі виклики охоплюють технічні, етичні та правові аспекти й потребують різноманітних стратегій для їх ефективного вирішення. Значний масив цифрового контенту, що створюється під час війни в Україні - відеоспостереження, фотографії, публікації у соціальних мережах - формує нові труднощі для його фіксації та належного збору. Забезпечення автентичності та збереження таких даних у хаотичних умовах неоголошеної війни є надскладним і водночас архіважливим завданням сьогодення. Відрізнити справжні докази від шахрайського чи фальшивого контенту стає дедалі складніше [5, с. 906].

У цьому контексті канадська філософиня Реджина Ріні стверджує, що «найважливішим ризиком є не те, що повірять у діпфейки, а те, що дуже тямущі споживачі інформації рефлексивно не довірятимуть усім матеріалам за визначенням» [2].

Варто звернути увагу, що одним із важливих пунктів Протоколу Берклі, який стосується допустимості використання інформації, здобутої за допомогою OSINT-аналізу, є пункт D (правила та процедури доказування). Згідно з ним епоха вільного розповсюдження цифрової інформації супроводжується ризиком появи неправдивих даних та дезінформації. У такому випадку надзвичайно важливо, щоб слідчі мали змогу визначити, чи є інформація у відкритому доступі достовірною, а також встановити або спростувати її автентичність із достатньою точністю [1].

Тобто інформація, отримана методом OSINT, може бути релевантним доказом, лише у тому якщо вона підтверджує ймовірність вчинення злочину та її доказова сила допомагає довести або спростувати певні факти, про які йдеться у відповідній справі.

Наприклад, у раніше згаданому випадку жорстокого поводження з військовополоненим українцем OSINT слугував інструментом ідентифікації постраждалої особи як українського військового через демонстрацію бронежилета на відео, де було видно шеврони українських військових формувань, які виконували бойові завдання на відповідній території [3]. Також було встановлено автора відео, його приналежність до відповідного підрозділу військових формувань рф та безпосередньо підтверджено факт катування й жорстокого поводження з військовополоненими.

Враховуючи викладене, варто наголосити, що ратифікація Україною Римського статуту 21 серпня 2024 року відкрила шлях до юрисдикції Міжнародного кримінального суду, що вимагає належної доказової бази для кваліфікації воєнних злочинів. В умовах обмеженого доступу до тимчасово окупованих чи іноземних територій, де утримуються громадяни України та інші особи, залучені до оборони держави, саме OSINT-аналіз забезпечує виявлення й фіксацію фактів порушення міжнародного гуманітарного права та прав людини з метою притягнення винних до кримінальної відповідальності.

Список використаних джерел:

1. Berkeley School of Law. Berkeley Protocol on Digital Open Source Investigations: Ukrainian translation. URL: https:// www.law.berkeley.edu/wp-content/uploads/archive/ 2022/03/ Ber keley- Protocol-Ukrainian.pdf (дата звернення: 10.05.2026).

2. Війна та правосуддя: як слідчим ефективно використовувати OSINT та що робити із рішеннями “судів” на

непідконтрольних територіях - Українська Гельсінська спілка з прав людини. *Українська Гельсінська спілка з прав людини*. URL:https://www.helsinki. org.ua/articles/viyna-ta-pravosuddia-iak-slidch ym-efektyvno-vykorystovuvaty-osint-ta-shcho-robyty-iz-rish enniam y-sudiv-na-nepidkontrolnykh-terytoriiakh/ (дата звернення: 09.05.2026).

3. Відео з відрізанням голови українському військовому. Все, що відомо про жорстокий злочин - BBC News Україна. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/ articles/ c3g648d2e87o (дата звернення: 09.05.2026).

4. Правове регулювання дотримання прав і свобод людини та громадянина в умовах адміністративно-правового режиму воєнного стану : колективна монографія / Є. Львова, О. Жильцов, О. Пасько та ін. ; за заг. ред. А. В. Денисової. – Одеса : Видавництво «Юридика», 2025 .–840с. URL:https://dspace.oduvs.edu.ua/server/api/core/bitstreams/e712e92f-e4c6-4b2c-9998-f216304a02f0/content (дата звернення: 09.05.2026).

5. Toma M. G., Vasylova O. V. OSINT tools: recording war crimes in Ukraine. *Analytical and Comparative Jurisprudence*. 2025. No. 2. P. 905–909. URL: https://doi.org/10.24144/2788-6018.2025.02.134 (date of access: 09.05.2026).

ЩОДО ПИТАННЯ ЕФЕКТИВНОГО ЗАСТОСУВАННЯ OSINT-ТЕХНОЛОГІЙ ПРИ ЗАБЕЗПЕЧЕННІ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ ТА ЗЛОЧИНІВ ПРОТИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Міщенко Дмитро Олексійович
т.в.о. заступника начальника управління – начальника відділу аналітичної роботи Управління кримінального аналізу Головного управління Національної поліції в Запорізькій області

З огляду на масштабні бойові дії та систематичні порушення міжнародного гуманітарного права, Запорізька область сьогодні є одним із ключових регіонів, де фіксуються численні воєнні злочини та злочини проти основ національної безпеки.

Якісне криміналістичне забезпечення розслідувань кримінальних проваджень вказаної категорії є складовою механізму документування та притягнення до відповідальності винних осіб.

Під криміналістичним забезпеченням розуміють застосування методів, засобів і прийомів, які дозволяють документувати факти воєнних злочинів, встановлювати обставини, засоби та суб'єктів правопорушення [1, с.81].

Аналіз наукових джерел з даного питання свідчить про основні виклики – відсутність спеціальних методик розслідування воєнних злочинів, водночас необхідність залучення аналітиків для обробки великих масивів значущої інформації, яка на 2022 рік лишалась достатньо обмеженою [2, с. 54].

Наразі ситуація, на нашу думку, значно покращилась. Зокрема, на прикладі Запорізької області можна прослідкувати за прогресуючим збільшенням частоти залучення працівників кримінального аналізу до формування аналітичних матеріалів при розслідуванні кримінальних правопорушень, передбачених ч.1, 2 ст. 438 КК України: у 2024 році – виконано 122 запити слідчих та оперативних підрозділів, у 2025 році – 179 запитів, за три з половиною місця поточного року – вже 139. Проведення аналітичних досліджень за воєнними злочинами дозволило сформувати певний емпіричний досвід.

Адекватна аналітика потребує системного збирання даних: свідчень очевидців, медичних звітів, фото/відео матеріалів, супутникових чи OSINT-даних, експертних висновків, даних правоохоронних органів. Водночас, для прифронтових територій характерні особливі виклики: обмежений доступ до потерпілих та місця події, постійна загроза безпеці, висока мобільність населення, ризики знищення чи втрати доказів через бойові дії, бомбові та дронові удари супротивника.

З огляду на викладене, OSINT-джерела лишаються важливим джерелом інформації для встановлення об'єктивної істини в справі, особливо по злочинах, вчинених на тимчасово окупованих територіях.

До загальнодоступних джерел OSINT зазвичай відносять [3, с. 146-147]:

– ЗМІ: преса, радіо, телебачення та ін. *(малоефективний при документуванні саме воєнних злочинів, проте ефективний при вивченні колабораційної діяльності)*;

– веб-контент: сайти, соціальні мережі та ін. *(найбільш інформативні ресурси в розрізі ідентифікації осіб, що вчинили злочини, частіше за все використовується разом із витоками з різних інформаційних баз; дуже ефективні при документуванні колаборантів)*;

– академічні публікації: наукові статті, публікації конференцій тощо *(так само малоефективний з огляду на профіль злочинів)*;

– офіційні загальнодоступні дані: відкриті урядові документи, оголошення державних підприємств тощо *(корисне джерело додаткової інформації, зокрема – відомості про нагородження із підсвічуванням персональних даних, посад військовослужбовців, та особливо цінне джерело при дослідженні колаборайційної діяльності)*.

Додатковими джерелами для пошуку інформації є *пошукові системи*, зокрема від Yandex, яка має окремий пошуковий модуль пошуку за зображеннями, що непогано зарекомендував себе в пошуку за російським сегментом.

Ще одним, досить цінним джерелом, на наш погляд, є *витоки* з різноманітних інформаційних баз, доступ до яких можна отримати через Telegram боти, онлайн сервіси, на кшталт «OsintKit», або локально за допомогою спеціального програмного забезпечення для роботи з базами даних (Cronos та ін.), попередньо здобувши їх на спеціалізованих ресурсах.

Також, з огляду на досвід роботи за воєнними злочинами не варто лишати поза увагою такі інформаційні джерела, як матеріали незалежних розслідувань, а також ресурс «Миротворець», що містить матеріали, зібрані незалежними OSINTерами.

Окремо варто відзначити використання автоматизованих рішень на основі аналізу інформації з відкритих джерел з допомогою AI алгоритмів, зокрема аналітичних платформ, що використовують бази даних, сформовані шляхом парсингу інформації з різних джерел, в тому числі соціальних мереж. Такі сервіси дозволять проводити пошук з допомогою технології розпізнання обличь – Search4faces, Clearview AI, PimEyes [4, с.140, 158-165]. Деякі з них, такі як Big Data People Artellence, дають значно ширший функціонал – можливість проаналізувати зв'язки особи, деталізувати її профілі у соціальних мережах, уподобання та ін. Цікавим продуктом є Neuro.identigraf, який здійснює пошук за фотозображеннями з раніше згаданого ресурсу «Миротворець».

Практика роботи з такими джерелами дозволяє погодитись з тезою про те, що у більшості випадків інформацію, отриману з відкритих джерел, слід обов'язково перевіряти на предмет достовірності [3, с.153]. Особливу увагу варто звертати на верифікацію відомостей, отриманих з баз витоків та ресурсів з узагальненими результатами роботи незалежних OSINTерів.

Застосування OSINT-джерел при документуванні воєнних злочинів має також важливі правові та процесуальні аспекти, зокрема: правильна фіксація та документування учасників та подій у тому числі їх цифрових слідів із дотримання стандартів міжнародного гуманітарного права й кримінального процесу.

Для досягнення таких цілей аналітики мають керуватися уніфікованими стандартами оформлення документації та застосовувати міжнародні підходи до документування злочинів відповідного характеру. Як приклад, доцільно застосувати рекомендації та методологію наведені у міжнародних дослідницьких проєктах щодо документування воєнних злочинів, зокрема Протоколі Берклі [5, с. 93-96, 6], який передбачає пошук інформації про події, факти або осіб у кількох незалежних джерелах, її аналіз та порівняння з метою верифікації здобутої інформації, що робить OSINT ефективним інструментом формування доказової бази.

Так, у 2022 році аналітиками управління кримінального аналізу ГУНП в Запорізькій області у взаємодії зі слідчими Управління СБУ в Запорізькій області та оперативниками Управління карного розшуку ГУНП в Запорізькій області з використанням методів OSINT та методології Протоколу Берклі зібрані докази протиправної злочинної діяльності «топ-посадовців» російських окупаційних органів та чиновників меншого рангу на тимчасово-окупованій території Запорізької області. Аналітиками встановлено та задокументовано більше як 90 осіб причетних до злочинів проти основ Національної безпеки України [6]. Зазначені матеріали разом з іншими процесуальними документами лягли в основу доказової бази під час підготовки зрадникам семи повідомлень про підозру та ухвалені двох вироків суду [7, 8].

Підсумовуючи викладене, слід підкреслити, що через відсутність прямого доступу до місця події та інші ризики, OSINT-інструменти лишаються важливим джерелом інформації для встановлення об'єктивної істини по злочинах, вчинених на тимчасово

окупованих територіях. Кваліфіковане використання таких джерел, а також коректна інтерпретація та верифікація, поєднані із правильною процесуальною фіксацією та документуванням, дозволяють досягти успішної реалізації у вигляді реальних судових рішень щодо притягнення до відповідальності винних осіб.

Список використаних джерел:

1. Левицький А.О., Москалюк О.М. «Криміналістичне забезпечення розслідування воєнних злочинів: окремі проблеми науково-теоретичних засад». Криміналістичний вісник, № 2(42), 2024, м. Київ. URL: https://visnyk.dndekc.mvs.gov.ua/index.php/visnuk/article/view/297/196 (дата звернення 15.04.2026).

2. О. Дуфенюк. Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації / Оксана Дуфенюк // Baltic Journal of Legal and Social Sciences, 2022 No. 1. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5150/1/1771-Article%20Text-2060-1-10-20220801.pdf (дата звернення 15.04.2026)

3. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288с.

4. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро: Дніпров. держ. ун-т внутр. справ, 2024. 180 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/15045/5/макет_Посібник%2024%20кафедра%20ЕтаІБ.pdf (дата звернення 15.04.2026).

5. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро: Дніпров. держ. ун-т внутр. справ, 2024. 180 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/15045/5/макет_Посібник%202024%20кафедра%20ЕтаІБ.pdf (дата звернення 15.04.2026).

6. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. URL: https://law.berkeley.edu/wpcontent/ uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення 15.04.2026).

7. Аналітичні матеріали Управління кримінального аналізу Головного управління Національної поліції в Запорізькій області.

8. Електронні примірники вироків суду. URL: https://reyestr.court.gov.ua /Review/111891367

ОСНОВНІ НАПРЯМКИ ІНДИВІДУАЛЬНО-ПРОФІЛАКТИЧНОГО ЗАПОБІГАННЯ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ УКРАЇНИ НЕЗАКОННОМУ ПОВОДЖЕННЮ ЗІ ЗБРОЄЮ, БОЙОВИМИ ПРИПАСАМИ АБО ВИБУХОВИМИ РЕЧОВИНАМИ

Педін Ростислав Артурович, *аспірант*
Одеський державний університет внутрішніх справ

Першим основним напрямом запобігання є контроль за ризиковою поведінкою конкретних власників або фактичних володільців зброї. У цьому контексті Закон України «Про Національну поліцію» [1] та наказ МВС України від 21.08.1998 р. № 622 [2] покладають на поліцію контроль за дотриманням фізичними і юридичними особами спеціальних правил зберігання та використання зброї, боєприпасів, вибухових речовин і матеріалів. У межах індивідуальної профілактики цей напрям передбачає вжиття таких заходів: перевірка умов зберігання зброї за місцем проживання; контроль чинності дозвільних документів; з'ясування, чи не допускає особа доступ сторонніх до зброї; реагування на повідомлення про втрату, незаконну передачу чи використання зброї; документування порушень правил її обігу. Індивідуально-профілактичний зміст цих заходів полягає в тому, що вони спрямовані не на невизначене коло осіб, а на конкретного власника або володільця зброї, поведінка якого вже свідчить про підвищений ступінь небезпеки.

Другим напрямом є профілактична робота з особами, які знайшли, отримали чи зберігають зброю, бойові припаси або вибухові речовини.

Як показало проведене дослідження, дієвими заходами запобігання в межах цього напряму є: індивідуальне роз'яснення особі умов декларування, прийняття від неї заяви, перевірка обставин знаходження або отримання зброї та боєприпасів до неї, контроль за дотриманням встановлених правил її подальшого зберігання, а в разі неможливості декларування – прийняття зброї та боєприпасів до неї як добровільно зданої. За офіційними роз'ясненнями НПУ, особа має негайно повідомити поліцію про знайдену або наявну зброю та боєприпаси до неї і протягом 24 годин прибути до

найближчого підрозділу поліції для її декларування або добровільної здачі [3].

Третім напрямом є індивідуально-роз'яснювальна та переконувальна робота, яка охоплює такі заходи, як: профілактичні бесіди, офіційні попередження, доведення до особи кримінально-правових наслідків незаконного носіння, зберігання, передачі чи збуту зброї та боєприпасів до неї, роз'яснення порядку добровільної здачі або декларування, інформування про правила поведінки у разі виявлення зброї, боєприпасів або вибухових речовин.

Четвертим напрямом є реагування на конфліктні та кризові ситуації, у яких зброя або боєприпаси поєднуються з агресивною поведінкою конкретної особи. Йдеться про випадки домашнього насильства, сімейних конфліктів, погроз, стану сп'яніння, психоемоційної нестабільності, коли наявність зброї різко підвищує ризик тяжких наслідків. Закон України «Про запобігання та протидію домашньому насильству» формує правову основу для спеціального реагування на такі ситуації, а відомчі нормативно-правові акти щодо організації реагування на заяви і повідомлення про правопорушення передбачають необхідність з'ясування обставин домашнього насильства та забезпечення безпеки потерпілих [4].

П'ятим напрямом є персоніфікована профілактика на деокупованих, прифронтових та «забруднених» зброєю і вибухонебезпечними предметами територіях. Індивідуальний профілактичний вплив за цим напрямом полягає у зміні рішення конкретної особи: не приховувати знайдену зброю, а перевести її у контрольований поліцією режим. Такий підхід підтримується і офіційною позицією МВС України [5], і роз'ясненнями територіальних органів НПУ [6; 7], де наголошується, що після декларування зброя вважається законною, а наявність незадекларованої зброї та боєприпасів тягне кримінальну відповідальність.

Список використаних джерел:

1. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради.* 2015. № 40-41. Ст. 379.

2. Про затвердження Інструкції про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та патронів до них, а також

боєприпасів до зброї, основних частин зброї та вибухових матеріалів: наказ Міністерства внутрішніх справ України від 21.08.1998 р. № 622. URL: https://zakon.rada.gov.ua/ laws/ show/z0637-98#Text (дата звернення: 08.04.2026).

3. Що потрібно знати про декларування зброї. *Головне управління Національної поліції в Одеській області*. URL: https://od.npu.gov.ua/news/shcho-potribno-znaty-pro-deklaruvannia-zbroi (дата звернення: 08.04.2026).

4. Про запобігання та протидію домашньому насильству: Закон України від 07.12.2017 р. № 2229-VIII. *Відомості Верховної Ради*. 2018. № 5. Ст. 35.

5. Про затвердження Порядку декларування вогнепальної зброї і боєприпасів до неї: наказ Міністерства внутрішніх справ України від 18.11.2024 р. № 768. URL: https://zakon.rada.gov.ua/laws/ show/z1739-24#Text (дата звернення: 08.04.2026).

6. Поліція нагадує громадянам про можливість законного зберігання знайденої зброї та боєприпасів. *Головне управління Національної поліції в Харківській області*. URL: https://hk.npu.gov.ua/news/politsiia-nahaduie-hromadianam-pro-mozhlyvist-zakonnoho-zberihannia-znaidenoi-zbroi-ta-boieprypasiv (дата звернення: 08.04.2026).

7. Що потрібно знати про декларування зброї. *Головне управління Національної поліції в Одеській області*. URL: https://od.npu.gov.ua/news/shcho-potribno-znaty-pro-deklaruvannia-zbroi (дата звернення: 08.04.2026).

ЦИФРОВІ ДЖЕРЕЛА ІНФОРМАЦІЇ ЯК ЗАСІБ МІНІМІЗАЦІЇ ВТОРИННОЇ ВІКТИМІЗАЦІЇ ПОТЕРПІЛИХ ВІД ВОЄННИХ ЗЛОЧИНІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стеценко Д.
аспірант аспірантури та ад'юнктури
Одеського державного університету внутрішніх справ

Повномасштабна збройна агресія російської федерації проти України істотно змінила як предмет доказування у кримінальних провадженнях щодо воєнних злочинів, так і способи отримання та перевірки доказової інформації. Для значної кількості таких

проваджень характерними є відкладений доступ до місця події, знищення матеріальних слідів, переміщення потерпілих за межі регіону проживання або за кордон, а також їхній тривалий психотравмувальний стан. За цих умов показання потерпілих залишаються одним із ключових джерел відомостей про подію злочину, проте їх повторне отримання, уточнення або відтворення в різних процесуальних формах здатне спричиняти вторинну віктимізацію, тобто додаткове травмування особи вже самим кримінальним провадженням [1; 2].

У сучасних дослідженнях проблематика цифрових джерел інформації найчастіше розглядається крізь призму доказування, допустимості та оцінки цифрових матеріалів. Водночас не менш важливим є їх правозахисний потенціал. Йдеться насамперед про те, що належно виявлені, зафіксовані та верифіковані фото- і відеоматеріали, супутникові знімки, геолокаційні дані, матеріали відкритих джерел, цифрові архіви міжнародних організацій та інші цифрові сліди події можуть використовуватися не лише для підтвердження фактичних обставин, а й для зменшення потреби у багаторазовому допиті потерпілого, повторному відтворенні ним травматичних подій і постійному процесуальному поверненні до пережитого насильства [3; 4].

Саме тому є необхідним з'ясування того, яким чином цифрові джерела інформації можуть використовуватися у кримінальному провадженні щодо воєнних злочинів як інструмент мінімізації вторинної віктимізації потерпілих, а також визначення основних напрямів удосконалення відповідної практики. Науковий інтерес у цьому аспекті зумовлений необхідністю поєднати завдання повного й ефективного доказування з вимогою гуманного, потерпіло-орієнтованого кримінального процесу.

Вторинна віктимізація у провадженнях про воєнні злочини має підвищений ризик порівняно з багатьма іншими категоріями кримінальних проваджень. Потерпілий нерідко повідомляє про події, пов'язані із загибеллю членів сім'ї, катуванням, сексуальним насильством, незаконним позбавленням волі, примусовим переміщенням, руйнуванням житла чи втратою майна. За відсутності належної процесуальної організації слідчі та інші процесуальні дії можуть перетворюватися на повторне проживання травматичного досвіду. У цьому контексті слушною є позиція С. Є. Абламського, відповідно до якої реальна цінність процесуального статусу

потерпілого визначається не лише формальним переліком прав, а ефективністю механізмів їх забезпечення [1]. Близький підхід відображено і в роботі О. О. Сольонової, яка підкреслює особливу вразливість показань потерпілого до впливу травматичного стану, часової дистанції та психологічного навантаження [2].

Цифрові джерела інформації здатні зменшувати вторинну віктимізацію щонайменше у трьох вимірах. По-перше, вони дозволяють частково компенсувати нестачу безпосередніх матеріальних слідів події, коли місце злочину недоступне або огляд був проведений із запізненням. У такому разі цифрові матеріали можуть підтверджувати окремі факти без повторного детального відтворення їх потерпілим. По-друге, вони сприяють процесуальній концентрації інформації: якщо фото, відео, супутникові дані або інші цифрові відомості вже фіксують ключові елементи події, потреба у повторному допиті з метою уточнення кожної деталі може бути зменшена. По-третє, належне використання цифрових матеріалів дає змогу більш раціонально планувати слідчі дії та зосереджувати комунікацію з потерпілим лише на тих питаннях, які не можуть бути перевірені іншими засобами [5; 6].

Разом із тим такий потенціал реалізується лише за умови правильної процесуальної організації роботи з цифровими джерелами. Д. В. Лісніченко обґрунтовано зазначає, що дані з медіа та відкритих джерел не повинні сприйматися як самостійний, позапроцесуальний масив інформації; вони мають бути введені до кримінального провадження через зрозумілі процесуальні форми документи, протоколи огляду, додатки до них, висновки експерта або інші передбачені законом засоби [3]. Для теми вторинної віктимізації це має принципове значення: лише тоді, коли цифровий матеріал є процесуально придатним і здатним нести доказове навантаження, він справді може замінити частину повторних комунікацій із потерпілим, а не лише дублювати вже отримані показання.

Окремої уваги потребує питання методології роботи з відкритими джерелами. О. Є. Користін і С. В. Демедюк переконливо доводять, що OSINT є не просто технічним пошуком інформації, а комплексною аналітичною діяльністю, яка вимагає професійної підготовки, послідовної верифікації та чіткої фіксації отриманих результатів [4]. Це означає, що для зменшення вторинної віктимізації потерпілих цифрові джерела повинні використовуватися не випадково і не епізодично, а в межах заздалегідь продуманої

доказової тактики. Чим вищою є якість первинного цифрового документування, тим менше підстав для неодноразового повернення до потерпілого з однаковими або суміжними питаннями.

Потерпіло-орієнтований вимір цієї проблеми особливо чітко простежується у міжнародних стандартах. У дослідженні щодо прав потерпілих від насильницьких злочинів в Україні наголошується, що сучасний підхід до роботи з потерпілим повинен бути зорієнтований на мінімізацію повторної травматизації, належне інформування, безпеку та процесуальну чутливість [7]. У свою чергу Протокол Берклі, хоча й спрямований передусім на ефективне використання цифрових відкритих джерел у розслідуванні міжнародних злочинів, фактично закладає також етичні орієнтири: планування збору даних, фіксацію контексту, перевірку достовірності та врахування ризиків для жертв, свідків і спільнот [8]. Для українського кримінального провадження це означає, що цифрові матеріали мають використовуватися не лише як технічний ресурс доказування, а і як інструмент більш обережної, менш травматичної комунікації з потерпілим.

На наш погляд, практичне використання цифрових джерел інформації як засобу мінімізації вторинної віктимізації потребує реалізації кількох взаємопов'язаних кроків. Перший розроблення методичних рекомендацій для слідчих і прокурорів щодо поєднання цифрового документування з потерпіло-орієнтованим підходом. У таких рекомендаціях доцільно передбачити, що перед повторним допитом або уточнювальною процесуальною дією має оцінюватися, чи можуть відповідні відомості бути отримані або перевірені за допомогою вже наявних цифрових матеріалів. Другий ширше залучення спеціалістів у сфері цифрової криміналістики та OSINT на ранніх етапах провадження, коли формується первинна доказова картина події. Третій нормативне й організаційне закріплення підходу, за яким цифрові джерела розглядаються не лише як додатковий доказовий інструмент, а як один із засобів забезпечення прав потерпілого в кримінальному провадженні.

Отже, цифрові джерела інформації у справах про воєнні злочини мають значення не лише для встановлення фактичних обставин, а й для побудови більш гуманної моделі кримінального процесу. Їх належне використання здатне зменшити потребу в повторному відтворенні потерпілим травматичних подій, сприяти мінімізації вторинної віктимізації та підвищити процесуальну

чутливість розслідування. Перспективним напрямом подальших досліджень є розроблення цілісної моделі взаємодії цифрового доказування та потерпіло-орієнтованого підходу у кримінальних провадженнях щодо міжнародних злочинів.

Список використаних джерел:

1. Абламський С. Є. Захист прав і законних інтересів потерпілого у кримінальному провадженні : монографія. Харків : Панов, 2015. 240 с.

2. Сольонова О. О. Показання потерпілого як джерело доказів у кримінальному провадженні : дис. ... канд. юрид. наук. Київ, 2018. 248 с.

3. Лісніченко Д. В. Використання даних з медіа та відкритих джерел (OSINT) у процесі доказування у кримінальних провадженнях. Право та державне управління. 2025. № 1. С. 234–240.

4. Користін О. Є., Демедюк С. В. OSINT: Open Source Intelligence. Теорія та методологія. Одеса : ОДУВС, 2025.

5. Шевчишена К. П. Розслідування воєнних злочинів в Україні: дис. ... д-ра філософії за спец. 081 «Право». Київ, 2024.

6. Розслідування воєнних злочинів і пов'язаних з війною кримінальних правопорушень: кримінально-правові, кримінальні процесуальні та криміналістичні аспекти : наук.-практ. посіб. / [І.В. Гловюк, О. М. Литвинов, Ю. В. Орлов та ін.] ; за заг. ред. д-ра юрид. наук, проф., члена-кор. НАПрН України В.В. Сокуренка; МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2023. – 400с.

7. Права потерпілих від насильницьких злочинів в Україні: міжнародні стандарти та національні практики / А. Орлеан, Т. Павлюковець, Є. Крапивін та ін.; за ред. В. Човгана. Київ : ВД «Артек», 2020. 206 с.

8. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York; Geneva : United Nations, 2022.

ЗАБЕЗПЕЧЕННЯ ПРАВ УЧАСНИКІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Теслюк Ірина Олександрівна
старший викладач кафедри кримінально-правових дисциплін
Одеського державного університету внутрішніх справ,
кандидат юридичних наук

Повномасштабна збройна агресія проти України зумовила безпрецедентні виклики для системи правосуддя, у тому числі, й для кримінального судочинства. Проведення процесуальних дій в умовах постійних обстрілів, тимчасової окупації територій, руйнування інфраструктури та масової міграції населення змусило законодавця оперативно адаптувати Кримінальний процесуальний кодекс (КПК) України до реалій воєнного стану.

Зокрема, стаття 615 Кримінального процесуального кодексу України [1] є ключовим інструментом, за допомогою якого законодавець адаптував кримінальне судочинство до умов воєнного стану. Ця норма фактично запровадила особливий режим досудового розслідування та судового провадження, який діє в умовах воєнного, надзвичайного стану або у районі проведення воєнних (бойових) дій.

Однак розширення повноважень органів досудового розслідування та прокуратури з метою забезпечення ефективності слідства нерідко створює ризики для дотримання основоположних прав учасників кримінального провадження - як сторони захисту (підозрюваного, обвинуваченого), так і сторони обвинувачення та інших учасників (потерпілих, свідків).

І.С. Ганенко зазначає, що система правосуддя в умовах збройного конфлікту виступає одним із основних інституцій, який спрямовує свою діяльність на карне переслідування за вчинення воєнних злочинів, злочинів геноциду, проти людяності та агресії, притягнення винних до відповідальності, забезпечення неупередженого правосуддя та відновлення справедливості для жертв збройного-конфлікту, дотримання прав підозрюваних та обвинувачених в ході кримінального провадження, взаємодію з міжнародними організаціями та судами, дотримання норм та принципів міжнародного гуманітарного права та ін. В умовах збройного

конфлікту судова система стикається з наступними складнощами в сфері здійснення правосуддя: недостатній рівень матеріально-технічного забезпечення, людських та фінансових ресурсів, знищення або втрата важливих доказів у справах, внутрішнє переміщення та виїзд за кордон ключових учасників процесу, зростанням кількості кримінальних правопорушень, впровадження нових норм до Кримінального кодексу України та кримінального процесуального законодавства, подолання судового імунітету рф та ін. [2].

Попри зазначене, динамічність законодавства та практики Верховного Суду потребує постійного переосмислення балансу між державним інтересом (ефективне розслідування воєнних та інших злочинів) та приватним інтересом (захист прав людини).

Правове забезпечення, поряд з особливостями кримінально-процесуального порядку, включає і винятковий (особливий) правовий режим, який введено на території збройного конфлікту з метою стабілізації обстановки, відновлення законності та правопорядку, що, у свою чергу, сприяє і проведенню належного розслідування кримінальних правопорушень. Крім виняткового (особливого) правового режиму, існує потреба і в спеціальних нормативних передумовах розслідування кримінальних правопорушень, вчинених військовослужбовцями в умовах збройного конфлікту, які містили б правовий механізм, що забезпечує проведення належного їх розслідування [3].

Особливого значення в сучасній моделі доказування набуває використання цифрових і аналітичних інструментів, які дозволяють компенсувати втрату або недоступність традиційних джерел доказів та забезпечити безперервність встановлення фактичних обставин. Поєднання технологічних рішень із процесуальними вимогами формує якісно новий підхід до доказування, орієнтований не лише на фіксацію подій, а й на їх глибоку верифікацію та логічне відтворення у межах судового розгляду. Судова оцінка доказів у таких умовах набуває підвищеної інтелектуальної складності, оскільки вимагає врахування не лише змісту доказової інформації, а й специфіки її походження і способів отримання. У сукупності це свідчить про становлення доказування в умовах воєнного стану як особливої процесуальної моделі, спрямованої на забезпечення балансу між ефективністю кримінального переслідування та дотриманням фундаментальних засад кримінального судочинства [4].

Основне процесуальне навантаження в умовах збройного конфлікту припало на ст. 615 КПК України, яка дозволила: тимчасово покладати окремі повноваження слідчих суддів на прокурорів (у разі об'єктивної неможливості виконання суддею своїх функцій); проводити окремі слідчі дії без попереднього дозволу суду; широко застосовувати дистанційну участь осіб у кримінальному провадженні.

Однак, можливе порушення щодо забезпечення прав учасників у таких випадках як:

А) Обмеження прав підозрюваного/обвинуваченого на захист та судовий контроль. Передача повноважень слідчого судді (наприклад, щодо обрання запобіжного заходу у вигляді тримання під вартою на строк до 90 діб) до рук прокурора є вимушеним кроком. Водночас це послаблює систему «стримувань і противаг» та нівелює класичний принцип незалежного судового контролю. Крім того, логістичні труднощі та руйнування зв'язку в зонах бойових дій часто ускладнюють конфіденційне спілкування підозрюваного з адвокатом.

Б) Проблеми реалізації прав потерпілих та свідків. У кримінальних провадженнях щодо воєнних злочинів потерпілі та свідки нерідко перебувають за кордоном або на тимчасово окупованих територіях. Забезпечення їхньої безпеки, належне фіксування їхніх показань (із дотриманням принципу безпосередності дослідження доказів судом) та залучення до процесу через інструменти міжнародної правової допомоги залишається технічно й процедурно складним завданням.

В) Належність та допустимість доказів. Спрощення процедур фіксації (наприклад, можливість незалучення понятих за умови безперервного відеозапису слідчої дії) потребує від правоохоронців високої цифрової грамотності. Найменші технічні порушення процедури верифікації відеозапису в майбутньому можуть стати підставою для визнання доказів недопустимими в суді.

Таким чином, збройний конфлікт вимагає від кримінального процесу гнучкості та швидкості, проте воєнний стан не є підставою для ігнорування прав людини. Україна, задекларувавши європейський вектор розвитку, повинна навіть у найважчих умовах дотримуватися стандартів Конвенції про захист прав людини і основоположних свобод та практики ЄСПЛ. Баланс між безпекою держави та правами особи у кримінальному провадженні

досягається не шляхом скасування процесуальних гарантій, а через впровадження чітких, прозорих та технологічних процедур, які мінімізують людський фактор та зловживання владою. Аналіз положень статті 615 КПК України доводить, що кожне спрощення процедури є прямим наступом на класичні процесуальні гарантії. Тому застосування таких норм має бути строго обмежене критерієм абсолютної неможливості діяти у загальному порядку.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua /laws/ show/4651-17#Text

2. Ганенко І.С. Роль суду у забезпеченні кримінально-процесуального захисту прав людини в умовах збройного конфлікту. Юридичний науковий електронний журнал. № 9. 2024. С. 368-371.

3. Янковий М. О. Розслідування кримінальних правопорушень, вчинених військовослуж бовцями під час збройного конфлікту: постановка проблеми. Академічні візії. 2023. № 18. URL: https://www.academy-vision.org/index.php/av/article/view/282.

4. Калініна О.В. Доказування в кримінальному процесі в умовах воєнного стану. Право і суспільство. № 1. 2026. С. 208-214.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Фещенко Ростислав Дмитрович
Курсант навчально-наукового інституту №4,
Харківський національний університет внутрішніх справ,
Кіріка Діана Володимирівна
кандидатка юридичних наук, доцентка
Кафедра адміністративної діяльності ННІ №3
Харківського національного університету внутрішніх справ,

Сучасні збройні конфлікти вирізняються невпинним збільшенням обсягу цифрової інформації, що публікується у відкритому доступі безпосередніми очевидцями, журналістами, а також самими учасниками бойових дій. Зокрема, мультимедійний контент, такий як фотографії, відеозаписи й аудіозаписи, які

поширюються через соціальні платформи на кшталт Telegram, X (колишній Twitter) та TikTok, стає важливим джерелом первинних доказів для підрозділів кримінального аналізу. Цей контент має ключове значення під час розслідування воєнних злочинів і фіксації руйнувань цивільної інфраструктури. Водночас правоохоронні органи стикаються зі значними викликами, зокрема з високою швидкістю поширення таких даних, умисним їх спотворенням та можливим видаленням доказів до їх виявлення відповідними підрозділами. Це, у свою чергу, створює суттєві часові обмеження для збереження релевантної інформації [3].

Одним із найактуальніших завдань криміналістичної практики є забезпечення юридичної валідності цифрових доказів для їх подальшого використання у міжнародних судових інстанціях, таких як Міжнародний кримінальний суд. Проблема ускладнюється з огляду на те, що більшість популярних месенджерів та соціальних мереж автоматично видаляють метадані файлів під час їхнього завантаження. З-поміж таких метаданих — EXIF-теги, GPS-координати, технічні параметри камери та точна дата зйомки. Це зумовлює потребу у створенні альтернативних підходів до верифікації матеріалів, зокрема шляхом застосування методів хронолокації (визначення точного часу події) та геолокації (установлення географічних координат). Проте ручний аналіз цих параметрів є надзвичайно трудомістким і повільним процесом, що істотно знижує ефективність розслідувань у ситуаціях, коли необхідна оперативність роботи зі значними масивами даних (Big Data).

Вирішенням цих проблем може бути автоматизація роботи підрозділів кримінального аналізу через застосування технологій збору й перевірки даних із відкритих джерел (OSINT). Наприклад, автоматизована хронолокація дозволяє оцінювати достовірність автентичності фото- та відеоматеріалів за опосередкованими ознаками, навіть за відсутності оригінальних метаданих. Використання інструментів на кшталт SunCalc дає змогу розраховувати кут та довжину тіні у кадрі й співставляти ці показники з астрономічними даними конкретного регіону. Ще одним допоміжним засобом є крос-верифікація погодних умов: спеціальні алгоритми порівнюють зображені на відео метеорологічні явища (наприклад, дощ, сніг, хмарність) із відомостями про погодні умови в архівах метеорадарів чи супутникових даних на обрану дату. У геолокації застосовуються технології просторового аналізу, які дозволяють автоматично ідентифікувати характерні риси

ландшафту або інфраструктури, такі як лінії електропередач, особливості рельєфу, дороги чи архітектурні елементи. Ця інформація автоматично порівнюється з актуальними супутниковими зображеннями високої роздільної здатності.

Важливим аспектом автоматизованих OSINT-досліджень є дотримання криміналістичних норм поводження з цифровими доказами (Chain of Custody). Згідно з вимогами Берклiївського протоколу, завантаження матеріалів із мережі має супроводжуватися створенням криптографічних хеш-функцій (SHA-256 чи SHA-512) для кожного файлу [2]. Реєстрація цих хешів у захищених базах даних чи за допомогою сервісів штампів часу гарантуватиме незмінність даних із моменту їхнього отримання та унеможливить будь-які спроби їх фальсифікації або несанкціонованої модифікації.

Зменшення суто рутинного навантаження на аналітика за рахунок автоматизованих рішень первинної верифікації дозволяє змістити фокус уваги на безпосередній аналіз зв'язків, виявлення системності у діях ворога та ідентифікацію конкретних осіб, причетних до вчинення злочинів [1]. Таким чином, збалансоване впровадження автоматизованих OSINT-технологій у діяльність підрозділів кримінального аналізу Національної поліції України є критично необхідним кроком для формування беззаперечної та стійкої доказової бази.

Список використаних джерел:

1. Пензар Д., Мотовилець М. Правовий статус цивільного населення під час війни та гарантії його захисту // Пропілеї права та безпеки. 2025. № 8. С. 137–140. DOI: https://doi.org/10.32620/pls.2025.8.30 (дата звернення: 17.05.2026)

2. Берклiївський протокол стосовно цифрових розслідувань відкритих джерел [Електронний ресурс] / Управління Верховного комісара ООН з прав людини; Центр з прав людини Каліфорнійського університету в Берклі. – 2024. – Режим доступу: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 17.05.2026).

3. Digital evidence in criminal justice: challenges of utilization / Y. Demidova, K. Latysh, M. Kapustina [Electronic resource]. – Access mode: https://epublications.vu.lt/object/elaba %3A188477732/188477732.pdf (date of access: 17.05.2026).

OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ В КОНТЕКСТІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Яголковська Єлизавета Олександрівна
курсант 201 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС
Науковий керівник: ***Свинаренко Юрій Павлович***
Завідувач кафедри оперативно-розшукової діяльності навчально- наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України, доктор філософії, доцент

Оперативно-розшукова діяльність (ОРД) є важливою складовою діяльності правоохоронних органів, що забезпечує своєчасне виявлення, попередження та розкриття кримінальних правопорушень. У сучасних умовах воєнного стану її значення суттєво зростає, оскільки правоохоронні органи стикаються з новими викликами, пов'язаними з документуванням воєнних злочинів, діяльністю диверсійно-розвідувальних груп, інформаційними операціями та використанням цифрових технологій у злочинній діяльності. Відповідно до Закону України «Про оперативно-розшукову діяльність», ОРД є системою гласних і негласних заходів, спрямованих на захист прав і свобод людини, власності та безпеки держави [1].

У зв'язку з цифровізацією суспільства та активним використанням мережі Інтернет особливого значення набувають технології OSINT (Open Source Intelligence), які полягають у зборі, аналізі та використанні інформації з відкритих джерел. До таких джерел належать соціальні мережі (Telegram, Facebook, TikTok), відкриті реєстри, супутникові знімки, медіаресурси, форуми та інші онлайн-платформи. Використання OSINT у діяльності оперативних підрозділів дозволяє значно розширити інформаційну базу та підвищити ефективність оперативного пошуку. Воєнні злочини, передбачені нормами міжнародного гуманітарного права та Кримінального кодексу України, характеризуються високим рівнем суспільної небезпеки та складністю доказування. Зокрема, йдеться про такі діяння, як умисні вбивства цивільного населення, катування, депортація, руйнування цивільної інфраструктури тощо. У багатьох випадках доступ до місця вчинення злочину є обмеженим або відсутнім, що

ускладнює традиційні методи збору доказів. У таких умовах OSINT стає одним із ключових інструментів фіксації подій.

У межах оперативно-розшукової діяльності OSINT використовується на різних етапах. На етапі оперативного пошуку здійснюється моніторинг відкритих джерел з метою виявлення інформації про можливі злочини або причетних осіб. Наприклад, аналіз відеозаписів із соціальних мереж може дозволити встановити місце обстрілу, тип озброєння та підрозділ, який його здійснив. На етапі оперативної перевірки проводиться верифікація отриманої інформації шляхом геолокації, аналізу метаданих, порівняння з іншими джерелами. На етапі оперативної розробки встановлюються зв'язки між особами, формується їх профіль, аналізується їхня діяльність у цифровому середовищі.Особливе значення має використання OSINT у поєднанні з негласними слідчими (розшуковими) діями. Відповідно до Кримінального процесуального кодексу України, НСРД є ефективним інструментом отримання доказів, однак їх застосування потребує відповідного процесуального оформлення та дозволу суду [3]. OSINT може виступати як підстава для ініціювання НСРД або як допоміжний інструмент для перевірки отриманої інформації. Таким чином, відбувається інтеграція відкритих та негласних методів збору інформації. Конституція України гарантує дотримання прав і свобод людини, зокрема права на приватність [2]. У зв'язку з цим застосування OSINT повинно здійснюватися з урахуванням принципів законності, необхідності та пропорційності. Незважаючи на те, що інформація отримується з відкритих джерел, її використання у правоохоронній діяльності повинно відповідати вимогам законодавства та не порушувати права особи.

Однією з ключових проблем є трансформація OSINT-інформації у допустимі докази. Відповідно до КПК України, доказами визнаються лише ті дані, які отримані у законний спосіб та належним чином оформлені [3, с. 87]. Це означає, що оперативні працівники повинні забезпечити фіксацію джерела інформації, збереження її цілісності, документування процесу отримання та аналізу. У протилежному випадку такі дані можуть бути визнані недопустимими у суді. Як зазначає О. В. Капліна, належне документування є ключовою умовою ефективного кримінального провадження, оскільки саме від якості доказової бази залежить можливість притягнення винних осіб до відповідальності [3, с. 102]. У цьому контексті OSINT виступає не лише як джерело інформації, але й як елемент доказової системи.

Важливим напрямом є також використання OSINT у міжнародному співробітництві. Документування воєнних злочинів часто здійснюється з метою передачі матеріалів до міжнародних судових інстанцій, зокрема Міжнародного кримінального суду. У таких випадках особливої уваги набуває дотримання міжнародних стандартів збору доказів, що передбачають їх достовірність, перевірюваність та збереження. Разом із тим існують проблеми використання OSINT у діяльності оперативних підрозділів. Серед них можна виділити: значний обсяг інформації, що ускладнює її обробку; наявність фейкових матеріалів; складність встановлення першоджерела; відсутність чітких методичних рекомендацій; недостатній рівень підготовки кадрів. Крім того, існує ризик використання інформації, що була змінена або змонтована, що може призвести до помилкових висновків. Перспективи розвитку OSINT у системі ОРД пов'язані з впровадженням сучасних технологій, зокрема штучного інтелекту, автоматизованих систем аналізу даних, а також створенням єдиних інформаційних платформ. Важливим є також удосконалення законодавства, яке повинно чітко регламентувати порядок використання відкритих джерел інформації у правоохоронній діяльності.

Таким чином, OSINT-технології є невід'ємною складовою сучасної оперативно-розшукової діяльності, особливо у сфері документування воєнних злочинів. Їх ефективне використання дозволяє підвищити якість розслідування, забезпечити належне документування злочинів та сприяти притягненню винних осіб до відповідальності. Водночас необхідним є подальше вдосконалення нормативно-правової бази, методичного забезпечення та підготовки кадрів.

Список використаних джерел:

1. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII.
2. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР.
3. Капліна О. В., Марочкін І. Є. Кримінальний процес : підручник. Харків : Право, 2018.
4. Федчак І. А. Основи кримінального аналізу. Львів : ЛьвДУВС, 2020.
5. Шендрик В. В. Оперативно-розшукова діяльність органів Національної поліції України : навч. посіб. Київ : Алерта, 2020.
6. Бахчеван В. Ю. Використання OSINT у правоохоронній діяльності // 2022.

СЕКЦІЯ 5.
ІНСТРУМЕНТИ, МЕТОДИ ТА АЛГОРИТМИ ЗАСТОСУВАННЯ OSINT У АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ

ІНТЕГРАЦІЯ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ ТА OSINT-ТЕХНОЛОГІЙ У ПРОЦЕСІ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ І ПРОГНОЗУВАННЯ КРИМІНАЛЬНИХ РИЗИКІВ

Балтовський Олексій Анатолійович
доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ.
Сіфоров Олександр Іванович
кандидат технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ.

У сучасних умовах стрімкої цифрової трансформації суспільства, глобалізації інформаційних потоків, інтенсивного розвитку кіберпростору та зростання рівня залежності державних інституцій, правоохоронних органів, фінансових систем і критичної інфраструктури від інформаційно-комунікаційних технологій особливої актуальності набуває проблема формування ефективних механізмів виявлення, аналізу та прогнозування кіберзагроз і кримінальних ризиків. Кіберпростір перетворився не лише на середовище інформаційної взаємодії, а й на окремий сегмент соціально-технічної реальності, у межах якого виникають нові форми злочинної діяльності, реалізуються складні транснаціональні кримінальні схеми, здійснюється інформаційно-психологічний вплив, координуються деструктивні дії організованих груп та відбувається незаконне використання цифрових ресурсів. Відповідно, сучасна система забезпечення національної безпеки та протидії злочинності потребує якісно нових науково-методологічних підходів, здатних забезпечити інтегроване поєднання

аналітичних, інформаційних, прогностичних та інтелектуальних механізмів обробки даних.

У цьому контексті особливого значення набуває інтеграція методів системного аналізу та технологій OSINT (Open Source Intelligence), які формують міждисциплінарний інструментарій для виявлення латентних загроз, моделювання поведінкових патернів злочинної активності, оцінювання ризиків та підтримки процесів прийняття управлінських рішень у сфері кримінального аналізу й кібербезпеки [1].

З позиції системного аналізу кіберзагроза є складною стохастичною системою, що характеризується невизначеністю, нелінійністю, адаптивністю та високим рівнем латентності. Це обумовлює необхідність використання багатофакторних моделей, методів когнітивного моделювання, сценарного прогнозування, аналізу ризиків, нечіткої логіки, ієрархічного аналізу процесів та математичного моделювання поведінкових моделей. Особливе значення при цьому має концепція ризик-орієнтованого підходу, відповідно до якої ключовим завданням кримінального аналізу стає не лише фіксація вже вчинених правопорушень, а й раннє виявлення потенційних деструктивних тенденцій, індикаторів підготовки злочинної діяльності та факторів ескалації криміногенних процесів.

OSINT-технології у сучасних умовах виступають одним із найефективніших інструментів збору та аналітичної обробки інформації. Їх особливість полягає у використанні відкритих джерел інформації, які, попри публічний характер, можуть містити критично важливі дані для виявлення злочинної активності, встановлення зв'язків між суб'єктами, ідентифікації цифрових слідів та прогнозування поведінки потенційно небезпечних груп або осіб. На відміну від традиційної оперативно-розшукової діяльності, OSINT дозволяє здійснювати безперервний моніторинг інформаційного простору в режимі реального часу, забезпечуючи високий рівень масштабованості та адаптивності аналітичних процедур [1,2].

У контексті кібербезпеки OSINT використовується для виявлення витоків інформації, аналізу діяльності кіберзлочинних угруповань, моніторингу даркнет-середовищ, виявлення фішингових кампаній, збору індикаторів компрометації, аналізу цифрових активів, дослідження мережевої інфраструктури та відстеження деструктивної інформаційної активності. При цьому

ефективність OSINT значною мірою залежить від можливості інтеграції великих масивів даних у єдину аналітичну систему, здатну забезпечити виявлення прихованих закономірностей, аномалій та потенційних ризиків.

Сучасний кримінальний аналіз дедалі більше орієнтується на концепцію intelligence-led policing, відповідно до якої ключову роль у діяльності правоохоронних органів відіграє аналітичне забезпечення процесів управління безпекою. У межах цього підходу інформація перетворюється на стратегічний ресурс, а аналітичні системи стають основою для прогнозування кримінальних процесів, визначення пріоритетів оперативної діяльності та розробки превентивних заходів. Інтеграція системного аналізу та OSINT-технологій дозволяє формувати багаторівневі моделі кримінальних ризиків, що враховують як технічні, так і соціально-поведінкові фактори [2,3].

Одним із ключових аспектів інтеграції зазначених підходів є формування системи індикаторів кіберзагроз та кримінальних ризиків. Такі індикатори можуть включати аномальну мережеву активність, зміни у цифровій поведінці користувачів, поширення деструктивного контенту, активізацію закритих онлайн-спільнот, збільшення кількості спроб несанкціонованого доступу, появу інформації про продаж викрадених даних, координацію інформаційних атак та інші ознаки потенційної злочинної діяльності. Використання системного підходу дозволяє інтегрувати ці індикатори у комплексну модель оцінювання ризиків, де кожен параметр розглядається у взаємозв'язку з іншими елементами системи.

Важливу роль у процесі прогнозування кримінальних ризиків відіграють методи машинного навчання та інтелектуального аналізу даних. Застосування алгоритмів класифікації, кластеризації, нейронних мереж, аналізу часових рядів та поведінкової аналітики дозволяє виявляти приховані закономірності у великих масивах інформації та прогнозувати ймовірність реалізації певних загрозових сценаріїв. У поєднанні з OSINT-технологіями це створює можливість автоматизованого моніторингу інформаційного середовища та побудови систем раннього попередження про потенційні кіберінциденти.

Особливої уваги заслуговує використання графових моделей та мережевого аналізу у кримінальному аналізі. Соціальні

мережі, цифрові комунікації та онлайн-платформи формують складні мережеві структури, в межах яких відбувається взаємодія між суб'єктами злочинної діяльності. Аналіз таких структур дозволяє виявляти ключові вузли, канали комунікації, ієрархічні зв'язки та механізми координації деструктивної активності. Використання методів соціометричного аналізу, центральності вузлів, аналізу спільнот та алгоритмів пошуку аномалій сприяє підвищенню ефективності оперативно-аналітичної діяльності правоохоронних органів.

Водночас інтеграція системного аналізу та OSINT-технологій супроводжується низкою викликів та обмежень. Однією з ключових проблем є надмірний обсяг інформації, що генерується у цифровому середовищі. Великі масиви даних характеризуються високим рівнем шуму, неоднорідністю, фрагментарністю та наявністю дезінформаційних елементів. Це обумовлює необхідність розробки ефективних механізмів фільтрації, верифікації та оцінювання достовірності інформації. У цьому аспекті особливого значення набувають методи семантичного аналізу, обробки природної мови, автоматизованого фактчекінгу та виявлення інформаційних маніпуляцій [2].

Іншою важливою проблемою є забезпечення балансу між ефективністю аналітичної діяльності та дотриманням принципів законності, захисту персональних даних і прав людини. Масштабне використання відкритих джерел інформації створює ризики порушення приватності, неправомірного збору персональних даних та надмірного цифрового контролю. У зв'язку з цим виникає необхідність формування чіткої нормативно-правової бази, яка б регламентувала використання OSINT-технологій у діяльності правоохоронних органів, визначала межі допустимого моніторингу та забезпечувала прозорість аналітичних процедур.

Важливим напрямом розвитку є створення інтегрованих інформаційно-аналітичних платформ, здатних об'єднувати дані з різних джерел та забезпечувати комплексне оцінювання ризиків у режимі реального часу. Такі системи повинні базуватися на принципах модульності, масштабованості, адаптивності та кіберстійкості. Інтеграція технологій Big Data, штучного інтелекту, системної динаміки та OSINT-аналітики дозволить сформувати нове покоління аналітичних систем, орієнтованих на проактивне управління безпекою.

У контексті сучасних гібридних загроз кіберпростір дедалі більше використовується як інструмент інформаційно-психологічного впливу, координації деструктивної діяльності та реалізації транснаціональних кримінальних схем. Це обумовлює необхідність міжвідомчої та міжнародної інтеграції у сфері обміну аналітичною інформацією, координації кібербезпекових заходів та формування спільних стандартів кримінального аналізу. Особливого значення набуває співпраця між правоохоронними органами, науковими установами, освітніми закладами та приватним сектором, оскільки лише комплексний міждисциплінарний підхід здатний забезпечити ефективну протидію сучасним кіберзагрозам [3].

Таким чином, інтеграція методів системного аналізу та OSINT-технологій є одним із ключових напрямів розвитку сучасного кримінального аналізу та систем забезпечення кібербезпеки. Поєднання системної методології, інтелектуального аналізу даних, відкритої розвідки та прогнозних моделей створює передумови для переходу від реактивної моделі протидії злочинності до проактивної системи управління ризиками. Використання таких підходів дозволяє не лише підвищити ефективність виявлення кіберзагроз, а й забезпечити стратегічне прогнозування криміногенних процесів, мінімізувати рівень невизначеності та підвищити адаптивність правоохоронних систем до нових викликів цифрової епохи [3].

Перспективи подальших наукових досліджень у зазначеному напрямі пов'язані з удосконаленням моделей когнітивного аналізу кіберзагроз, розвитком систем ситуаційної обізнаності, впровадженням технологій explainable AI у кримінальному аналізі, розробкою інтелектуальних систем підтримки прийняття рішень та формуванням цифрових екосистем безпеки, орієнтованих на інтеграцію аналітичних, прогностичних і превентивних механізмів управління ризиками. У сучасних умовах саме синергія системного аналізу, OSINT-технологій та інтелектуальних інформаційних систем здатна забезпечити належний рівень стійкості держави, суспільства та правоохоронної системи до складних багатовекторних кіберзагроз і кримінальних викликів XXI століття.

Список використаних джерел:

1. Ісмайлов К.Ю., Балтовський О.А., Сіфоров О.І. Основні підходи щодо вирішення завдання оптимального календарного планування з використанням спеціалізованих алгоритмів.

Електронне наукове видання «Порівняльно аналітичне право». 2019. №2. С. 98 - 101.

2. Гіренко О. В., Гіренко О. О., Кулик Н. С. Методологія системного аналізу та прогнозування ризиків // Вісник Київського національного торговельно-економічного університету. Серія «Економіка і управління». 2021. № 2. С. 12-20.

3. Гіренко О. В., Гіренко О. О., Кулик Н. С. Методи прогнозування ризиків у системному аналізі // Вісник Київського національного торговельно-економічного університету. Серія «Менеджмент». 2022. № 1. С. 23-30.

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT У КРИМІНАЛЬНОМУ АНАЛІЗІ

Зеленчук Володимир Васильович
начальник ВКА ГУНП
в Івано-Франківській області
Куций Роман Володимирович
кандидат юридичних наук
заступник начальника ВКА ГУНП
в Івано-Франківській області
Черній Андрій Ігорович
старший інспектор з ОД ВКА ГУНП
в Івано-Франківській області

Актуальність дослідження. У сучасних умовах особливої актуальності набуває розвиток цифрових технологій та зростання кількості високотехнологічних загроз, що в свою чергу виникає необхідність в удосконаленні традиційних підходів до отримання й аналізу інформації. Інструменти OSINT (Open Source Intelligence) відіграють ключову роль, як засіб оперативного отримання, перевірки та систематизації відомостей із відкритих джерел що розміщенні на інтернет платформах. Запровадження підходів, заснованих на моделі Intelligence-led Policing, сприяє перетворенню розрізнених цифрових даних на структурований аналітичний продукт, який може бути використаний у процесі документування та розслідування кримінальних правопорушень. Це, у

свою чергу, підвищує ефективність діяльності правоохоронних органів у сфері протидії злочинності в інформаційному просторі [1, с. 251].

Метою даних тезисів є дослідження теоретичних та практичних аспектів використання інструментів OSINT у діяльності підрозділів кримінального аналізу, визначення їх ролі у процесі збору, верифікації та аналітичної обробки інформації з відкритих джерел, а також обґрунтування ефективності застосування сучасних цифрових технологій для протидії високотехнологічній злочинності в умовах розвитку моделі Intelligence-led Policing.

Основний матеріал.

Кримінальний аналіз визначається як специфічний вид інтелектуальної діяльності, спрямований на ідентифікацію та точного визначення внутрішніх зв'язків між фрагментарними відомостями про об'єкти дослідження [2, с. 9]. Ключовою науковою проблемою застосування OSINT є пошук та перетворення неструктурованого інформаційного масиву на достовірний аналітичний продукт через багаторівневу верифікацію та оцінку [3, с. 21].

Аналітичний процес базується на циклічній моделі, що включає такі етапи:

1. Постановка завдання та планування: формування запиту на основі селекторів — ПІБ, номерів телефонів, акаунтів у месенджерах та інших цифрових ідентифікаторів [4, с. 71].
2. Збирання та накопичення: систематичний пошук даних у реєстрах та соціальних медіа [4, с. 34] з обов'язковим дотриманням операційної безпеки (OPSEC) [3, с. 61].
3. Перевірка інформації за методологією EJTA, а саме достовірності джерела та надійності змісту інформації, що дозволяє уникнути використання дезінформації.
4. Аналіз та візуалізація аналітичного продукту: побудова схем зв'язків, діаграм, що дозволяє виявляти латентні структури та ієрархію всередині груп.

На сьогодні, сучасний прикладний інструментарій аналітика дозволяє автоматизувати пошук та підвищити точність атрибуції даних, наприклад:

- Ідентифікація осіб та SOCMINT: пріоритетним напрямом у сучасних умовах є застосування технологій розпізнавання обличь на основі масивів зображень з відкритих джерел (Clearview

AI, PimEyes, FaceCheck.ID), що дозволяє за лічені хвилини встановити особу та отримати перші анкетні дані про об'єкт. Паралельно застосовуються інструменти пошуку цифрових відбитків через адреси електронної пошти та номери телефонів (OSINT Industries), а також комплексні системи ідентифікації (Artellence) для встановлення повного профілю особи [5, с. 5].

- Моніторинг месенджера Telegram: використання автоматизованих ботів (наприклад, Sherlock, Osint_kit) для збору інформації по номеру телефону або ID користувача. Аналітика каналів здійснюється через ресурси Telemetrio, TGstat, Telepathy [5, с. 2].
- Верифікація контенту та GEOINT: аналіз метаданих зображень та відео (InVID, metadata2go) [5, с. 1]. Геопросторова верифікація за допомогою супутникових сервісів (Google Earth Pro) та інструментів аналізу інсоляції та тіней (SunCalc, Shadow Map) [5, с. 7-10].
- Робота з реєстрами та Big Data: використання Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, а також систем бізнес-аналітики та моніторингу (Vkursi, YouControl, Clarity Project) для встановлення бенефіціарів та перевірки активів фігурантів та юридичних осіб [2, с. 270; 5, с. 1].

Обов'язковим є використання інструментів цифрового архівування (Wayback Machine, Hunchly, Archive.today) для збереження цілісності та автентичності інформації згідно з міжнародними стандартами Протоколу Берклі [5, с. 11-12; 1, с. 258].

Висновок. Системне використання передових інструментів у поєднанні з перевіреними методами оцінки даних дозволяє гарантувати високу якість і достовірність зібраної інформації, що є необхідною умовою для ефективної протидії викликам сучасної високотехнологічної злочинності. Юридична сила результатів OSINT-досліджень повинна забезпечуватися належною процесуальною фіксацією та оцінкою отриманих даних на предмет їх допустимості у відповідності до чинного законодавства України.

Список використаних джерел:

1. Главюк І. В. Оцінка результатів OSINT у судовій практиці: окремі питання. Юридичний науковий електронний журнал. 2025. № 91. С. 251–259.

2. Федчак І. А. Основи кримінального аналізу: навч. посібник. Львів: ЛьвДУВС, 2021. 288 с.
3. OSINT Open Source Intelligence. Інструменти та методи: навч. посібник / О. Користін, С. Демедюк та ін. Київ: 7БЦ, 2025. 460 с.
4. Кисельов А. О., Копилов Е. В., Худенко Д. М. Основи кримінального аналізу: навч. посібник. Дніпро: ДДУВС, 2023. 152 с.
5. Компендіум OSINT-інструментів / за підтримки ЄС та МФ «Відродження», 2024. 14 с.

OSINT В УМОВАХ AI-КОНТЕНТУ: ПРОБЛЕМА ВЕРИФІКАЦІЇ СИНТЕТИЧНИХ ОСОБИСТОСТЕЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Ісмайлов Карен Юрійович
кандидат юридичних наук, доцент
професор кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету внутрішніх справ
Заєць Олександр Михайлович
кандидат юридичних наук, доцент

У сучасних умовах правоохоронна діяльність дедалі більше залежить не лише від здатності отримувати інформацію з відкритих джерел, а й від можливості встановлювати її достовірність, походження та придатність для подальшого аналітичного або процесуального використання. Якщо раніше OSINT переважно розглядався як інструмент пошуку, збору, зіставлення та попереднього аналізу відкритих даних, то в умовах масового поширення AI-контенту його функціональне призначення істотно ускладнюється. На перший план виходить не просто виявлення інформації, а її верифікація, встановлення автентичності цифрової особи, джерела походження зображення, відео, голосового повідомлення, профілю в соціальній мережі або цифрової біографії. Так як не вірне первинна інтерпретація займе в подальшому багато часу для виявлення.

Особливої гостроти проблема набуває у зв'язку з поширенням синтетичних особистостей – штучно створених або частково

змодельованих цифрових ідентичностей, які можуть включати AI-згенеровані фотографії, фальшиві біографічні дані, історію активності у соціальних мережах, імітовані професійні зв'язки, голосові повідомлення, deepfake-відео та інші елементи цифрової присутності. Європол у звіті IOCTA 2025 прямо зазначає, що викрадені дані можуть використовуватися для створення діпфейків, синтетичних медіа та фальшивих ідентичностей, що ускладнює протидію злочинності, а особливо кіберзлочинності та організованій злочинності [1].

У правоохоронній діяльності такі явища створюють декілька взаємопов'язаних ризиків: помилкову ідентифікацію особи; використання фейкових профілів для шахрайства, вербування, дезінформації або соціальної інженерії; дискредитацію реальних осіб через синтетичний контент; ускладнення доказування у кримінальному провадженні; зниження довіри до відкритих джерел як допоміжного інструменту кримінального аналізу. Інтерпол у межах Project SynthWave окремо розвиває правоохоронні спроможності щодо виявлення AI-згенерованих синтетичних медіа, що підтверджує міжнародне визнання проблеми як практично значущої для органів правопорядку [2].

Для України ця проблематика має додаткове значення в умовах воєнного стану, гібридних загроз, інформаційно-психологічних операцій, документування воєнних злочинів, кіберзлочинності та активного використання відкритих цифрових джерел у правоохоронній діяльності. Закон України «Про Національну поліцію» прямо передбачає здійснення поліцією інформаційно-аналітичної діяльності для реалізації її повноважень [3], а Закон України «Про основні засади забезпечення кібербезпеки України» визначає участь Національної поліції України у взаємодії в межах національної системи реагування на кіберінциденти, кібератаки та кіберзагрози [4].

Проблематика OSINT у правоохоронній діяльності вже стала предметом наукової уваги як міжнародних, так і українських дослідників та інституцій. На міжнародному рівні питання використання відкритих джерел, цифрової ідентичності, діпфейків та AI-контенту активно розглядаються в аналітичних матеріалах Europol, INTERPOL, ENISA, UNODC [5-7]. Зокрема, Europol у SOCTA 2025 звертає увагу на те, що злочинці за допомогою синтетичних медіа можуть вводити в оману потерпілих, імітувати

реальних осіб, здійснювати дискредитацію або шантаж. UNODC у 2025 році також зазначає, що злочинні групи дедалі активніше використовують AI для створення deepfake, голосового клонування та синтетичних ідентичностей у кіберзлочинних схемах.

У міжнародному науково-практичному дискурсі особливу увагу приділено не лише технічному виявленню AI-контенту, а й формуванню комплексної моделі реагування: поєднанню цифрової криміналістики, аналітики відкритих джерел, міжнародної співпраці, підготовки спеціалістів та правового регулювання. У матеріалах EL PAcCTO 2.0, присвячених «weaponizing AI», окремо наголошується на необхідності посилення правоохоронних спроможностей через спеціалізовані підрозділи, інструменти криміналістичного аналізу AI-контенту, алгоритмічну простежуваність, підготовку фахівців і міжнародну взаємодію [8].

В українській науковій площині питання OSINT розглядаються у працях, присвячених кримінальному аналізу, інформаційно-аналітичній діяльності поліції, фіксації воєнних злочинів, забезпеченню національної безпеки та використанню відкритих джерел у сфері публічної безпеки. Так, Олексій Деревягін досліджує OSINT у правоохоронній діяльності з урахуванням міжнародного досвіду використання відкритих джерел у розслідуванні кіберзлочинів, терористичних актів і воєнних злочинів [9]. Р. Биба аналізує поняття OSINT у сфері публічного порядку та безпеки, підкреслюючи потребу в удосконаленні адміністративно-правового регулювання й понятійного апарату [10]. М. Тома та О. Василова розглядають інструменти OSINT у контексті фіксації воєнних злочинів в Україні [11].

Окремо слід зазначити праці, які стосуються інформаційно-аналітичного забезпечення діяльності поліції та кримінального аналізу. В. Маковій досліджує інформаційно-аналітичну підтримку діяльності поліції як складову забезпечення інформаційної безпеки держави [12]. Крім того, у сучасних українських дослідженнях OSINT пов'язується з реалізацією філософії Intelligence-Led Policing у системі кримінального аналізу Національної поліції України [13-17].

Водночас аналіз наукових джерел свідчить, що проблема саме верифікації синтетичних особистостей в умовах AI-контенту ще не отримала достатнього комплексного висвітлення в українській

правовій науці. Переважна частина досліджень зосереджена на загальних можливостях OSINT, використанні відкритих джерел у розслідуванні, фіксації воєнних злочинів або інформаційно-аналітичному забезпеченні поліції. Менш розробленими залишаються питання правової оцінки синтетичної цифрової ідентичності, критеріїв її виявлення, стандартів документування результатів OSINT-перевірки та меж доказового використання інформації, отриманої в умовах поширення AI-згенерованого контенту.

Метою статті є наукове обґрунтування проблеми верифікації синтетичних особистостей у правоохоронній діяльності в умовах поширення AI-контенту, а також визначення основних організаційно-правових і методологічних підходів до використання OSINT для перевірки достовірності цифрової ідентичності.

Для досягнення цієї мети необхідно вирішити такі завдання: по-перше, визначити сутність синтетичної особистості як об'єкта OSINT-аналізу; по-друге, охарактеризувати основні ризики використання AI-контенту для правоохоронної діяльності; по-третє, запропонувати логіку OSINT-верифікації синтетичних цифрових профілів; по-четверте, окреслити правові та організаційні умови допустимого використання результатів такої перевірки.

Синтетична особистість у контексті правоохоронної OSINT-аналітики може бути визначена як штучно створена або істотно модифікована цифрова ідентичність, що формується шляхом поєднання реальних, викрадених, вигаданих або AI-згенерованих даних з метою імітації існування конкретної особи у цифровому середовищі. На відміну від звичайного фейкового акаунта, синтетична особистість може мати більш складну структуру: стабільну цифрову історію, зображення, створені генеративними моделями, мережу контактів, публікації, коментарі, електронні адреси, телефонні номери, фінансові або професійні атрибути.

У правоохоронній діяльності такі профілі можуть використовуватися для вчинення шахрайства, збору інформації про потерпілих, підготовки кіберзлочинів, поширення дезінформації, дискредитації державних посадових осіб, приховування реального суб'єкта злочинної діяльності або створення фіктивного інформаційного сліду. Тому основною проблемою стає не сам факт існування відкритого джерела, а питання його достовірності, стабільності, походження та зв'язку з реальною особою.

Перше завдання OSINT у таких умовах полягає у встановленні ознак синтетичності цифрової ідентичності. До таких ознак можуть належати: відсутність природної історії цифрової активності; надмірно «ідеалізовані» або стилістично однотипні фотографії; невідповідність між датами створення профілю та заявленою біографією; штучна або шаблонна мовна поведінка; неприродна мережа контактів; відсутність незалежних підтверджень існування особи в інших джерелах; використання зображень, які мають ознаки генерації або маніпуляції; збіг елементів біографії з іншими підозрілими профілями.

Друге завдання полягає у багаторівневій верифікації цифрового профілю. Така перевірка не може обмежуватися одним джерелом або одним технічним інструментом. Доцільним є застосування поетапної моделі: первинна ідентифікація профілю; фіксація доступних даних; перевірка зображень і медіаконтенту; аналіз часової лінії активності; перевірка зв'язків; зіставлення з відкритими реєстрами та іншими незалежними джерелами; оцінка ризику синтетичності; документування результатів. Саме така логіка дає змогу перейти від інтуїтивної оцінки до структурованого аналітичного висновку.

Третє завдання пов'язане з розмежуванням технічної, аналітичної та процесуальної оцінки OSINT-результатів. Технічна оцінка дозволяє виявити ознаки AI-генерації або цифрової модифікації. Аналітична оцінка дає змогу визначити ймовірність того, що профіль є синтетичним або використовується для приховування реального суб'єкта. Процесуальна оцінка має значення тоді, коли результати OSINT можуть бути використані в кримінальному провадженні, для орієнтування слідства, формування версій, підготовки запитів, призначення експертиз або документування цифрових слідів.

Важливо підкреслити, що OSINT сам по собі не повинен підміняти процесуальне доказування. Його результати можуть бути цінними для виявлення джерел інформації, побудови слідчих версій, встановлення зв'язків, попередньої ідентифікації ризиків та орієнтування оперативної або слідчої діяльності. Проте у випадках, коли йдеться про доказове використання AI-контенту або висновків щодо синтетичної особистості, необхідними є належна фіксація, збереження цифрових слідів, документування часу доступу, джерела,

способу отримання інформації, технічних параметрів файлів, а за потреби – призначення відповідної експертизи.

Четверте завдання стосується організаційно-правового забезпечення такої діяльності. У межах Національної поліції України OSINT-верифікація синтетичних особистостей має розглядатися як частина ширшої інформаційно-аналітичної діяльності, що здійснюється виключно в межах законних повноважень. Стаття 25 Закону України «Про Національну поліцію» закріплює повноваження поліції у сфері інформаційно-аналітичного забезпечення, зокрема формування та використання інформаційних ресурсів для виконання завдань поліції [3, ст. 25]. Водночас використання OSINT має відповідати принципам законності, необхідності, пропорційності, захисту персональних даних і недопущення необґрунтованого втручання у приватне життя.

Окремого значення набуває підготовка правоохоронців до роботи з AI-контентом. Звичайні навички пошуку інформації у відкритих джерелах уже недостатні. Потрібна спеціалізована підготовка з аналізу діпфейків, синтетичних медіа, цифрової поведінки бот-мереж, виявлення AI-згенерованих зображень, оцінки достовірності цифрових біографій, а також правильного документування результатів. Національна поліція України вже використовує навчальні підходи, пов’язані з OSINT, протидією дезінформації та технологіями кримінального аналізу, що підтверджує практичну потребу у розвитку цього напряму.

З урахуванням викладеного OSINT в умовах AI-контенту має розглядатися не як допоміжний «пошуковий» інструмент, а як комплексна методологія перевірки цифрової реальності. Її сутність полягає у переході від простого накопичення відкритих даних до встановлення їх походження, автентичності, взаємозв’язку, стабільності та придатності для правоохоронного використання. Саме тому проблема синтетичних особистостей є не лише технологічною, а й правовою, організаційною та доказовою.

Проведений аналіз дає змогу сформулювати такі висновки.

Синтетична особистість є новим об’єктом правоохоронного OSINT-аналізу, оскільки поєднує ознаки фейкового акаунта, AI-згенерованого медіаконтенту, цифрової легенди та потенційного інструмента злочинної діяльності. Її небезпека полягає не лише у неправдивості окремих даних, а у створенні переконливої

цифрової ідентичності, здатної вводити в оману потерпілих, правоохоронців, установи та автоматизовані системи перевірки.

Основним завданням OSINT в умовах AI-контенту стає верифікація, а не лише пошук інформації. Правоохоронна аналітика має бути орієнтована на перевірку автентичності джерела, походження медіаконтенту, природності цифрової поведінки, реальності соціальних зв'язків і відповідності біографічних даних незалежним відкритим джерелам.

Результати OSINT-перевірки синтетичних особистостей потребують стандартизованого документування. Доцільним є запровадження внутрішніх методичних рекомендацій для підрозділів поліції щодо фіксації цифрових слідів, збереження копій сторінок, опису інструментів перевірки, зазначення часу доступу, джерел інформації та рівня достовірності встановлених даних.

Перспективним напрямом удосконалення правоохоронної діяльності є поєднання OSINT, кримінального аналізу та цифрової криміналістики. Такий підхід дозволить не лише ефективніше виявляти синтетичні особистості, а й забезпечувати належну якість інформаційно-аналітичних матеріалів, які можуть використовуватися для формування слідчих версій, оперативного реагування та подальшого процесуального закріплення доказів.

Список використаних джерел:

1. Steal, deal and repeat - How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025. European Union Agency for Law Enforcement Cooperation, 2025. 25 p.

2. Project SynthWave develops capabilities for law enforcement to detect AI-generated synthetic media and counter the threats posed by this technology. March 2025 – February 2026. URL: https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-SynthWave

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

4. 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

5. European union serious and organised crime threat assessment the changing dna of serious and organised crime. European Union

Agency for Law Enforcement Cooperation. UNODC, 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

6. Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia. Cybercrime Technical Brief Series. September 2025. 24 p. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf

7. Incident reporting. ENISA. 2025. URL: https://ciras.enisa.europa.eu

8. Weaponizing artificial intelligence: how ai reshapes the world of organized crime. European Union Agency for Law Enforcement Cooperation. Luxembourg: Publications Office of the European Union, 2025. 49 p. URL: https://www.expertisefrance.fr/ sites/ expertise/files/2026-02/eng_elpaccto2-weaponizingai_compress.pdf

9. Борисова К., Жмуровська К., Кришталь, Є., Деревягін О. OSINT у правоохоронній діяльності: міжнародний досвід та українські перспективи. *UNIVERSUM. №* 25. 2025. С. 205-210.

10. Риба Р.Ю. Поняття OSINT у сфері публічного порядку та безпеки. *Науковий вісник Ужгородського національного університету*. Серія: Право. Том 3 № 92. 2025. С. 38-43/

11. Василенко В.М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. *Вісник Кримінологічної асоціації України*. 2024. Т. 32, № 2. С. 945-958.

12. Маковій В.П., Усата Г.О. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави. *Морська безпека та оборона.* № 1. 2023. С. 62-68.

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

14. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113

15. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Бутко Р., Денисенко Б., Ісмайлов К.Ю. та ін., за заг. ред. Користіна О.Є. Київ: «ВАІТЕ», 2024. 444 с.

16. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2019. Одеса. 296 с.

17. Савенко Д.О., Ісмайлов К.Ю. OSINT та соціальні мережі: загрози та можливості для молодіжних комунікацій. *The 7th International scientific and practical conference «Sociological and psychological models of youth communication»* (February 18-21, 2025) Copenhagen, Denmark. International Science Group. 2025. с. 242-246.

OSINT В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ДІЯЛЬНОСТІ ОРГАНІВ ПРАВОПОРЯДКУ

Кардашевський Юрій Романович
доктор філософії у галузі права,
керівник відділу внутрішнього контролю НАЗК

В умовах глобалізації та інтенсивного розвитку цифрових технологій економічна безпека стала однією з найважливіших складових національної безпеки. Використання відкритих джерел інформації (OSINT) у системі економічної безпеки дозволяє органам правопорядку ефективно реагувати на нові виклики, що виникають у різних сферах економічної діяльності, таких як корупція, шахрайство, кіберзлочинність та інші форми економічних правопорушень. OSINT, завдяки своєму доступу до широкого кола публічних джерел, має значний потенціал у сфері розвідки та аналізу економічної ситуації, що допомагає органам правопорядку забезпечити стійкість економічної системи і протидіяти злочинним проявам в економічній сфері.

У той же час, OSINT в контексті економічної безпеки можна визначити як процес збору, аналізу та використання публічно доступної інформації, що стосується різних аспектів економічної діяльності, з метою забезпечення національної безпеки та економічної стабільності. Це може включати дані з фінансових звітів, публічних оголошень, корпоративних повідомлень, баз даних, соціальних мереж та медіа-ресурсів.

Завдяки використанню OSINT у сфері економічної безпеки, органи правопорядку отримують можливість:

– виявляти потенційно небезпечні економічні операції, у тому числі відмивання грошей, фінансування тероризму, шахрайство, контрабанду та інші види економічних злочинів;

– проводити моніторинг діяльності компаній та організацій, під час якого виявляти незаконні схеми або порушення фінансових правил;

– аналізувати макроекономічні показники, що дозволяє прогнозувати загрози для економічної безпеки, такі як економічні кризи, валютні спекуляції чи інші ризики, що можуть вплинути на стабільність національної економіки;

– використовувати дані для прогнозування злочинних дій, а також для попередження і своєчасного реагування на можливі загрози в економічному середовищі.

Процес збору економічних даних за допомогою OSINT є багатогранним і включає кілька основних етапів. Перш за все, потрібно чітко визначити, яку інформацію необхідно зібрати та для яких цілей вона буде використовуватися. Для цього важливо враховувати специфіку економічної безпеки і можливі загрози, з якими стикаються органи правопорядку.

Основні джерела даних для збору через OSINT включають:

– *публічні фінансові звіти та оголошення компаній*: компанії та організації публікують фінансові звіти, які містять інформацію про їхні доходи, витрати, активи та зобов'язання. Ці дані допомагають виявити аномалії або порушення, такі як маніпуляції з фінансами або непрозорі операції;

– *соціальні мережі та онлайн-платформи*: дані з таких платформ, як LinkedIn, Facebook, допомагають виявити зв’язки між підприємцями, політиками, банками, злочинними групами.

Аналіз публічних комунікацій дає можливість виявити не тільки зв'язки, але й схеми організації злочинної діяльності;

– *бази даних та реєстри*: державні реєстри та публічні бази даних, такі як реєстрація компаній, банківські звіти, реєстрація прав власності та інші, є важливим інструментом для перевірки законності діяльності підприємств та осіб, зокрема виявлення фальшивих компаній або підозрілих фінансових операцій;

– *медіа-ресурси*: новини, статті, прес-релізи та інші публікації в медіа часто містять інформацію про незаконні або сумнівні економічні операції. Зокрема, фінансові скандали, розслідування й аналітичні матеріали можуть дати важливі вказівки для розслідувань;

– *інтернет-форуми та платформи для обміну інформацією*: на різноманітних форумах і спеціалізованих платформах часто обговорюються нелегальні або сумнівні економічні практики, що може бути корисним для органів правопорядку при виявленні незаконної діяльності.

Для того, щоб зібрана інформація мала реальну цінність для правоохоронних органів, необхідно застосовувати методи аналізу та обробки даних. Зокрема, використання спеціалізованих інструментів для обробки великих обсягів даних (Big Data) допомагає виявляти патерни, тенденції та зв'язки між різними елементами інформації.

Однією з основних функцій OSINT у системі економічної безпеки є своєчасне виявлення потенційних загроз, які можуть призвести до порушень стабільності економічної системи. Це включає як прогнозування загроз, так і своєчасне реагування на них.

OSINT дозволяє:

– виявляти нелегальні фінансові операції, такі як відмивання грошей чи фінансування тероризму, аналізуючи фінансові потоки, транзакції та інші економічні дані;

– виявляти корупційні схеми, зокрема у державному секторі, завдяки моніторингу публічної інформації про діяльність державних службовців, контрактів, закупівель та інших економічних аспектів;

– виявляти й розслідувати шахрайські схеми в бізнесі, такі як фальшиві компанії, фіктивні фінансові операції, схемні інвестиції або маніпуляції на ринку цінних паперів;

– проводити моніторинг конкурентної діяльності, що дозволяє виявляти порушення антимонопольного законодавства або незаконні угоди між компаніями.

Завдячуючи інструментам OSINT можна не лише виявити загрози, але й прогнозувати їх, надаючи органам правопорядку час для реагування та вжиття заходів.

Хоча OSINT має великий потенціал, його використання в системі економічної безпеки не позбавлене низки проблем та викликів. Зокрема:

– *перевантаження інформацією*: великий обсяг даних, що надходить з відкритих джерел, може ускладнити процес аналізу та прийняття рішень. Важливо вміти фільтрувати корисну інформацію від неактуальних даних;

– *правові та етичні питання*: збір публічної інформації нерідко не супроводжується чіткими правовими межами, що може створити ризик для прав людини, зокрема порушення приватності. Важливо дотримуватися балансу між інтересами безпеки та правами громадян;

– *маніпуляції з інформацією*: дані з відкритих джерел можуть бути неповними або маніпульованими, що ставить перед органами правопорядку завдання з перевірки та верифікації цієї інформації;

– *кіберзагрози*: при зборі та обробці даних через інтернет існує ризик кіберзагроз, зокрема атак на системи збору даних, витоків інформації або хакерських атак.

Забезпечення безпеки є ключовим аспектом при використанні OSINT в економічній безпеці. Оскільки OSINT часто включає роботу з чутливою інформацією, необхідно впроваджувати низку заходів для захисту даних:

– *шифрування та захист каналів зв'язку* (для забезпечення безпеки передачі даних потрібно використовувати шифрування інформації та захищені канали зв’язку);

– *анонімність слідчих та аналітиків* (органи правопорядку повинні забезпечити анонімність своїх співробітників при зборі даних, щоб уникнути витоків або ризиків для особистої безпеки);

– *захист від кіберзагроз* (необхідно регулярно оновлювати програмне забезпечення та впроваджувати заходи для захисту від

кібератак, таких як впровадження фаєрволів і систем виявлення вторгнень).

Підсумовуючи вище зазначене, можна стверджувати, що OSINT відіграє важливу роль у системі економічної безпеки, надаючи органам правопорядку потужні інструменти для збору, аналізу та моніторингу економічної інформації з відкритих джерел. Це дозволяє ефективно боротися з економічною злочинністю, виявляти порушення і сприяти збереженню стабільності економічної системи. Однак для ефективного використання OSINT необхідно подолати численні виклики, пов'язані з великим обсягом інформації, правовими питаннями та забезпеченням безпеки. Розвиток інструментів і методологій OSINT, а також впровадження належних заходів безпеки, дозволять органам правопорядку покращити свою діяльність і досягти кращих результатів у забезпеченні економічної безпеки.

ІНТЕГРАЦІЯ МЕТОДІВ OSINT ТА СИСТЕМНОГО АНАЛІЗУ У ПРОЦЕСІ КРИМІНАЛЬНОГО АНАЛІЗУ КІБЕРІНЦИДЕНТІВ

Козленко Олександр Олександрович
кандидат юридичних наук, доцент

Сучасний етап розвитку інформаційного суспільства характеризується безпрецедентним рівнем цифровізації соціально-економічних процесів, трансформацією інформаційного середовища та стрімким розширенням кіберпростору як глобальної системи взаємодії державних інституцій, бізнес-структур, громадянського суспільства та окремих індивідів. Водночас зазначені процеси супроводжуються суттєвим зростанням кількості кіберзагроз, ускладненням механізмів реалізації кіберзлочинної діяльності та формуванням нових моделей функціонування транснаціональних кіберкримінальних угруповань. У сучасних умовах кіберзлочинність характеризується високим рівнем технологічної адаптивності, використанням засобів анонімізації, автоматизації атак, штучного інтелекту та розподілених інформаційних інфраструктур, що суттєво ускладнює процеси виявлення, ідентифікації та

аналізу кіберінцидентів у діяльності правоохоронних органів. За таких умов особливого значення набуває інтеграція сучасних інформаційно-аналітичних підходів, здатних забезпечити комплексне дослідження цифрового середовища, виявлення прихованих взаємозв'язків між суб'єктами кіберпростору та прогнозування потенційних загроз у сфері інформаційної безпеки [1,3].

Одним із найбільш перспективних напрямів розвитку сучасного кримінального аналізу є поєднання методів OSINT та системного аналізу у процесі дослідження кіберінцидентів. Використання відкритих джерел інформації у поєднанні із системними підходами до аналізу складних динамічних систем створює передумови для формування принципово нової моделі інформаційно-аналітичного забезпечення діяльності правоохоронних органів у сфері протидії кіберзлочинності. Особливість сучасного кіберпростору полягає у тому, що значна частина інформації про потенційні кіберзагрози, шкідливу активність, кіберзлочинні угруповання та механізми реалізації кібератак міститься у відкритих або умовно відкритих джерелах інформації, зокрема у соціальних мережах, тематичних форумах, цифрових медіа, телекомунікаційних платформах, ресурсах даркнету, відкритих базах даних та інформаційних репозиторіях. Аналіз зазначених інформаційних масивів дозволяє формувати комплексне уявлення про структуру кіберзагроз, встановлювати зв'язки між суб'єктами кіберзлочинної діяльності та прогнозувати можливі сценарії розвитку кіберінцидентів.

У сучасній науковій парадигмі OSINT розглядається не лише як технологія збору інформації з відкритих джерел, але і як комплексна система методів інтелектуального пошуку, верифікації, структуризації та аналітичної інтерпретації інформації, спрямована на формування нових знань для підтримки прийняття управлінських рішень. У сфері кримінального аналізу кіберінцидентів OSINT виступає важливим інструментом отримання оперативно значущої інформації про кіберзагрози, цифрові сліди злочинної діяльності, інфраструктуру кібератак, засоби анонімізації та механізми функціонування кіберзлочинних мереж. Використання OSINT-технологій дозволяє здійснювати моніторинг інформаційного простору у режимі реального часу, виявляти інформаційні аномалії, аналізувати поведінкові характеристики суб'єктів кіберпростору та формувати аналітичні моделі розвитку кіберзагроз.

Разом із тим, ефективність використання відкритих джерел інформації безпосередньо залежить від здатності аналітичних систем інтегрувати та інтерпретувати значні обсяги різнорідних даних. Саме тому інтеграція OSINT із методами системного аналізу набуває особливого значення у процесі кримінального аналізу кіберінцидентів. Системний аналіз дозволяє розглядати кіберпростір як складну багаторівневу систему взаємопов'язаних елементів, у межах якої кіберінцидент виступає результатом взаємодії великої кількості технічних, організаційних, соціальних та поведінкових факторів. Такий підхід забезпечує можливість комплексного дослідження причинно-наслідкових зв'язків між елементами інформаційного середовища, виявлення прихованих закономірностей функціонування кіберзлочинних структур та прогнозування можливих сценаріїв розвитку кіберзагроз [1].

У межах системного аналізу кіберінцидент може розглядатися як динамічний процес, що включає декілька взаємопов'язаних стадій, серед яких підготовка атаки, збір інформації про ціль, проникнення в інформаційну систему, закріплення у мережі, реалізація шкідливих дій, приховування слідів та подальша ескалація атаки. Аналіз кожного із зазначених етапів потребує використання комплексних аналітичних механізмів, здатних інтегрувати інформацію з різних джерел та забезпечити побудову цілісної картини кіберінциденту. Саме інтеграція методів OSINT та системного аналізу дозволяє реалізувати багаторівневий підхід до кримінального аналізу, у межах якого інформація про кіберінцидент розглядається не ізольовано, а як елемент складної системи інформаційних взаємодій.

Особливого значення набуває використання методів системного моделювання для дослідження структури кіберзлочинних мереж та механізмів їх функціонування. У сучасних умовах кіберзлочинність дедалі частіше реалізується у формі децентралізованих мережевих структур, які використовують механізми криптографічного захисту, анонімізації та розподіленого управління. Аналіз таких структур потребує застосування методів теорії графів, мережевого аналізу, когнітивного моделювання та системної динаміки. Інтеграція OSINT із зазначеними підходами дозволяє виявляти ключові вузли кіберзлочинних мереж, аналізувати інформаційні потоки, визначати центри координації атак та

встановлювати приховані взаємозв'язки між суб'єктами кіберпростору [3].

Важливим напрямом використання OSINT у процесі кримінального аналізу кіберінцидентів є дослідження інформаційної активності у соціальних мережах та цифрових комунікаційних платформах. Сучасні кіберзлочинні угруповання активно використовують соціальні мережі, месенджери, тематичні форуми та ресурси даркнету для координації діяльності, поширення шкідливого програмного забезпечення, обміну викраденими даними та здійснення інформаційно-психологічного впливу. Використання технологій OSINT дозволяє здійснювати автоматизований моніторинг зазначених ресурсів, аналізувати цифрову активність користувачів, виявляти ознаки підготовки кібератак та прогнозувати можливі напрями розвитку загроз. У поєднанні із системним аналізом зазначені технології забезпечують можливість побудови моделей інформаційної взаємодії між суб'єктами кіберпростору та прогнозування динаміки розвитку кіберінцидентів.

Особливу роль у процесі інтеграції OSINT та системного аналізу відіграють технології штучного інтелекту та інтелектуального аналізу даних. Використання алгоритмів машинного навчання дозволяє автоматизувати процеси збору, класифікації та інтерпретації інформації з відкритих джерел, а також забезпечити виявлення прихованих закономірностей у великих масивах цифрових даних. Сучасні методи Data Mining, Natural Language Processing та Deep Learning створюють передумови для автоматизованого аналізу текстової інформації, виявлення семантичних зв'язків між об'єктами, розпізнавання аномальної поведінки та прогнозування потенційних кіберзагроз. У межах кримінального аналізу зазначені технології дозволяють формувати інтелектуальні аналітичні системи, здатні здійснювати комплексний моніторинг кіберпростору та підтримку прийняття управлінських рішень у сфері протидії кіберзлочинності.

Водночас інтеграція OSINT та системного аналізу супроводжується низкою складних проблем методологічного, технологічного та правового характеру. Однією з ключових проблем є надмірна інформаційна насиченість сучасного цифрового середовища, що ускладнює процеси фільтрації, верифікації та інтерпретації даних. Значна кількість інформації у відкритих джерелах

характеризується низьким рівнем достовірності, наявністю маніпулятивного контенту, дезінформації та штучно сформованих інформаційних потоків. У таких умовах особливого значення набуває розроблення механізмів оцінювання достовірності інформації, автоматизованого виявлення фейкових повідомлень та верифікації цифрових слідів [1].

Не менш актуальною проблемою є забезпечення правового регулювання використання OSINT-технологій у діяльності правоохоронних органів. Використання відкритих джерел інформації нерідко пов'язане із питаннями захисту персональних даних, дотримання прав людини, забезпечення цифрової приватності та недопущення неправомірного втручання у приватне життя. У зв'язку з цим необхідним є формування комплексної нормативно-правової бази, яка б забезпечувала баланс між ефективністю інформаційно-аналітичної діяльності та дотриманням принципів законності, пропорційності та правової визначеності у сфері цифрової безпеки.

У сучасних умовах особливого значення набуває концепція проактивного кримінального аналізу кіберінцидентів, яка передбачає не лише дослідження вже реалізованих кібератак, але й прогнозування потенційних загроз та попередження їх виникнення. Реалізація зазначеного підходу є можливою саме завдяки інтеграції OSINT та системного аналізу, що забезпечує можливість комплексного дослідження інформаційного середовища, виявлення ранніх ознак кіберзагроз та моделювання потенційних сценаріїв розвитку кіберінцидентів. Використання предиктивних аналітичних моделей дозволяє формувати системи раннього попередження про кіберзагрози, оцінювати рівень ризиків та забезпечувати підтримку прийняття рішень у діяльності правоохоронних органів.

Перспективним напрямом подальшого розвитку інтеграції OSINT та системного аналізу є створення комплексних інформаційно-аналітичних платформ кримінального аналізу, здатних забезпечити автоматизовану інтеграцію даних із відкритих джерел, мережевих систем моніторингу, баз даних правоохоронних органів та міжнародних інформаційних ресурсів. Використання технологій Big Data, хмарних обчислень, інтелектуальних систем підтримки прийняття рішень та цифрових платформ ситуаційної обізнаності створює передумови для формування єдиного

інформаційного середовища кримінального аналізу кіберінцидентів. У межах такого середовища забезпечується автоматизоване виявлення загроз, побудова аналітичних профілів кіберзлочинних угруповань, прогнозування ризиків та координація діяльності суб'єктів забезпечення кібербезпеки [3].

Таким чином, інтеграція методів OSINT та системного аналізу у процесі кримінального аналізу кіберінцидентів виступає одним із найбільш перспективних напрямів розвитку сучасної системи інформаційно-аналітичного забезпечення діяльності правоохоронних органів у сфері кібербезпеки. Використання комплексних міждисциплінарних підходів дозволяє забезпечити ефективне виявлення, аналіз та прогнозування кіберзагроз, підвищити рівень ситуаційної обізнаності, удосконалити механізми підтримки прийняття управлінських рішень та забезпечити належний рівень протидії сучасним формам кіберзлочинності. Подальший розвиток зазначеного напряму потребує вдосконалення методологічних засад кримінального аналізу, розвитку інтелектуальних технологій обробки інформації, підготовки висококваліфікованих фахівців у сфері кримінального аналізу та кібербезпеки, а також інтеграції сучасних цифрових рішень у практичну діяльність правоохоронних органів України.

Список використаних джерел:

1. Панасюк В. В. Системний аналіз: Підручник. 2-е вид., перероб. і доп. Київ: ВПЦ «Київський університет», 2022. 448 с.
2. Гіренко О. В., Гіренко О. О., Кулик Н. С. Методологія системного аналізу та прогнозування ризиків // Вісник Київського національного торговельно-економічного університету. Серія «Економіка і управління». 2021. № 2. С. 12-20.
3. Гіренко О. В., Гіренко О. О., Кулик Н. С. Методи прогнозування ризиків у системному аналізі // Вісник Київського національного торговельно-економічного університету. Серія «Менеджмент». 2022. № 1. С. 23-30.

РОЛЬ І МІСЦЕ OSINT В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ, КЕРОВАНІЙ АНАЛІТИЧНОЮ РОЗВІДКОЮ (ILP)

Ковчі Атгіла Ласлович
прокурор управління процесуального керівництва досудовим розслідуванням та підтримання публічного обвинувачення Генеральної інспекції Офісу Генерального прокурора

У сучасному світі, де технології та інформація є основними рушіями соціально-економічного розвитку, правоохоронні органи стають залежними від інноваційних підходів до збору та аналізу даних. Одним з таких підходів є інтеграція розвідки з відкритих джерел (OSINT) в аналітичну розвідку, яка лежить в основі сучасної правоохоронної діяльності. Особливо актуальним цей підхід є в контексті інтеграції з так званою керованою аналітичною розвідкою (Intelligence-Led Policing, ILP), яка забезпечує ефективне управління інформацією та прийняття рішень на основі даних. В умовах, коли злочинність стає все більш складною та глобалізованою, роль OSINT в ILP стає незамінною.

Правоохоронна діяльність, керована аналітичною розвідкою (ILP), передбачає, перш за все, стратегічний менеджмент, що фокусується на аналізі та інтерпретації розвідувальних даних для прийняття рішень. Вона передбачає не лише оперативне реагування на злочини, але й націлену, проактивну роботу з прогнозування злочинної діяльності та запобігання її вчиненню. Підхід ILP забезпечує інтеграцію аналітичних даних з різних джерел для формування стратегії боротьби з злочинністю.

OSINT, або розвідка з відкритих джерел, — це процес збору, аналізу та використання публічно доступної інформації з Інтернету, медіа, публікацій, соціальних мереж, офіційних документів та інших джерел. Оскільки ця інформація доступна для широкої аудиторії, вона є важливим елементом у створенні повної картини для правоохоронних органів, особливо в межах аналітичної розвідки.

Інтеграція OSINT в ILP створює потужний інструмент для правоохоронних органів, що дозволяє не тільки швидко реагувати на події, але й прогнозувати майбутні злочини, зокрема організовані,

терористичні та кіберзлочини. Для ефективної роботи в цьому напрямку правоохоронні органи мають здатність обробляти великий обсяг даних, швидко виділяти важливу інформацію та використовувати її для прийняття оперативних рішень.

OSINT відіграє важливу роль у зборі інформації про злочинні групи, осіб, організації та події, що можуть вплинути на безпеку держави. Важливою особливістю OSINT є те, що він забезпечує доступ до величезних обсягів даних, які можуть бути використані для прогнозування злочинної діяльності, виявлення схем, зв'язків між злочинцями та їх діяльністю, а також для виявлення потенційних загроз.

У контексті ILP, OSINT може використовуватися для:

ідентифікації ключових осіб у злочинних організаціях або терористичних групах, їхніх зв'язків і місцезнаходжень;

моніторингу соціальних мереж для виявлення активності потенційних злочинців або терористів, що поширюють загрози або агітують за насильницькі дії;

аналізу публічно доступних даних для виявлення змін у схемах діяльності злочинців, таких як переміщення або зміна тактики.

Завдяки можливості збирати та аналізувати відкриту інформацію, правоохоронці можуть оперативно реагувати на зміни у поведінці злочинних елементів, що дозволяє зменшити час між виявленням загрози та її нейтралізацією.

Існує багато конкретних прикладів застосування OSINT у правоохоронній діяльності. Одним з них є виявлення потенційних загроз через соціальні мережі та інші відкриті джерела. Наприклад, використання технологій для моніторингу Twitter, Facebook та інших платформ дозволяє виявити осіб, які планують вчинення злочинів або, навпаки, вже активно залучені до кримінальної діяльності.

Ще одним важливим аспектом є використання OSINT для аналізу тенденцій злочинності та прогнозування її розвитку. Зібрані з відкритих джерел дані, такі як відомості про судові процеси, статистика злочинності та коментарі громадськості, дозволяють створювати моделі, які прогнозують найбільш ймовірні місця та типи злочинів у майбутньому.

Крім того, OSINT допомагає правоохоронним органам відслідковувати зміни у діяльності терористичних груп або злочинних організацій, виявляти нові стратегії та методи, що

використовуються для вчинення злочинів. Це дозволяє правоохоронцям адаптувати свої методи боротьби з новими викликами.

Для ефективного використання OSINT в рамках ILP правоохоронним органам необхідно володіти спеціалізованими інструментами та технологіями, які дозволяють збирати, обробляти та аналізувати великі обсяги даних з різних відкритих джерел. До таких інструментів відносяться:

платформи моніторингу соціальних мереж, які дозволяють відстежувати публікації, коментарі та інші взаємодії, що можуть свідчити про підготовку злочинів або терористичних актів.

інструменти аналізу великих даних (Big Data), які допомагають знаходити закономірності та взаємозв'язки між різними елементами даних, що зберігаються у відкритих джерелах;

машинне навчання та штучний інтелект, які дозволяють автоматизувати процеси аналізу та виявлення загроз у реальному часі;

системи геолокації для відстеження переміщення осіб чи об'єктів на основі публічних даних.

Ці інструменти надають правоохоронним органам можливість не лише швидко реагувати на злочинні дії, але й здійснювати їх прогнозування, що є важливим елементом аналітичної розвідки.

Хоча OSINT має величезний потенціал для застосування в ILP, існують певні виклики та обмеження, з якими стикаються правоохоронні органи при його використанні. Одним із головних викликів є *недосконалість технологій* збору та аналізу даних. Не всі доступні джерела є надійними, і існує великий ризик отримання недостовірної або неповної інформації.

Ще однією проблемою є *порушення прав людини*. Відкрита інформація з соціальних мереж і інших джерел може містити приватні дані, що можуть бути використані без згоди осіб, про яких йдеться. Це ставить під сумнів етичні та правові аспекти використання OSINT у правоохоронній діяльності.

З точки зору ILP, важливо забезпечити *правову визначеність* щодо того, які дані можуть бути використані, а також чітко визначити правила та процедури, за якими здійснюється збір і обробка інформації.

Інтеграція OSINT в ILP має величезний потенціал для розвитку правоохоронної діяльності. Перспективи цього процесу пов'язані з подальшим вдосконаленням технологій збору та обробки даних,

розвитку аналітичних платформ, а також з ростом співпраці між державними органами і приватним сектором, зокрема в частині надання технічних засобів для збору відкритих даних.

У майбутньому важливо зосередити увагу на розробці *етичних стандартів і правових норм* щодо використання OSINT в правоохоронній діяльності, що дозволить забезпечити баланс між ефективністю боротьби зі злочинністю та захистом прав і свобод громадян.

Отже, роль OSINT у правоохоронній діяльності, керованій аналітичною розвідкою (ILP), є критично важливою для ефективного управління інформацією та прийняття рішень на основі даних. Інтеграція відкритої розвідки з відкритих джерел в ILP дозволяє правоохоронним органам не лише швидко реагувати на злочини, але й прогнозувати їх, забезпечуючи більш проактивний підхід до боротьби зі злочинністю. Однак для повної реалізації потенціалу OSINT необхідно подолати технічні, правові та етичні виклики, що стоять на шляху його ефективного використання в правоохоронній діяльності.

ВИКОРИСТАННЯ OSINT ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ (THREAT INTELLIGENCE)

Лятушинська Анна
здобувачка вищої освіти
Інститут права та безпеки
Одеський державний університет внутрішніх справ
Науковий керівник: ***Грезіна Олена Миколаївна***
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

У сучасному цифровому середовищі кіберзагрози набувають дедалі складніших форм, а їх своєчасне виявлення стає критично важливим завданням для фахівців з інформаційної безпеки. Одним із найефективніших підходів до збору та аналізу даних про потенційні загрози є використання методології OSINT (Open Source Intelligence) — розвідки на основі відкритих джерел. Цей

підхід дозволяє організаціям отримувати актуальну інформацію про кіберзагрози без залучення закритих або платних баз даних, використовуючи лише загальнодоступні ресурси. За даними звіту ENISA Threat Landscape 2024, понад 60% виявлених індикаторів компрометації у корпоративних середовищах були отримані саме з відкритих джерел [1].

OSINT у контексті кібербезпеки охоплює широкий спектр джерел: відкриті репозиторії шкідливого програмного забезпечення (VirusTotal, MalwareBazaar), форуми та майданчики даркнету, стрічки загроз (threat feeds), соціальні мережі, технічні блоги дослідників безпеки, а також бази даних про вразливості — NVD та CVE. Усі ці джерела разом формують комплексну картину актуального ландшафту загроз. Процес збору розвідувальних даних (Threat Intelligence) охоплює кілька етапів: визначення цілей збору, моніторинг визначених джерел, нормалізацію зібраних даних у стандартизований формат STIX/TAXII та подальшу кореляцію для виявлення індикаторів компрометації (IoC) і тактик, технік та процедур (TTP) зловмисників згідно з матрицею MITRE ATT&CK [2].

Серед практичних інструментів OSINT для Threat Intelligence варто виділити кілька ключових платформ. Shodan і Censys дозволяють виявляти підключені до інтернету пристрої та інфраструктуру зловмисників. Платформа Maltego забезпечує візуалізацію зв'язків між суб'єктами загроз. MISP (Malware Information Sharing Platform) є відкритою системою для обміну IoC між організаціями, а OpenCTI дає змогу будувати граф знань про кіберзагрози на основі відкритих даних. Ресурси Abuse.ch, Threatfox та URLhaus публікують актуальні індикатори у відкритому доступі, що спрощує збагачення систем захисту реальними даними. Згідно з дослідженням Recorded Future 2025 року, організації, що інтегрували автоматизовані OSINT-потоки у свої SIEM-системи, скоротили середній час виявлення загроз на 34% порівняно з попереднім роком [3].

Важливим аспектом є моніторинг даркнету як джерела ранніх попереджень про майбутні атаки. Аналітики відстежують форуми та маркетплейси, де кіберзлочинці обговорюють плани, продають доступи до скомпрометованих систем або пропонують шкідливе програмне забезпечення. Такий проактивний підхід дозволяє

дізнатися про загрозу ще до її реалізації. Разом із тим моніторинг даркнету вимагає суворого дотримання правових норм, оскільки деякі дії навіть у дослідницьких цілях можуть порушувати законодавство. Цифова звітність Європолу за 2024 рік зафіксувала зростання кількості операцій з нейтралізації кіберзлочинців, де вирішальну роль відіграли дані, отримані саме через OSINT-моніторинг закритих форумів [4].

Значну роль у сучасному OSINT-аналізі відіграє автоматизація. Системи класу SOAR (Security Orchestration, Automation and Response) інтегрують потоки OSINT-даних із внутрішніми засобами захисту — SIEM, IDS/IPS, брандмауерами — та автоматично оновлюють правила блокування на основі отриманих індикаторів. Машинне навчання активно застосовується для класифікації загроз, визначення їх пріоритетності та відсіювання хибнопозитивних спрацювань серед великих масивів OSINT-даних. Дослідники з MIT Lincoln Laboratory у 2024 році продемонстрували, що моделі на основі графових нейронних мереж здатні автоматично виявляти кластери пов'язаних IoC у відкритих стрічках загроз із точністю понад 89%, що значно перевищує показники традиційних сигнатурних методів [5].

Попри очевидні переваги, OSINT-підхід має певні обмеження. Відкриті джерела можуть містити застарілі або навмисно хибні дані, які зловмисники розміщують для введення дослідників в оману. Крім того, обсяги даних, що підлягають обробці, є надзвичайно великими, тому без якісних інструментів фільтрації ефективність аналізу суттєво знижується. Результативність OSINT значною мірою залежить від кваліфікації аналітиків та їхнього вміння інтерпретувати зібрані дані в контексті конкретної організації. Отже, OSINT є потужним і доступним інструментом у системі Threat Intelligence, який дозволяє організаціям будь-якого масштабу проактивно виявляти кіберзагрози та формувати ситуаційну обізнаність щодо актуального ландшафту загроз. При грамотному застосуванні у поєднанні з автоматизацією та аналітичними платформами OSINT стає невід'ємною складовою зрілої стратегії кібербезпеки сучасної організації.

Список використаних джерел:

1. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity (ENISA). 2024. https://www.enisa.europa.eu/ publications/enisa-threat-landscape-2024

2. MITRE ATT&CK Framework v15. MITRE Corporation. 2024. https://attack.mitre.org/

3. Recorded Future. 2025 Threat Intelligence Report: Trends in Open Source Intelligence Integration. Recorded Future, 2025. URL: https://www.recordedfuture.com/research

4. Europol Internet Organised Crime Threat Assessment (IOCTA) 2024. Europol, 2024. URL: https://www.europol. europa.eu/ publications-events/publications/iocta-2024

5. Bowman B., Shi C., et al. Detecting Threat Intelligence IoC Clusters Using Graph Neural Networks // MIT Lincoln Laboratory Technical Report.

ЗАСТОСУВАННЯ ГРАФОВИХ АЛГОРИТМІВ ДЛЯ АВТОМАТИЧНОГО ВИЯВЛЕННЯ ЗВ'ЯЗКІВ МІЖ СУБ'ЄКТАМИ OSINT

Макаліш Богдан Дмитрович
курсант 2-го курсу навчально-наукового інституту № 4 підготовки фахівців з інформаційно-аналітичного забезпечення та кібербезпеки Національної поліції України Харківського національного університету внутрішніх справ
Кам'янський Ярослав Богданович
курсант 2-го курсу навчально-наукового інституту № 4 підготовки фахівців з інформаційно-аналітичного забезпечення та кібербезпеки Національної поліції України Харківського національного університету внутрішніх справ
Науковий керівник: ***Слободянюк Олександр Васильович***
кандидат технічних наук, доцент кафедри інформаційних систем та технологій навчально-наукового інституту № 4 підготовки фахівців з інформаційно-аналітичного забезпечення та кібербезпеки Національної поліції України Харківського національного університету внутрішніх справ

Сучасна OSINT-аналітика стикається з проблемою надлишку даних і ще більшої надлишковості зв'язків між ними. У відкритих джерелах одночасно існують домени, IP-адреси, криптогаманці, акаунти, телефони, витоки реєстраційних даних і метадані

цифрових слідів, які створюють заплутану мозаїку, де часто одне суперечить іншому. Ручний аналіз у таких умовах неминуче призводить до втрати непрямих зв'язків, які не видно при покроковій перевірці окремих об'єктів, але стають очевидними при переході до мережевого представлення даних. Саме тому графові алгоритми розглядаються як інструмент, щоб із великої кількості різнорідних даних побачити загальну картину зв'язків. Граф не дає готової відповіді - він лише робить приховані зв'язки видимими. [2].

Кожен зв'язок може також включати джерело походження, і рівень достовірності, щоб уникнути змішування достовірної та сумнівної інформації в одній структурі [1]. Навіть з однієї маленької зачіпки можна розкрутити цілу мережу за допомогою так званих «pivot-зв'язків», що збільшує його розмір до повноцінної мережі взаємопов'язаних елементів інфраструктури, часто за короткий проміжок часу — від одного домену чи одного користувача до іншого [3].

Графи виявляють те, що при ручному аналізі залишається невидимим. Наприклад, під час аналізу дезінформаційних мереж у соціальних платформах часто буває так, коли окремі акаунти не мають прямих зв'язків, але діють синхронно, публікують схожий контент або згадують один одного. У графовій моделі такі характеристики перетворюються на структурні зв'язки, що формують кластери взаємопов'язаних вузлів [3].

PageRank є корисним в інформаційних мережах, де цінність вузла не обов'язково корелює з кількістю прямих посилань на нього. Цей алгоритм використовується для виявлення вузлів із найбільшим впливом. Центральність посередництва допомагає знайти ті вузли, через які проходить максимальна кількість шляхів між іншими вузлами в мережі; в аналітичній практиці вони часто пов'язані з учасниками, які виступають як хаби або посередники в інфраструктурі, що координує дії в мережі, – відомими як «координатори».

Для базової оцінки важливості вузлів у мережі може використовуватися метрика ступеня центральності (Degree Centrality), яка демонструє кількість прямих зв'язків об'єкта з іншими елементами мережі [1, 2]:

$$C_D(v) = \frac{deg\ (v)}{n-1}$$

де $deg(v)$ – кількість зв’язків конкретного вузла, а n – загальна кількість вузлів у мережі. Простими словами, у контексті OSINT-розслідувань, чим більше виявлених зв'язків має об'єкт, тим вищою є його потенційна значущість для подальшого аналізу [2].

Таблиця 1

Аналітична інтерпретація графових алгоритмів

Алгоритм	**Аналітичне значення**	**Практичне застосування в OSINT**
PageRank	Рівень структурного впливу	Виявлення ключових акаунтів або доменів
Betweenness Centrality	Посередництво у зв’язках	Координатори мереж або інфраструктурні вузли
Louvain / Leiden	Виявлення кластерів	Групи акаунтів або організаційні структури
BFS (Shortest Path)	Найкоротший шлях між вузлами	Встановлення непрямих зв’язків між суб’єктами
Link Prediction	Ймовірні приховані зв’язки	Виявлення невідомих зв’язків між сутностями
Temporal Analysis	Зміна структури у часі	Виявлення активації або згортання мереж

Алгоритми виявлення спільнот, зокрема Louvain і Leiden, працюють найкраще, коли ми заздалегідь не знаємо, як побудована мережа. Вони дозволяють автоматично розділяти граф на щільно зв’язані підмножини, які часто відповідають реальним організаційним або інформаційним групам. На практиці, коли працюємо з OSINT, це допомагає розрізняти ізольовані інформаційні кластери.[6].

Практичний приклад застосування графового підходу було реалізовано нами під час аналізу інформаційних мереж Telegram-екосистеми. Для цього ми побудували тестовий граф у середовищі Neo4j на основі вибірки з 50 Telegram-каналів, що висвітлювали події під час воєнного стану. Зв’язок між каналами визначався за наявності щонайменше двох спільних ознак: взаємних згадок, повторюваних посилань, спільних адміністраторів або синхронної публікації контенту в близькому часовому проміжку. Цей підхід дозволив зменшити кількість випадкових збігів і краще відокремити стійкі інформаційні зв’язки.

Будуючи граф та враховуючи взаємні згадки, спільних адмінів і одночасні пости, вдалося виділити ядро мережі, яке виконувало функцію генерації контенту, тоді як периферійні вузли виступали ретрансляторами. Наприклад, частина каналів демонструвала майже одночасну появу однакових повідомлень із різницею в декілька хвилин, що вказувало не на випадковий збіг, а на можливу координацію або використання єдиного джерела контенту. Візуалізована структура чітко проявляється як щільний кластер із високою внутрішньою зв'язаністю та слабкими зовнішніми зв'язками (рис. 1) [3].

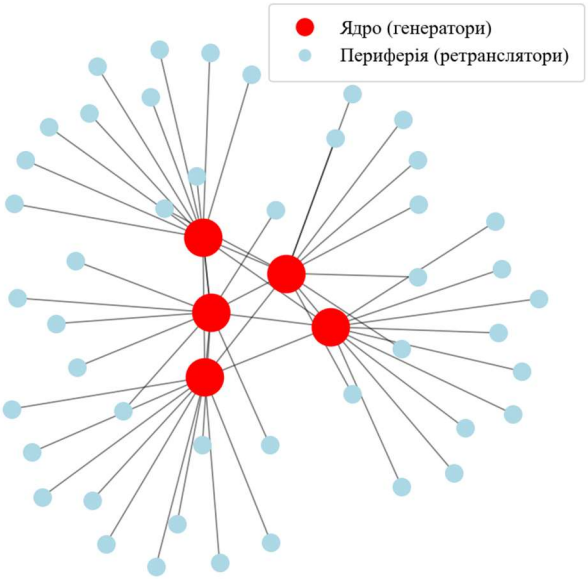

Рис. 1. Графова модель взаємодії Telegram-каналів (ядро генерації контенту та вузли-ретранслятори).

Окрему роль у сучасному OSINT відіграє Link Prediction, який дозволяє оцінювати ймовірність існування зв'язку між двома вузлами на основі їхнього оточення в графі. Це критично там, де прямого цифрового сліду немає, але структурна подібність свідчить про потенційну взаємодію. У таких задачах використовуються підходи на основі статистичних індексів подібності або графових нейронних мереж, що дозволяє формувати

обґрунтовані припущення щодо потенційних зв’язків між сутностями, які надалі потребують додаткової перевірки [5].

Технічна реалізація графових OSINT-систем базується на використанні спеціалізованих інструментів. Для зберігання та обробки даних застосовуються графові бази даних, зокрема Neo4j, які справляються з великими обсягами даних і дають змогу робити складні запити досить швидко. На відміну від реляційних БД, вони орієнтовані саме на зв'язки, а не на окремі записи. Аналітичні операції реалізуються через Graph Data Science Library або бібліотеки Python, такі як NetworkX. У випадках потокового аналізу використовуються системи, що підтримують real-time обробку графів[4].

Процес формування графа зазвичай відбувається через послідовність pivot-операцій. Початковий об’єкт, наприклад IP-адреса, дозволяє отримати домени, пов’язані з нею через WHOIS-записи. Далі ці домени можуть вести до SSL-сертифікатів, а вони вже ведуть до інших IP-адрес чи елементів інфраструктури. Так крок за кроком будується багаторівнева мережа [1].

Графові системи стабільно працюють із багатоглибинними зв'язками там, де реляційні БД ”сідають” по швидкості на рекурсивних запитах. Тому вони краще підходять для роботи зі складними OSINT-даними, де кількість проміжних вузлів може бути значною [2].

Водночас існують суттєві обмеження, пов’язані з якістю вихідних даних. Shared hosting, VPN-інфраструктура та повторне використання IP-адрес можуть створювати хибні зв’язки між незалежними сутностями. У соціальних мережах те саме відбувається з ботами або масовими акаунтами, які імітують поведінку реальних користувачів. У таких умовах критично важливим стає використання зважених ребер, де кожен зв’язок має рівень достовірності, що знижує ризик хибних висновків.

Наприклад, спільна IP-адреса сама по собі не завжди означає реальний зв’язок між суб’єктами, оскільки одна інфраструктура може використовуватися сотнями незалежних ресурсів. Саме тому підтвердження зв’язку через кілька незалежних джерел є критично важливим етапом аналізу [1].

Для зменшення кількості хибних зв’язків у графі доцільно використовувати вагу ребра, яка враховує рівень довіри до джерела та кількість підтверджень зв’язку [1]:

$$W(e) = \sum_{i=1}^{n} c_i$$

де $W(e)$ — загальна вага зв'язку, а c_i — рівень достовірності окремого джерела або підтвердження. Наприклад, якщо однаковий зв'язок підтверджується одночасно через WHOIS-запис, витік даних і профіль у соцмережі, його надійність суттєво зростає [1].

Темпоральний аналіз дозволяє відстежувати, як структура мережі змінюється з часом. Це важливо, коли потрібно зафіксувати момент активації кластера - наприклад, коли раніше слабко пов'язані канали раптово починають синхронно поширювати контент. Граф перестає бути статичним знімком і перетворюється на інструмент спостереження за розвитком мережі.

У підсумку графові алгоритми в OSINT дозволяють переходити від окремих фрагментів інформації до розуміння цілісної структури взаємозв'язків між об'єктами. Це не замінює роботу аналітика, однак суттєво скорочує час пошуку зв'язків і дозволяє швидше виявляти приховані закономірності, які складно помітити під час ручного аналізу.

Список використаних джерел:

1. Сулейманов С.-Б., Рибачок Д. Масштабований аналіз мережевих структур на основі комп'ютерно математичних моделей. *Наука і техніка сьогодні*.2026.№2(56).URL: https://doi.org/10.52058/2786-6025-2026-2(56)-2253-2262

2. Newman M. E. J. Networks: An Introduction. Oxford University Press, 2018. URL: https://doi.org/10.1093/oso/ 9780198 805090.003.0001

3. Bellingcat. Cross-platform network analysis in OSINT investigations. URL: https://lnk.ua/Q8Vi0R7Ng

4. Neo4j Documentation. Graph Data Science Library. https://neo4j.com/docs/graph-data-science/

5. RAND Corporation. Research on Open-Source Intelligence (OSINT) and all-source intelligence integration (RR1964, RRA314 series). URL: https://www.rand.org/pubs/research_reports/RRA314-1.html

6. Traag V. A., Waltman L., van Eck N. J. From Louvain to Leiden: guaranteeing well-connected communities. Scientific Reports. 2019. T. 9, №1. URL: https://doi.org/10.1038/s41598-019-41695-z

ІНСТРУМЕНТИ, МЕТОДИ ТА АЛГОРИТМИ ЗАСТОСУВАННЯ OSINT В АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ

Максімов Тарас Юрійович
начальник відділу кримінального аналізу головного оперативно-розшукового відділу 17 прикордонного загону ім. полковника Олександра Жуковського

Вступ.

Сучасний етап розвитку інформаційного суспільства характеризується активною цифровізацією суспільних процесів, стрімким поширенням соціальних мереж, функціонуванням відкритих державних реєстрів, електронних архівів та картографічних сервісів, що зумовлює підвищення ролі розвідки з відкритих джерел (OSINT) у системі інформаційно-аналітичного забезпечення. За таких умов практична цінність OSINT полягає у можливості оперативного виявлення, збирання, перевірки, систематизації, зіставлення та узагальнення публічно доступної інформації з метою підтримки управлінських, правоохоронних і безпекових рішень.

Застосування методів OSINT забезпечує можливість отримання актуальних відомостей, встановлення взаємозв'язків між об'єктами дослідження, перевірки достовірності інформації, документування подій, а також формування обґрунтованих аналітичних висновків, придатних для практичного використання у правоохоронній та безпековій діяльності.

У наукових, навчально-методичних і прикладних джерелах OSINT визначається як діяльність, спрямована на збирання, оцінювання, аналіз та використання інформації з відкритих джерел для отримання відповіді на конкретне аналітичне запитання [1–6]. У зв'язку з цим OSINT дедалі активніше використовується як інструмент інформаційно-аналітичного забезпечення діяльності правоохоронних органів, суб'єктів сектору безпеки і оборони, а також органів державної влади.

Теоретичні засади.

Сутність OSINT доцільно розглядати не як звичайний пошук інформації у мережі Інтернет, а як комплексний та системний процес збирання, обробки, верифікації й аналізу відомостей з відкритих джерел. Такий процес охоплює дослідження соціальних

мереж, вебсередовища, геопросторових даних, цифрових слідів, метаданих, відкритих державних реєстрів, фото- та відеоматеріалів, а також інших видів публічно доступної інформації.

Зазначений підхід дає змогу розглядати OSINT як важливу складову інформаційно-аналітичного забезпечення правоохоронної діяльності та кримінального аналізу. Використання відкритих джерел інформації забезпечує можливість встановлення зв'язків між особами та суб'єктами господарювання, перевірки достовірності фактів, документування подій, аналізу цифрової присутності об'єктів дослідження, а також формування аналітичного продукту, придатного для практичного застосування [1; 2].

Методи та алгоритм застосування.

Методично правильне застосування OSINT передбачає реалізацію послідовного алгоритму дій, спрямованого на отримання, перевірку та аналітичне опрацювання інформації з відкритих джерел. На початковому етапі формується аналітичний запит та визначається об'єкт дослідження, яким можуть виступати особа, суб'єкт господарювання, адреса, цифровий профіль, подія або геолокація. Після цього встановлюються вихідні ідентифікатори, зокрема прізвище та ім'я, номер телефону, адреса електронної пошти, ім'я користувача, код суб'єкта, адреса або зображення.

Наступним етапом є систематичний збір даних, їх верифікація, зіставлення та подальше аналітичне опрацювання. Завершальним етапом виступає оформлення результатів дослідження у вигляді довідки, профілю об'єкта, схеми зв'язків або іншого аналітичного документа, придатного для практичного використання [1; 2].

На всіх етапах проведення OSINT-дослідження мають забезпечуватися дотримання принципів законності, пропорційності, перевірюваності, відтворюваності результатів та належної фіксації джерел інформації.

Інструменти OSINT.

Сучасні засоби OSINT охоплюють широкий спектр спеціалізованих ресурсів і платформ, призначених для збору, перевірки, систематизації та аналітичного опрацювання інформації з відкритих джерел. Залежно від функціонального призначення окремі інструменти використовуються для дослідження корпоративних зв'язків, цифрової ідентифікації осіб, аналізу геопросторових

даних, обробки великих масивів інформації та встановлення транскордонних економічних взаємозв'язків.

YouControl та Sayari доцільно розглядати як комплексні інструменти для проведення OSINT-досліджень. YouControl використовується для перевірки суб'єктів господарювання, бенефіціарів, контрагентів, корпоративних змін і зв'язків між суб'єктами на основі відкритих офіційних джерел [5]. Sayari забезпечує можливість дослідження міжнародних корпоративних і торговельних зв'язків, встановлення бенефіціарної структури, перевірки ризикових контрагентів та аналізу транскордонних економічних зв'язків [9]. У поєднанні ці інструменти дають змогу формувати цілісну аналітичну картину як на національному, так і на міжнародному рівнях.

OSINT Industries використовується для цифрової ідентифікації особи або профілю шляхом пошуку за номером телефону, адресою електронної пошти, іменем користувача та іншими цифровими ідентифікаторами [6]. Clearview AI є спеціалізованим інструментом пошуку за зображенням обличчя, який може застосовуватися для встановлення осіб за фотоматеріалами, однак його використання пов'язане з підвищеними ризиками втручання у приватність та потребує особливо виваженого правового й етичного підходу [7].

Artellence доцільно розглядати як інструмент для аналізу значних масивів відкритих даних та автоматизації окремих аналітичних процесів пов'язаних з активністю користувачів у соціальних мережах [8]. SeaVision є спеціалізованим веборієнтованим ресурсом для відображення суден на карті, перегляду історії їх переміщення та підвищення рівня морської ситуаційної обізнаності. У ширшому аналітичному контексті цей інструмент демонструє значення геопросторового та транспортного напрямів відкритої аналітики [10].

Навігаційні ресурси та навчальна база.

Окреме значення у сфері OSINT має ресурс The Ultimate OSINT Collection на платформі Start.me, який являє собою структуровану добірку інструментів, книг, методичних матеріалів, навчальних програм і тематичних підбірок. Практична цінність зазначеного ресурсу полягає не у проведенні дослідження замість аналітика, а у систематизації засобів OSINT та скороченні часу на

пошук релевантних ресурсів для виконання конкретних практичних завдань [11].

Відомчі напрацювання Державної прикордонної служби України.

Особливої уваги заслуговує розроблений Державною прикордонною службою України сервіс osint-tools.platypus.ink, призначений для збору, систематизації та узагальнення відомих OSINT-інструментів. Практичне значення зазначеного ресурсу полягає у формуванні зручного навігаційного середовища для аналітичної роботи, у межах якого інструменти згруповано за категоріями та напрямами використання. Це забезпечує можливість оперативного добору необхідних засобів залежно від поставленого завдання, зокрема для пошуку осіб, аналізу цифрових слідів, роботи з документами, архівами, вебсередовищем, геоданими та іншими видами відкритої інформації [12].

Крім того, у відомстві розроблено комплексний аналітичний агрегатор, який забезпечує можливість оперативного опрацювання та аналізу значних масивів інформації, у тому числі відомостей із державних реєстрів, із подальшим поданням результатів у зручному для аналітичної роботи форматі.

Додатково слід зазначити, що Державна прикордонна служба України системно розвиває спроможності у сфері OSINT. Про це свідчать профільні тренінги щодо використання OSINT-засобів, а також участь команди кримінальних аналітиків служби у національному OSINT-хакатоні. Зазначене свідчить про поступове впровадження OSINT у діяльність правоохоронних органів та сектору безпеки.

Проблематика.

Разом із тим сучасні можливості OSINT не усувають наявних правових і методичних проблем. Наукові джерела акцентують увагу на ризиках деанонімізації особи, втручання у приватність, неправильного тлумачення відкритих даних, виникнення інформаційного шуму та помилкового встановлення зв'язків між суб'єктами [2; 3]. Саме тому результати OSINT-досліджень не повинні сприйматися автоматично як безумовно достовірні. Отримані відомості мають бути перевірені за допомогою кількох незалежних джерел, належним чином зафіксовані та оформлені з урахуванням вимог кримінального процесуального законодавства [1; 13–15].

Особливо актуальною залишається проблема відсутності в Україні єдиної державної інтегрованої платформи для проведення OSINT-досліджень у діяльності правоохоронних органів. Наразі аналітики та оперативні працівники використовують окремі приватні сервіси, відкриті інструменти, державні реєстри, навчальні платформи та довідкові ресурси, які не формують єдиного захищеного інформаційного середовища. Це створює ризики фрагментарності, неоднаковості підходів, залежності від сторонніх постачальників та ускладнює подальшу процесуальну легалізацію отриманих результатів.

У зв'язку з цим перспективним напрямом розвитку має стати інтеграція відкритих джерел, державних реєстрів, засобів аналітики зв'язків, геопросторового аналізу, журналювання дій користувача та формування звітності в межах єдиного державного ліцензованого середовища.

Пропозиції.

Перспективним напрямом розвитку OSINT у діяльності правоохоронних органів має стати створення єдиної державної інтегрованої платформи для проведення OSINT-досліджень із забезпеченням її інтеграції з державними реєстрами та засобами аналітики зв'язків. Важливе значення також має впровадження обов'язкової фіксації дій користувача та збереження цифрового сліду дослідження. Окремої уваги потребують розроблення стандартизованих методичних рекомендацій щодо проведення OSINT-досліджень і продовження системної підготовки аналітиків, слідчих та прокурорів у сфері використання OSINT-засобів. Наявність сервісу osint-tools.platypus.ink та комплексного аналітичного агрегатора свідчить про наявність в Україні практичного підґрунтя для подальшого формування єдиної державної системи OSINT-забезпечення правоохоронної діяльності.

Висновки.

Отже, OSINT є важливою складовою сучасної інформаційно-аналітичної діяльності. Ефективність його застосування визначається не кількістю використаних інструментів, а правильністю алгоритму їх застосування, здатністю перевіряти інформацію, критично оцінювати джерела та належним чином документувати результати дослідження. Використання таких ресурсів, як YouControl, Sayari, Artellence, OSINT Industries, Clearview AI,

Start.me та osint-tools.platypus.ink, суттєво розширює можливості аналітичної роботи, однак не замінює необхідності дотримання правових гарантій і методичної дисципліни. Ключовим напрямом подальшого розвитку має стати створення в Україні єдиної державної інтегрованої платформи, результати функціонування якої можуть бути використані як джерело цифрових доказів у межах кримінального провадження.

Ключові слова: OSINT, аналітична діяльність, відкриті джерела, кримінальний аналіз, цифрові докази, державні реєстри, правоохоронна діяльність.

Список використаних джерел:

1. Користін О. Є., Демедюк С. В. та ін. OSINT Open Source Intelligence. Інструменти та методи : навчальний посібник. Київ : 7БЦ, 2025. 460 с. DOI: 10.32782/osint-instruments-2025. ISBN 978-617-8794-17-0.

2. Главацька А. Л., Ангельська О. В., Опірський І. Р. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі // Кібербезпека: освіта, наука, техніка. 2024. № 1 (25). DOI: 10.28925/2663-4023.2024.25.1950.

3. Жарков Я. М., Васильєва А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 38–41.

4. Gill R. What is Open-Source Intelligence? // SANS Institute.

5. About YouControl // офіційний сайт YouControl.

6. OSINT Industries | Powerful Tools for Online Investigations // офіційний сайт OSINT Industries.

7. Clearview AI | Criminal Investigations; Clearview AI | Principles // офіційний сайт Clearview AI.

8. Artellence // офіційний сайт.

9. Overview | Sayari | Docs; About Sayari // офіційний сайт Sayari.

10. SeaVision Improves Africa's Maritime Picture // Volpe National Transportation Systems Center.

11. The Ultimate OSINT Collection // Start.me.

12. Osint Tools // osint-tools.platypus.ink.

13. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI.

14. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова Кабінету Міністрів України від 21.10.2015 № 835.

15. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.

OSINT У ПРОЦЕСАХ КІБЕРРОЗВІДКИ (CYBER THREAT INTELLIGENCE, CTI)

Никитенко Альбіна
здобувачка вищої освіти Інститут права та безпеки
Одеський державний університет внутрішніх справ
*Науковий керівник**: Грезіна Олена Миколаївна***
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

OSINT— розвідка на основі відкритих джерел — це методологія збору, обробки та аналізу загальнодоступної інформації з метою отримання розвідувальних даних [1]. OSINT охоплює пошук інформації, її реєстрацію, облік та аналіз, аналітико-синтетичну переробку первинної інформації та забезпечення безпеки інформаційних результатів.

У контексті Cyber Threat Intelligence (CTI) — кіберрозвідки загроз — OSINT є одним із ключових інструментів, що дозволяє організаціям виявляти, аналізувати та нейтралізувати потенційні кіберзагрози превентивно. CTI охоплює процеси збору даних про актуальні та потенційні кіберзагрози, тактики, техніки й процедури (TTP) зловмисників, а також відстеження відомих загрозливих акторів. OSINT забезпечує основу для цих процесів, оскільки значна частина розвідувальної інформації є публічно доступною [2].

У межах CTI фахівці використовують широкий спектр відкритих джерел. Технічні ресурси включають бази даних вразливостей (CVE, NVD), платформи індикаторів компрометації (IOC), репозиторії зловмисного програмного забезпечення (VirusTotal, MalwareBazaar), а також пошукові системи для виявлення

вразливих пристроїв (Shodan, Censys). Соціальні й комунікаційні джерела охоплюють форуми даркнету, Telegram-канали та спеціалізовані спільноти, де учасники обговорюють нові атаки, інструменти та вразливості [3].

В українському контексті важливу роль відіграє CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події України, яка публікує відкриті бюлетені про кіберактивність APT-груп (зокрема UAC-0001/APT28, UAC-0200), індикатори компрометації та рекомендації щодо захисту. Ці звіти є цінним публічним джерелом OSINT для аналітиків CTI [5]. Пасивна розвідка DNS, WHOIS-запити, аналіз сертифікатів SSL/TLS та метаданих документів дозволяють встановлювати інфраструктуру зловмисників [2].

Цикл кіберрозвідки складається з планування, збору, обробки, аналізу, поширення та зворотного зв'язку. OSINT інтегрується на кожному етапі: під час збору формуються автоматизовані фіди загроз; на етапі аналізу проводиться кореляція індикаторів компрометації з відомими кампаніями та атрибуція атак конкретним групам. Як зазначає сертифікований інструктор ISSP Training Center Юрій Самохвалов, навіть інформацію з відкритих джерел зловмисники активно використовують для планування атак, що зобов'язує захисників так само системно моніторити ці ж джерела [5].

Практичним прикладом у вітчизняному контексті є моніторинг фішингових кампаній через відстеження нещодавно зареєстрованих доменів. Аналітики CTI відстежують домени, що імітують легітимні організації, ще до початку атаки. Аналогічно, відстеження активності у підпільних форумах і Telegram-каналах дозволяє завчасно виявляти оголошення про продаж вкрадених облікових даних або доступу до корпоративних мереж. Такі платформи, як MISP та OpenCTI, дозволяють агрегувати та візуалізувати дані з множини OSINT-джерел [3].

Незважаючи на широкі можливості, OSINT у CTI має суттєві обмеження. У науковій статті Легомінової С. та ін. зазначається, що організації не можуть повністю запобігти збору даних про себе з відкритих джерел, однак зобов'язані бути готовими до протидії наслідкам такого збору [3]. Ключовою проблемою є значний обсяг інформаційного шуму — більшість зібраних даних потребує ретельної фільтрації та верифікації. Існують також правові та етичні ризики, пов'язані зі збором даних у «сірих зонах» мережі.

Атрибуція атак на основі лише відкритих джерел може бути хибною через використання техніки false-flag, коли зловмисники навмисно залишають сліди, що вказують на інших акторів [2].

OSINT є невід'ємною складовою сучасної кіберрозвідки, забезпечуючи аналітиків CTI критичними даними про загрози, актори та інфраструктуру зловмисників. Відкриті звіти CERT-UA, публікації дослідницьких платформ, дані з форумів та технічних реєстрів у сукупності формують потужну розвідувальну базу. Ефективне застосування методів OSINT дозволяє організаціям перейти від реактивного до проактивного підходу в кібербезпеці – виявляти загрози раніше, ніж вони завдадуть реальної шкоди [4;5].

Список використаних джерел:

1. Дрижакова Д., Волинець Р. Використання відкритих джерел інформації(OSINT) у сфері безпеки держави: технології та перспективи. Матеріали конференцій МЦНД. Дніпро, 2025. С. 138–141. URL: https://archives.mcnd.org.ua/index.php/conference-proceeding / article/view/599

2. Легомінова С., Щавінський Ю., Рабчун Д., Запорожченко М.,Будзинський О. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації.*Кібербезпека: освіта, наука, техніка*.2024. № 1(25). С. 294–303. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/630

3. Кіберрозвідка (I-OSINT CR): програма навчання. ISSP Training Center. URL: https://www.issp.training/programs/i-osint-cr

4. CERT-UA — Урядова команда реагування на комп'ютерні надзвичайніподії України. Звіти про кіберінциденти та бюлетені безпеки. URL: https://cert.gov.ua

5. Самохвалов Ю. Як працює OSINT-розвідка? Від бізнес-аналізу дооборони України.ISSP Training Center.2022. URL: https://www.issp.trai ning/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny

ВИКОРИСТАННЯ ПОШУКОВИХ ОПЕРАТОРІВ (GOOGLE DORKS) В OSINT

Прутяну Дарія Сергіївна
здобувачка вищої освіти Інститут права та безпеки
Одеський державний університет внутрішніх справ
Науковий керівник: ***Грезіна Олена Миколаївна***
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

У сучасному цифровому середовищі інформація стала одним із найцінніших ресурсів. Значна її частина перебуває у відкритому доступі, що дає можливість використовувати її для аналітики, досліджень та безпеки. Саме на цьому базується концепція OSINT (Open Source Intelligence) — розвідки на основі відкритих джерел. OSINT передбачає збір і аналіз інформації з публічно доступних ресурсів, таких як вебсайти, соціальні мережі, новини та офіційні документи. Одним із ключових інструментів у цьому процесі є використання розширених можливостей пошукових систем, зокрема спеціальних операторів пошуку, відомих як Google Dorks [2].

Google Dorks — це спеціальні пошукові запити, які дозволяють значно звузити результати пошуку та знайти саме ту інформацію, яка є необхідною. Вони не є інструментом злому, а лише способом більш ефективного використання пошукової системи.

До основних операторів належать:

- site: — дозволяє здійснювати пошук у межах конкретного сайту;
- filetype: — використовується для пошуку файлів певного формату (наприклад, PDF або DOCX);
- intitle: — знаходить сторінки з певними словами у заголовку;
- inurl: — дозволяє шукати сторінки за частиною URL-адреси;
- лапки ("") — використовуються для точного пошуку фрази.

Комбінування цих операторів відкриває значні можливості для аналітиків. Наприклад, можна знайти офіційні документи організацій, які не відображаються у звичайному пошуку, або виявити структуру вебресурсу.

У сфері OSINT такі методи застосовуються для збору даних про компанії, дослідження інформаційного простору, перевірки фактів, а також у журналістських розслідуваннях. Це дозволяє отримати більш повну картину без використання закритих або незаконних джерел.

Водночас важливо дотримуватися етичних норм. Використання пошукових операторів має здійснюватися виключно в межах закону. Недопустимо використовувати знайдену інформацію для порушення конфіденційності або завдання шкоди.

Серед переваг використання Google Dorks можна виділити високу швидкість пошуку, безкоштовність та значну точність отриманих результатів. Використання спеціальних пошукових операторів дозволяє суттєво звузити коло інформації та знаходити саме ті дані, які необхідні для проведення аналізу. Завдяки цьому дослідники, журналісти, аналітики та фахівці з кібербезпеки можуть оперативно виявляти відкриті документи, технічну інформацію, сторінки авторизації, файли певного формату чи інші ресурси, що мають практичне значення в межах OSINT-досліджень. Крім того, Google Dorks не потребують використання складного програмного забезпечення, що робить цей інструмент доступним навіть для користувачів із базовими технічними навичками.

Водночас існують і певні обмеження використання пошукових операторів. Насамперед ефективність Google Dorks залежить від індексації ресурсів пошуковими системами: якщо вебсторінка або файл не проіндексовані, знайти їх за допомогою таких запитів буде неможливо. Також важливим фактором є правильне формулювання пошукових запитів, оскільки некоректне використання операторів може призвести до отримання великої кількості нерелевантних результатів. Додатково варто враховувати, що частина інформації може бути обмежена налаштуваннями конфіденційності, захищена авторизацією або видалена з відкритого доступу.

Окремої уваги потребують етичні та правові аспекти використання Google Dorks. Незважаючи на те, що пошук здійснюється у відкритих джерелах, необережне або неправомірне використання знайденої інформації може порушувати право на приватність чи норми інформаційної безпеки. Саме тому застосування таких методів повинно здійснюватися виключно в межах законодавства та професійної етики.

Отже, використання пошукових операторів є важливим елементом ефективної роботи з відкритими джерелами інформації. Вони значно підвищують якість і результативність пошуку, дозволяють швидко отримувати цінні дані та оптимізують процес OSINT-аналізу. Водночас ефективне застосування Google Dorks потребує належного рівня підготовки, уважності до деталей та відповідального підходу до роботи з інформацією.

Список використаних джерел:

1. Google Search Help. URL: https://support.google.com/websearch/
2. SANS Institute. URL:https://www.sans.org/
3. Bellingcat. URL:https://www.bellingcat.com/
4. Exploit Database (Google Hacking Database). URL: https://www.exploit-db.com/google-hacking-database

ВИКОРИСТАННЯ ПРИНЦИПІВ РОЙОВОГО ІНТЕЛЕКТУ В OSINT-ДОСЛІДЖЕННЯХ ТА БЕЗПЕКОВІЙ АНАЛІТИЦІ

Ревак Ірина Олександрівна
доктор економічних наук, професор
завідувач науково-дослідної лабораторії
OSINT-досліджень та безпекової аналітики
(Львівський державний університет внутрішніх справ)

Концепція ройового інтелекту сформувалася на основі дослідження колективної поведінки біологічних систем, зокрема колоній мурах, роїв бджіл, зграй птахів та інших самоорганізованих природних екосистем, у яких складні форми поведінки виникають без централізованого управління. Основу ройового інтелекту становить взаємодія великої кількості автономних агентів, які діють за відносно простими правилами, однак у процесі локальної комунікації та обміну інформацією формують ефективні механізми адаптації, координації та колективного прийняття рішень. Ключовими принципами ройового інтелекту є децентралізація управління, самоорганізація, розподіленість функцій, адаптивність, емерджентність, стійкість до втрати окремих елементів системи та здатність до колективного накопичення інформації. У

межах такого підходу кожен окремий елемент системи є носієм обмеженого обсягу інформації та виконує окремі функції, однак у сукупності взаємодія між усіма агентами забезпечує формування цілісної моделі реагування на зовнішні виклики та загрози.

У сучасних умовах розвитку цифрового середовища та стрімкого зростання обсягів відкритих даних принципи ройового інтелекту набувають особливої актуальності у сфері OSINT-досліджень та безпекової аналітики. Застосування такого підходу дає змогу розглядати аналітичну діяльність як децентралізовану систему колективної взаємодії аналітиків, автоматизованих інструментів, алгоритмів моніторингу та цифрових платформ, що спільно забезпечують виявлення, обробку, верифікацію та інтерпретацію інформації з відкритих джерел. У цьому контексті окремі аналітики або програмні агенти виконують функції збору та первинного аналізу даних, тоді як інтеграція результатів їх діяльності формує комплексне аналітичне розуміння ситуації. Така модель сприяє підвищенню оперативності реагування на інформаційні загрози, більш ефективному виявленню латентних взаємозв'язків між подіями, адаптації до динамічних змін інформаційного середовища, а також забезпечує стійкість аналітичної системи до втрати або дезорганізації окремих її елементів.

Колективна когнітивна аналітика в сучасних умовах розглядається як форма розподіленого інтелекту, що формується через взаємодію великої кількості автономних учасників, які спільно генерують, перевіряють та інтерпретують інформацію. У межах OSINT-середовища такий підхід реалізується через механізми краудсорсингового інтелекту (*crowdsourcing intelligence*), за яких аналітичні результати формуються не внаслідок централізованої експертної роботи, а шляхом акумулювання індивідуальних висновків. Така модель відповідає загальним положенням теорії колективного інтелекту, згідно з якою групи здатні демонструвати вищу ефективність у прийнятті рішень порівняно з окремими індивідами завдяки систематизації різнорідної інформації та набутого досвіду. У безпековій аналітиці це дає змогу швидше виявляти загрози, особливо в умовах інформаційної перенасиченості та динамічності цифрового середовища. Водночас ключовим чинником ефективності таких систем виступає якість координації взаємодій між учасниками та здатність до структурованої

обробки даних, що забезпечує перехід від масивів розрізнених сигналів до цілісних аналітичних висновків.

Сучасний етап розвитку аналітичних систем характеризується поступовою інтеграцією принципів ройового інтелекту з технологіями штучного інтелекту, що формує гібридні моделі колективного інтелекту нового покоління. У таких системах аналітики та алгоритмічні агенти виступають як взаємодоповнюючі елементи однієї мережевої структури, де частина задач виконується автоматизовано, а частина – через когнітивну інтерпретацію даних. Дослідження у сфері штучного колективного інтелекту підтверджують, що поєднання алгоритмічної обробки даних із колективною взаємодією учасників дає можливість суттєво підвищити точність прогнозування та якість прийняття рішень у порівнянні з індивідуальними підходами [1]. Відтак ройовий інтелект у поєднанні зі штучним інтелектом виступає основою формування інтелектуальних систем підтримки рішень та характеризується такими властивостями як самоорганізація, здатність до масштабування та підвищена стійкість до інформаційних впливів.

Мережева стійкість аналітичних систем з позиції ройового інтелекту визначається здатністю децентралізованої структури зберігати функціональність та ефективність навіть за умов часткової втрати елементів або порушення комунікаційних зв'язків. На відміну від централізованих моделей, ройові системи базуються на принципах самоорганізації та локальної взаємодії, що забезпечує їхню високу адаптивність до змін середовища. У теорії колективного інтелекту така властивість розглядається як одна з ключових характеристик розподілених інтелектуальних систем, де ефективність залежить не від окремих компонентів, а від структури їх взаємодії. У практиці OSINT-досліджень та кібербезпеки це проявляється у здатності аналітичних мереж протидіяти інформаційним атакам, блокуванню джерел даних або цілеспрямованому поширенню дезінформації. Крім того, мережева стійкість здатна забезпечити безперервність аналітичних процесів у кризових умовах, що є особливо важливим для систем раннього виявлення загроз і підтримки прийняття рішень у сфері національної та міжнародної безпеки. Відтак ройовий інтелект можемо розглядати не лише як алгоритмічний або кібернетичний підхід, а і як

концептуальну основу сучасних колективних OSINT-досліджень та мережевої безпекової аналітики.

Список використаних джерел:

1. L. Rosenberg, G. Willcox, H. Schumann (2023). Towards Collective Superintelligence, a Pilot Study. *International Conference on Human-Centered Cognitive Systems*. URL: https: //arxiv.org/pdf/2311.00728v1

«ВИКОРИСТАННЯ OSINT У ЦИФРОВІЙ КРИМІНАЛІСТИЦІ (DIGITAL FORENSICS)»

Синюкова Анастасія
здобувачка вищої освіти Інститут права та безпеки
Одеський державний університет внутрішніх справ
Науковий керівник: ***Грезіна Олена Миколаївна***
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

Стрімкий розвиток інформаційних технологій та масове поширення відкритих цифрових джерел зумовили появу нового напряму у правоохоронній і слідчій діяльності — використання методів розвідки на основі відкритих джерел (OSINT, Open Source Intelligence) у цифровій криміналістиці [1]. OSINT охоплює збір, аналіз та верифікацію даних із загальнодоступних ресурсів: соціальних мереж, публічних реєстрів, геопросторових сервісів, новинних порталів та інших відкритих платформ. Інтеграція цього підходу в цифрову криміналістику дозволяє значно розширити доказову базу, встановлювати особи підозрюваних і відновлювати хронологію подій — навіть у випадках, коли традиційні слідчі методи виявляються недостатніми [2].

Цифрова криміналістика (digital forensics) — це галузь судової науки, що займається виявленням, збором, аналізом та документуванням цифрових доказів для цілей кримінального або цивільного судочинства [6]. Традиційно вона спирається на вилучення даних із комп'ютерів, мобільних пристроїв, хмарних сховищ та

мереж. OSINT доповнює ці методи, надаючи слідчим змогу досліджувати цифровий слід фігурантів справ у відкритому інформаційному просторі [2].

Ключова відмінність OSINT від класичних криміналістичних методів полягає в тому, що дані збираються без прямого доступу до пристроїв підозрюваних і без необхідності отримувати судові ордери на кожне джерело [4]. Це робить OSINT особливо цінним на початкових етапах розслідування — для формування гіпотез, побудови мереж зв'язків та визначення пріоритетних напрямів подальшої роботи [1].

Серед найбільш поширених методів OSINT у цифровій криміналістиці виокремлюють такі напрями[1;2]:

Аналіз соціальних мереж, а саме Facebook, Instagram, Telegram, X (Twitter) та LinkedIn, містять колосальні масиви інформації про осіб: фотографії, геомітки, коло спілкування, хронологію активності. Інструменти на зразок Maltego, Sherlock, SpiderFoot дозволяють автоматизувати збір і систематизацію таких даних [1].

Використання Google Maps та супутникових знімків (Sentinel Hub, Planet Labs) допомагає верифікувати місця подій, відстежувати переміщення підозрюваних і реконструювати обстановку [5].

Цифрові файли (фотографії, документи, відео) можуть містити приховані метадані — EXIF-інформацію з координатами, часом зйомки, моделлю пристрою. Утиліти ExifTool і Jeffrey's Exif Viewer широко застосовуються для їх вилучення [6].

OSINT-фахівці використовують спеціалізовані пошукові системи (Ahmia, OnionSearch) та моніторингові платформи для відстеження активності злочинних угруповань у прихованих сегментах мережі [7].

Сервіси Shodan, WHOIS, VirusTotal, Censys допомагають встановлювати власників веб-ресурсів, виявляти фішингові сайти та відстежувати інфраструктуру кіберзлочинців [3].

На практиці OSINT успішно застосовується в розслідуванні кіберзлочинів, тероризму, торгівлі людьми, шахрайства та корупції [5]. Показовим прикладом є діяльність міжнародної групи Bellingcat, яка за допомогою виключно відкритих джерел встановила осіб причетних до катастрофи MH17 та задокументувала численні воєнні злочини. Правоохоронні органи США, Євросоюзу

та України все активніше впроваджують OSINT-методики у стандартні процедури розслідування [3;4].

Разом із тим, використання OSINT у криміналістиці стикається з низкою суттєвих викликів. По-перше, постає питання допустимості доказів: суди різних юрисдикцій мають відмінні стандарти щодо прийнятності даних, зібраних із відкритих джерел, а неправильне документування процесу збору може знецінити докази [4]. По-друге, зростання алгоритмів дезінформації та deepfake-контенту вимагає обов'язкової верифікації знайдених матеріалів [7]. По-третє, виникають етико-правові колізії між ефективністю розслідування та захистом приватності осіб, які потрапляють у поле зору слідчих [2].

OSINT став невід'ємним компонентом сучасної цифрової криміналістики, що суттєво розширює можливості слідчих у роботі з відкритим інформаційним простором [1;2]. Ефективне поєднання традиційних криміналістичних методів та OSINT-інструментів дозволяє вирішувати складні справи, які раніше залишались нерозкритими [5;6]. Водночас розвиток галузі потребує розробки єдиних стандартів збору та верифікації даних, навчання фахівців і формування відповідної нормативно-правової бази, здатної збалансувати інтереси правосуддя та захист прав людини [4;7].

Список використаних джерел:

1. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. — Одеса : Юридика, 2024. — 180 с. URL: https://doi.org/10.32837/11300.27740.

2. Пашковський М. І. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. — Харків, 2024. — С. 233–274. DOI: https://doi.org/10.31359/9786178612139.

3. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. Вісник Кримінологічної асоціації України. 2024. Т. 32, № 2. С. 945–958. URL: https://doi.org/10.32631/vca.2024.2.74.

4. Шехавцов Р. М. Правове регулювання використання OSINT та його результатів під час встановлення обставин кримінальних правопорушень. Науковий вісник Львівського державного

університету внутрішніх справ. Серія юридична. 2025. URL: https://journals.lvduvs.lviv.ua/index.php/law/article/view/1013.

5. Тітко І. А. Використання методик OSINT у межах розслідування кримінальних правопорушень: успішні кейси у практиці іноземних правоохоронних органів та інститутів громадянського суспільства. Аналітично-порівняльне правознавство. 2026. URL: https://journal-app.uzhnu.edu.ua/article/view/358390.

6. Криміналістика і судова експертиза : міжвідом. наук.-метод. зб. / КНДІ судових експертиз ; редкол.: О. Г. Рувін та ін. — Київ : Ліра-К, 2023.

7. Використання OSINT у кримінальному провадженні: правові засади та проблеми захисту персональних даних. Юридичний науковий електронний журнал. 2024. № 11. С. 108. URL: https://www.lsej.org.ua/11_2024/108.pdf

ІНСТРУМЕНТИ, МЕТОДИ ТА АЛГОРИТМИ ЗАСТОСУВАННЯ OSINT У АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ

Щурат Тарас Григорович
доцент кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС, кандидат юридичних наук, доцент
Тритяк Марія Володимирівна
курсант 201 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України ОДУВС

Оперативно-розшукова діяльність (ОРД) є одним із ключових напрямів діяльності правоохоронних органів, що забезпечує отримання, аналіз та використання інформації з метою протидії злочинності. В умовах цифровізації суспільства та зростання ролі інформаційного середовища особливого значення набуває аналітична складова ОРД, яка базується на обробці великих масивів даних. Одним із сучасних інструментів такої діяльності є OSINT (Open Source Intelligence) — розвідка з відкритих джерел [1].

Відповідно до Закону України «Про оперативно-розшукову діяльність», ОРД визначається як система гласних і негласних заходів, спрямованих на виявлення та припинення кримінальних правопорушень [2]. У межах цієї діяльності використання відкритих джерел інформації є законним та доцільним, оскільки дозволяє отримувати значний обсяг даних без втручання у приватне життя особи на початкових етапах перевірки інформації.

Аналітична діяльність оперативних підрозділів передбачає застосування спеціалізованих інструментів OSINT. До них належать пошукові системи з розширеними можливостями (Google Dorks), аналітичні платформи (Maltego, IBM i2 Analyst's Notebook), сервіси аналізу соціальних мереж, бази відкритих даних, а також геоінформаційні системи. Застосування таких інструментів дозволяє встановлювати зв'язки між особами, виявляти структуру злочинних груп та відстежувати їх діяльність у цифровому середовищі [3, с. 45].

Методи застосування OSINT в аналітичній діяльності включають контент-аналіз, соціальний мережевий аналіз (SNA), геопросторовий аналіз, часовий аналіз та кримінальний аналіз. Зокрема, соціальний мережевий аналіз дозволяє визначати роль кожного учасника злочинної групи, виявляти лідерів та встановлювати характер зв'язків між ними. Геоаналіз використовується для встановлення місця перебування осіб або локалізації подій, що має важливе значення у розслідуванні злочинів. Як зазначає І. А. Федчак, кримінальний аналіз забезпечує систематизацію інформації та сприяє прийняттю ефективних управлінських рішень у діяльності правоохоронних органів [4, с. 64]. Особливого значення набуває алгоритм застосування OSINT у діяльності оперативних підрозділів. Він включає послідовність дій, спрямованих на отримання достовірної та релевантної інформації. До основних етапів належать: визначення мети пошуку, збір інформації з відкритих джерел, її фільтрація, верифікація, аналітична обробка, встановлення зв'язків та формування висновків. Завершальним етапом є документування результатів та їх передача для використання у кримінальному провадженні.

У межах ОРД результати OSINT можуть виступати підставою для проведення негласних слідчих (розшукових) дій. Відповідно до Кримінального процесуального кодексу України, такі дії здійснюються з метою отримання доказів та перевірки інформації [5].

Зокрема, статті 246 та 260 КПК України визначають порядок проведення негласних заходів, що дозволяє інтегрувати результати аналітичної діяльності у процес доказування. Важливим є питання допустимості інформації, отриманої за допомогою OSINT. Згідно з КПК України, доказами є лише ті дані, які отримані у законний спосіб і належним чином оформлені [5, с. 87]. Це означає, що оперативні працівники повинні забезпечити фіксацію джерел інформації, її збереження та підтвердження достовірності. Недотримання цих вимог може призвести до визнання доказів недопустимими.

Конституція України гарантує дотримання прав і свобод людини, зокрема права на невтручання в особисте і сімейне життя [6]. У зв'язку з цим використання OSINT повинно здійснюватися з дотриманням принципів законності, пропорційності та обґрунтованості. Навіть при роботі з відкритими джерелами існує необхідність контролю за межами використання отриманої інформації. Практичне значення OSINT у діяльності оперативних підрозділів полягає у можливості швидкого отримання інформації, встановлення осіб, причетних до злочинів, аналізу їх поведінки та прогнозування подальших дій. Це особливо актуально у протидії організованій злочинності, кіберзлочинам та злочинам, пов'язаним із використанням інформаційних технологій. Разом із тим існують проблеми застосування OSINT, серед яких: великий обсяг інформації, складність її перевірки, наявність дезінформації, відсутність єдиних стандартів використання та недостатній рівень підготовки працівників. У зв'язку з цим необхідним є вдосконалення методичного забезпечення аналітичної діяльності та підвищення рівня професійної підготовки оперативних працівників.

Перспективи розвитку OSINT у системі ОРД пов'язані з впровадженням сучасних технологій аналізу даних, зокрема штучного інтелекту, автоматизованих систем обробки інформації та інтеграції різних джерел у єдині інформаційні системи. Важливим є також удосконалення нормативно-правової бази, що регулює використання відкритих джерел інформації у правоохоронній діяльності. Таким чином, OSINT є важливим інструментом аналітичної діяльності оперативних підрозділів, що дозволяє підвищити ефективність ОРД. Його застосування забезпечує своєчасне отримання інформації, однак потребує дотримання правових норм, належного документування та професійної підготовки кадрів.

Список використаних джерел:

1. OSINT Framework : офіційний ресурс. URL: https://osintframework.com
2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII.
3. Europol. Open Source Intelligence (OSINT) and its applications in law enforcement. Hague, 2021.
4. Федчак І. А. Основи кримінального аналізу. Львів : ЛьвДУВС, 2020.
5. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.
6. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР.

СЕКЦІЯ 6.
ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ ТА КІБЕРБЕЗПЕЦІ АНАЛІТИЧНІ, ТЕХНОЛОГІЧНІ ТА ПРАВОВІ АСПЕКТИ

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АНАЛІЗІ ДАНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Атаманенко Юлія Юріївна
кандидатка технічних наук, старша дослідниця,
провідна наукова співробітниця науково-дослідної
лабораторії публічної безпеки громад навчально-наукового
інституту права та соціального менеджменту
Донецького державного університету внутрішніх справ

Сучасний етап розвитку інформаційних технологій характеризується інтенсивним застосуванням безпілотних літальних апаратів (БпЛА) у правоохоронній діяльності. У зв'язку з цим стрімко зростають обсяги даних, отриманих за допомогою БпЛА (відео, фотоматеріали, телеметрія), що зумовлюють створення нових викликів щодо їх оперативного опрацювання. У цьому контексті особливого значення набуває застосування технологій штучного інтелекту (ШІ) в кримінальному аналізі, які дозволяють автоматизувати процес аналізу та сприяють підвищенню ефективності прийняття рішень [1]. Отже, актуальність дослідження в умовах сьогодення зумовлена комплексними трансформаціями у сфері безпеки, цифровізації та правоохоронної діяльності, що потребують інтеграції інноваційних технологій, зокрема ШІ та БпЛА у процеси кримінального аналізу з метою підвищення ефективності, оперативності та прогностичних можливостей.

Слід зазначити, що інтеграція ШІ значно розширює можливості БпЛА у кримінальних розслідуваннях, адже дозволяють літальному апарату автономно класифікувати різні типи доказів під час аерознімання з точністю до 98 %, що спрощує процес їх реєстрації, тим самим пришвидшуючи збір даних на 30 % у

порівнянні з традиційними методами. Також технології ШІ доповнюють передові можливості візуалізації БпЛА, які включають ультрафіолетові та інфрачервоні датчики, які сприяють виявленню прихованих доказів, таких як відбитки пальців та інші важливі деталі, без шкоди для цілісності доказів [2]. Отже, ШІ виступає як інструмент, що не лише обробляє інформацію, а й у поєднанні з БпЛА має низку суттєвих переваг, таких як:

– оперативність (значне скорочення часу обробки даних);
– точність (зменшення впливу людського фактору);
– масштабованість (можливість обробки великих обсягів інформації);
– автоматизація (зниження навантаження на аналітиків);
– аналітична глибина (виявлення прихованих закономірностей) тощо.

Ці переваги особливо важливі в умовах обмежених ресурсів, необхідністю швидкого реагування, що є ключовими факторами сучасної правоохоронної діяльності в умовах цифрової трансформації. Проте, інтеграція ШІ в аналіз даних БпЛА для кримінального аналізу викликає значні проблеми [3], які потребують ретельного розгляду, як-от питання щодо:

- похибки алгоритмів, які можуть призводити до неправильного розпізнавання об'єктів або інтерпретації даних;
- правових обмежень, пов'язаних з використанням отриманої інформації як доказу у кримінальному провадженні;
- захисту персональних даних та приватності, оскільки БпЛА можуть фіксувати інформації про осіб без їх згоди;
- етичних аспектів, зокрема щодо автоматизації прийняття рішень та можливості упередженості алгоритмів;
- технічного забезпечення та підготовки фахівців, здатних працювати з такими технологіями.

Отже, застосування технологій ШІ в аналізі даних БпЛА є перспективним напрямом розвитку сучасного кримінального аналізу, адже поєднання можливостей БпЛА щодо збору інформації та ШІ щодо її обробки дозволяє значно підвищити оперативність виявлення криміногенних загроз, рівень автоматизації аналітичних процесів та якість прийняття управлінських рішень у сфері правоохоронної діяльності. Проте, для повноцінного впровадження таких технологій та вирішення окреслених проблем доцільно запропонувати такі рекомендації як:

- створити інтегровані аналітичні платформи для централізованої обробки даних, отриманих із безпілотних літальних апаратів, із використанням алгоритмів машинного навчання та штучного інтелекту;
- впровадити технологію глибинного навчання для автоматичного розпізнавання об'єктів, подій та аномальної поведінки в режимі реального часу;
- сприяти розвитку системи предиктивної аналітики злочинності, що дозволяє прогнозувати потенційні кримінальні ризики на основі просторово-часових та історичних даних;
- запровадити правові та етичні стандарти використання ШІ, спрямованих на забезпечення балансу між ефективністю кримінального аналізу та дотриманням прав і свобод людини;
- реалізувати принцип «human-in-the-loop», який передбачає обов'язкову участь аналітика у верифікації результатів, отриманих за допомогою штучного інтелекту;
- забезпечити кібербезпеку та захист даних БпЛА шляхом використання криптографічних технологій та захищених каналів передачі інформації;
- підготувати спеціалізованих фахівців, здатних ефективно працювати на перетині кримінального аналізу, штучного інтелекту та безпілотних технологій.

Таким чином, комплексна реалізація запропонованих заходів сприятиме формуванню сучасної, технологічно орієнтованої моделі кримінального аналізу, підвищенню ефективності діяльності правоохоронних органів та адаптації правової системи до умов цифрової трансформації суспільства.

Список використаних джерел:

1. How AI & Analytics Are Revolutionizing Law Enforcement Surveillabce. Critical Tech Solution. URL: https://surl.li/qrmovb (дата звернення: 25.04.2026).

2. Bhoopesh Kumar Sharma, Geetanjali Chandra, Ved P. Mishra. Comparitive Analysis and Implication of UAV and AI in Forensic Investigations. *IEEE.* 2019. P. 824 – 827.

3. Voloch N., Hirschprung R. S. Both ends of artificial intelligence impacting privacy: a review of violation and protection. *Front. Artif. Intelligence.* 2026. P/ 1 –26. doi: 10.3389/frai.2026.1686454.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ПРАВООХОРОННИХ ОРГАНІВ

Балтовський Олексій Анатолійович
доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ

У сучасних умовах трансформації глобального інформаційного середовища, інтенсивної цифровізації суспільних процесів та стрімкого розвитку кіберфізичних систем особливої актуальності набуває проблема забезпечення належного рівня кібербезпеки інформаційно-аналітичних систем правоохоронних органів. Динаміка розвитку цифрових технологій, інтеграція засобів автоматизованого аналізу даних у діяльність суб'єктів сектору безпеки і оборони, а також зростання масштабів використання інформаційно-комунікаційних технологій у сфері кримінального аналізу формують нові виклики для національної системи кібербезпеки. Вказані процеси супроводжуються не лише розширенням функціональних можливостей інформаційно-аналітичних платформ, але й суттєвим підвищенням рівня їх вразливості до деструктивних інформаційних впливів, кібератак, несанкціонованого доступу, маніпуляцій з даними та інтелектуальних форм кіберзлочинності [3].

Інформаційно-аналітичні системи правоохоронних органів у сучасних умовах функціонують як складні багаторівневі організаційно-технічні комплекси, що забезпечують накопичення, інтеграцію, оброблення, інтерпретацію та прогнозування інформації, необхідної для підтримки управлінських рішень, виявлення кримінальних загроз, аналізу ризиків та протидії транснаціональній злочинності. Такі системи характеризуються високим рівнем інформаційної насиченості, багатокомпонентною структурою, інтеграцією розподілених баз даних, використанням хмарних сервісів, засобів Big Data-аналітики, геоінформаційних технологій, систем підтримки прийняття рішень та автоматизованих механізмів моніторингу. У зв'язку з цим забезпечення їх кіберстійкості стає

не лише технічним, але й стратегічним завданням державної політики у сфері безпеки [1,2].

Особливого значення набуває використання технологій штучного інтелекту та інтелектуального аналізу даних як інструментів підвищення ефективності функціонування систем кіберзахисту. Концептуально штучний інтелект у сфері кібербезпеки слід розглядати як комплекс методів і алгоритмів, здатних здійснювати автоматизоване виявлення аномалій, моделювання поведінкових патернів, класифікацію кіберзагроз, прогнозування потенційних інцидентів, аналіз ризиків та підтримку прийняття управлінських рішень у режимі реального часу. Інтелектуальний аналіз даних, у свою чергу, виступає фундаментальним методологічним інструментарієм виявлення прихованих закономірностей, причинно-наслідкових зв'язків, латентних залежностей та структурних характеристик інформаційних потоків, що циркулюють у цифровому середовищі правоохоронних органів.

Сучасний етап розвитку кіберзагроз характеризується переходом від традиційних форм комп'ютерних атак до складних адаптивних моделей кібернетичного впливу, які використовують механізми соціальної інженерії, генеративного штучного інтелекту, автоматизованих бот-мереж, поліморфного шкідливого програмного забезпечення та технологій маскування цифрової активності. В умовах постійного ускладнення архітектури кібератак класичні сигнатурні підходи до виявлення загроз демонструють обмежену ефективність, оскільки орієнтовані переважно на відомі шаблони поведінки. Саме тому пріоритетного значення набуває впровадження інтелектуальних систем аналізу, здатних до самоадаптації, машинного навчання та прогнозування нових типів загроз.

Використання методів машинного навчання у сфері забезпечення кібербезпеки дозволяє реалізувати принципово новий рівень автоматизації процесів аналізу інформації. Алгоритми supervised learning забезпечують класифікацію мережевої активності на основі попередньо сформованих наборів даних та дозволяють виявляти шкідливі сценарії поведінки користувачів або системних процесів. Методи unsupervised learning спрямовані на виявлення аномалій у великих масивах неструктурованих даних та забезпечують ідентифікацію потенційних кіберінцидентів без необхідності попереднього маркування інформації. Технології reinforcement learning дозволяють системам кіберзахисту

адаптуватися до змін середовища та оптимізувати механізми реагування на інциденти шляхом накопичення досвіду функціонування [3].

Особливу роль у забезпеченні кібербезпеки інформаційно-аналітичних систем правоохоронних органів відіграють нейромережеві технології. Глибокі нейронні мережі забезпечують можливість аналізу великих обсягів мережевого трафіку, лог-файлів, інформаційних журналів та поведінкових характеристик користувачів з метою виявлення нетипових сценаріїв активності. Використання рекурентних нейронних мереж дозволяє здійснювати часовий аналіз послідовностей подій, що є надзвичайно важливим у контексті прогнозування етапів розвитку складних кібератак. Конволюційні нейронні мережі можуть застосовуватися для виявлення шкідливого програмного забезпечення шляхом аналізу структурних характеристик файлів та цифрових артефактів.

Інтелектуальний аналіз даних у діяльності правоохоронних органів має міждисциплінарний характер та поєднує елементи системного аналізу, математичного моделювання, теорії ризиків, теорії прийняття рішень, криптографії, комп'ютерної лінгвістики та когнітивної аналітики. Використання Data Mining-технологій дозволяє здійснювати глибоку обробку інформації, виявляти латентні взаємозв'язки між подіями, суб'єктами та цифровими об'єктами, формувати прогностичні моделі кіберзагроз та оцінювати рівень інформаційних ризиків. У контексті кримінального аналізу це створює передумови для переходу від реактивної моделі забезпечення безпеки до проактивної концепції попередження кіберзлочинності.

Суттєвий науковий та практичний інтерес становить використання технологій штучного інтелекту у процесі аналізу поведінкових характеристик користувачів інформаційно-аналітичних систем. Поведінкова аналітика базується на побудові цифрових профілів користувачів, моделюванні типових сценаріїв взаємодії із системою та виявленні відхилень від нормативної поведінки. Такий підхід дозволяє своєчасно ідентифікувати ознаки внутрішніх загроз, компрометації облікових записів або спроб несанкціонованого доступу. Особливої актуальності це набуває в умовах використання віддалених форм доступу до інформаційних ресурсів та інтеграції мобільних платформ у систему службової діяльності правоохоронних органів.

Одним із ключових напрямів застосування інтелектуальних технологій є автоматизація процесів реагування на кіберінциденти. У сучасних умовах традиційні моделі реагування часто не забезпечують необхідної швидкості прийняття рішень через значні обсяги інформації та високий рівень динамічності кіберзагроз. Використання технологій SOAR та SIEM у поєднанні з алгоритмами штучного інтелекту дозволяє автоматизувати процеси кореляції подій, аналізу журналів безпеки, виявлення аномалій та формування рекомендацій щодо реагування на інциденти. Це суттєво підвищує оперативність діяльності аналітичних підрозділів та забезпечує мінімізацію часу між виявленням загрози та реалізацією заходів протидії.

Не менш важливим аспектом є використання штучного інтелекту для прогнозування кіберризиків. Прогностичні моделі, побудовані на основі аналізу історичних даних, поведінкових патернів та характеристик мережевої активності, дозволяють визначати потенційно критичні ділянки інформаційної інфраструктури, прогнозувати ймовірність виникнення інцидентів та формувати ризик-орієнтовані стратегії кіберзахисту. Застосування системного аналізу у поєднанні з методами машинного навчання створює передумови для комплексної оцінки стійкості інформаційно-аналітичних систем до зовнішніх і внутрішніх загроз [4].

У контексті функціонування правоохоронних органів особливого значення набуває проблема забезпечення достовірності та цілісності інформації, що обробляється в інформаційно-аналітичних системах. В умовах гібридних загроз та інформаційних операцій противника маніпуляція цифровими даними може мати критичні наслідки для процесів прийняття управлінських рішень. Технології штучного інтелекту дозволяють здійснювати автоматизовану верифікацію інформації, виявляти ознаки фальсифікації даних, аналізувати цифрові сліди втручання та формувати механізми забезпечення інформаційної довіри. У цьому аспекті особливої актуальності набуває використання алгоритмів аналізу цифрових аномалій, криптографічних методів контролю цілісності та блокчейн-технологій.

Проблематика впровадження штучного інтелекту у сферу кібербезпеки інформаційно-аналітичних систем правоохоронних органів має також виражений правовий та етичний вимір. Автоматизація процесів прийняття рішень, використання алгоритмів

прогнозування поведінки та аналізу персональних даних потребують дотримання принципів законності, пропорційності, прозорості та недискримінаційності. У зв'язку з цим важливого значення набуває формування нормативно-правових механізмів регулювання використання технологій штучного інтелекту у діяльності правоохоронних структур, визначення меж автоматизації аналітичної діяльності та забезпечення належного рівня контролю за функціонуванням інтелектуальних систем [1-3].

Складність сучасного кіберпростору обумовлює необхідність формування інтегрованої архітектури кіберзахисту, що базується на принципах адаптивності, масштабованості, багаторівневості та прогнозованості. У цьому контексті інформаційно-аналітичні системи правоохоронних органів мають трансформуватися у комплексні когнітивні платформи, здатні забезпечувати автоматизоване сприйняття, інтерпретацію та прогнозування кіберзагроз. Використання технологій штучного інтелекту дозволяє реалізувати концепцію інтелектуальної кібероборони, в межах якої система не лише реагує на інциденти, але й здійснює постійний аналіз цифрового середовища, моделює потенційні сценарії атак та формує превентивні механізми протидії.

Перспективним напрямом розвитку систем кібербезпеки є використання когнітивних моделей аналізу інформації. Когнітивна аналітика дозволяє інтегрувати механізми машинного навчання, семантичного аналізу, оброблення природної мови та системного моделювання для виявлення прихованих взаємозв'язків між подіями, суб'єктами та інформаційними потоками. У діяльності правоохоронних органів це створює можливості для автоматизованого аналізу великих масивів текстової інформації, OSINT-даних, соціальних мереж, цифрових комунікацій та інших джерел інформації з метою виявлення ознак підготовки кіберзлочинів або координації протиправної діяльності.

Важливим елементом сучасної системи кібербезпеки є інтеграція засобів штучного інтелекту з технологіями аналізу великих даних. Big Data-підхід дозволяє здійснювати оброблення значних обсягів структурованої та неструктурованої інформації у режимі реального часу, забезпечуючи можливість комплексного аналізу цифрового середовища. Для правоохоронних органів це означає формування нових можливостей щодо оперативного виявлення

кіберзагроз, прогнозування криміногенних тенденцій та підтримки стратегічного управління ризиками.

Одним із найбільш складних викликів у сфері кібербезпеки є проблема протидії адаптивним інтелектуальним атакам, що використовують алгоритми штучного інтелекту для обходу традиційних механізмів захисту. У зв'язку з цим особливої актуальності набуває концепція AI-driven cybersecurity, яка передбачає використання інтелектуальних механізмів для забезпечення автоматизованої протидії інтелектуальним загрозам. Реалізація такої концепції потребує створення комплексних систем кібермоніторингу, здатних до самоадаптації, автономного аналізу інформації та безперервного навчання.

Науково-методологічна основа застосування штучного інтелекту у сфері кібербезпеки має базуватися на системному підході, який передбачає розгляд інформаційно-аналітичних систем як складних відкритих систем із багаторівневою структурою взаємозв'язків. Використання методів системного аналізу дозволяє здійснювати декомпозицію складних процесів забезпечення кібербезпеки, визначати критичні елементи інфраструктури, аналізувати потоки інформації та оцінювати рівень стійкості системи до деструктивних впливів. Поєднання системного підходу з алгоритмами штучного інтелекту створює концептуальні передумови для формування адаптивних моделей кіберзахисту нового покоління [4].

Таким чином, використання штучного інтелекту та інтелектуального аналізу даних у забезпеченні кібербезпеки інформаційно-аналітичних систем правоохоронних органів є стратегічним напрямом розвитку сучасної системи безпеки держави. Інтелектуальні технології забезпечують можливість автоматизації процесів аналізу інформації, прогнозування кіберризиків, виявлення аномалій, підтримки прийняття управлінських рішень та формування проактивних механізмів протидії кіберзагрозам. Їх впровадження сприяє підвищенню ефективності діяльності правоохоронних органів, зміцненню стійкості інформаційної інфраструктури та розвитку сучасних підходів до кримінального аналізу в умовах цифрової трансформації суспільства. Перспективи подальших досліджень у даному напрямі пов'язані з удосконаленням методів когнітивної аналітики, розвитком адаптивних систем кіберзахисту, інтеграцією генеративного штучного інтелекту у процеси аналізу інформації, а також формуванням комплексних

міждисциплінарних моделей забезпечення кібербезпеки у діяльності правоохоронних органів [4].

Список використаних джерел:

1. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень: навчальний посібник. Одеса: РВВ ОДУВС. 2022. 176 с.

2. Сучасні підходи щодо адаптивного автоматизованого управління складними системами в умовах невизначеності: монографія. /Кокошко В.С та ін.; за заг. ред. Форос Г.В. Одеса: ОДУВС, 2020. 180 с.

3. Шульга Є.М. Калугін В. Ю. Вдосконалення інформаційного забезпечення діяльності правоохоронних органів України. Матеріали круглого столу «Імплементація ILP моделі в Україні», 15 березня 2023 року. ОДУВС, 2023, С. 84-85

4. .Ханькевич А.М. Імплементація ilp моделі поліцейської діяльності у внутрішній безпековий сектор держави – з чого починати? Наукові перспективи № 5(35) 2023 с. 185-186/

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ ТА КІБЕРБЕЗПЕЦІ:АНАЛІТИЧНІ, ТЕХНОЛОГІЧНІ ТА ПРАВОВІ АСПЕКТИ

Борисович Надія Олександрівна
здобувач вищої освіти бакалавра
1 курс, 1 група, «Правоохоронна діяльність»
Одеського державного університету внутрішніх справ
Науковий керівник: ***Меликов Руслан***
Науковий співробітник науково-дослідної лабораторії
з актуальних питань кримінального аналізу
доктор філософі в галузі права

Сучасний розвиток інформаційних технологій суттєво впливає на діяльність правоохоронних органів та систему забезпечення національної безпеки держави. Одним із найбільш перспективних напрямів модернізації правоохоронної діяльності є використання технологій штучного інтелекту у кримінальному аналізі та кібербезпеці. Впровадження інтелектуальних систем дозволяє

автоматизувати процеси обробки великих масивів інформації, підвищити ефективність виявлення злочинів та забезпечити оперативне реагування на сучасні кіберзагрози [1, с. 32–35].

У сфері кримінального аналізу технології штучного інтелекту використовуються для збору, систематизації та аналізу значних обсягів інформації, які неможливо швидко обробити традиційними методами. За допомогою алгоритмів машинного навчання правоохоронні органи можуть встановлювати приховані зв'язки між особами, подіями, фінансовими операціями та іншими елементами кримінальної діяльності [3, p. 1–20]. Такі системи сприяють прогнозуванню криміногенних ризиків, виявленню закономірностей злочинної поведінки та оптимізації процесу прийняття управлінських рішень [1, с. 40–43].

Особливого значення використання штучного інтелекту набуває у сфері кібербезпеки. Сучасні системи захисту інформації застосовують автоматизований аналіз мережевого трафіку для виявлення підозрілої активності та попередження кібератак у режимі реального часу. Інтелектуальні технології дозволяють своєчасно виявляти шкідливе програмне забезпечення, фішингові атаки, спроби несанкціонованого доступу до інформаційних систем та інші кіберзагрози [5, с. 41–48]. Це суттєво підвищує рівень захисту державних інформаційних ресурсів і персональних даних громадян.

Крім того, технології штучного інтелекту активно застосовуються у системах відеоспостереження та розпізнавання облич. Автоматизовані системи можуть аналізувати відеопотоки, ідентифікувати осіб, які перебувають у розшуку, а також встановлювати маршрути їх пересування. Такі технології значно підвищують ефективність діяльності правоохоронних органів та сприяють швидкому розкриттю злочинів [1, с. 44–46]. Водночас їх використання породжує низку дискусій щодо дотримання права на приватність, захисту персональних даних та недопущення необґрунтованого втручання у права людини [4].

Важливим аспектом є правове регулювання використання штучного інтелекту. В Україні формування державної політики у цій сфері здійснюється відповідно до Концепції розвитку штучного інтелекту в Україні, схваленої Кабінетом Міністрів України у 2020 році [2]. Особливого значення набувають питання відповідальності за рішення, прийняті автоматизованими системами,

забезпечення прозорості алгоритмів та недопущення алгоритмічної дискримінації [4]. Недосконалість правового регулювання може призводити до порушення прав і свобод людини, тому впровадження інтелектуальних технологій потребує належного державного контролю.

Разом із перевагами використання штучного інтелекту існують і певні ризики. Серед них можна виокремити можливу упередженість алгоритмів, непрозорість функціонування нейронних мереж, ризик помилкового розпізнавання осіб та використання інтелектуальних технологій у протиправних цілях [1, с. 46–48]. Саме тому застосування штучного інтелекту у правоохоронній діяльності повинно супроводжуватися дотриманням етичних стандартів, законодавчих норм та міжнародних принципів захисту прав людини [4].

Отже, використання технологій штучного інтелекту у кримінальному аналізі та кібербезпеці є важливим напрямом модернізації правоохоронної системи та забезпечення інформаційної безпеки держави. Інтелектуальні системи сприяють підвищенню ефективності боротьби зі злочинністю, удосконаленню аналітичної діяльності та захисту інформаційного простору [1, с. 45–49; 5, с. 49–50]. Водночас подальший розвиток таких технологій потребує вдосконалення правового регулювання та забезпечення балансу між інтересами безпеки держави і дотриманням прав людини

Список використаних джерел:

1. Баранов О.А. Визначення терміну «штучний інтелект» // Інформація і право. 2023. № 1(44). С. 32–49.

2. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р.

3. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge : MIT Press, 2016.

4. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021.

5. Селіхов Д. А. Кібербезпека як складова інформаційної безпеки: теоретичні та прикладні аспекти // Аналітично-порівняльне правознавство. – 2024. – № 2.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ КІБЕРБЕЗПЕКИ

Виходець Юрій Олександрович
доктор філософії, доцент, професор кафедри кримінології та інформаційних технологій, Національної академії внутрішніх справ

Сучасний етап розвитку інформаційного суспільства характеризується інтенсивною цифровою трансформацією соціально-економічних, управлінських та безпекових процесів, що супроводжується стрімким зростанням ролі інформаційно-комунікаційних технологій у функціонуванні державних інституцій, правоохоронних органів, об'єктів критичної інфраструктури та приватного сектору. Водночас глобальна цифровізація створює не лише нові можливості для розвитку суспільства, але й формує комплекс принципово нових викликів у сфері кібербезпеки, пов'язаних із постійним зростанням кількості кіберінцидентів, удосконаленням механізмів реалізації кібератак, активізацією діяльності транснаціональних кіберзлочинних угруповань та ускладненням структури сучасних інформаційних систем. У сучасних умовах кіберпростір перетворюється на середовище високого рівня ризикогенності, де динаміка розвитку загроз значно випереджає можливості традиційних механізмів реагування. Саме тому особливого значення набуває впровадження інтелектуалізованих систем підтримки прийняття управлінських рішень, здатних забезпечити оперативний аналіз інформації, прогнозування кіберзагроз та формування ефективних стратегій забезпечення кібербезпеки [1-3].

Одним із ключових напрямів трансформації сучасної системи кібербезпеки є використання технологій штучного інтелекту, які виступають основою для створення адаптивних, самонавчальних та інтелектуально орієнтованих інформаційно-аналітичних систем. У сучасній науковій парадигмі штучний інтелект розглядається як сукупність методів, алгоритмів та програмно-технічних засобів, здатних моделювати окремі аспекти інтелектуальної діяльності людини, здійснювати аналіз великих масивів даних, виявляти приховані закономірності, формувати прогностичні моделі

та підтримувати процеси прийняття рішень у складних умовах невизначеності. У сфері кібербезпеки використання технологій штучного інтелекту забезпечує можливість переходу від реактивних моделей захисту до проактивних систем прогнозування та попередження кіберзагроз, що є критично важливим у контексті забезпечення стійкості інформаційної інфраструктури держави.

Особливість сучасного кіберпростору полягає у надзвичайно високій швидкості генерації інформації, багатовекторності кіберзагроз та постійній зміні сценаріїв реалізації кібератак. Традиційні механізми аналізу інформації та підтримки управлінських рішень виявляються недостатньо ефективними в умовах функціонування складних багаторівневих інформаційних систем, де обсяги даних перевищують можливості їх оперативної обробки людиною. За таких умов технології штучного інтелекту набувають особливого значення як інструмент автоматизованого аналізу інформації, здатний забезпечити високий рівень ситуаційної обізнаності, виявлення аномальної активності та прогнозування потенційних кіберінцидентів. Використання інтелектуальних систем дозволяє суттєво скоротити часові витрати на обробку інформації, підвищити точність аналітичних оцінок та забезпечити обґрунтованість управлінських рішень у сфері кібербезпеки [1].

У сучасних умовах технології штучного інтелекту активно використовуються у процесах моніторингу інформаційного простору, аналізу мережевого трафіку, виявлення ознак шкідливого програмного забезпечення, класифікації кіберзагроз та прогнозування поведінки кіберзлочинців. Особливого значення набувають алгоритми машинного навчання, які забезпечують здатність систем самостійно виявляти закономірності у великих масивах даних без жорстко заданих правил. Використання алгоритмів класифікації, кластеризації, нейронних мереж, методів глибинного навчання та інтелектуального аналізу даних створює передумови для формування інтелектуальних систем підтримки прийняття рішень, здатних адаптуватися до нових типів кіберзагроз та забезпечувати високий рівень ефективності кіберзахисту.

Важливим напрямом використання штучного інтелекту у сфері кібербезпеки є автоматизоване виявлення аномалій у функціонуванні інформаційних систем. Сучасні кіберзагрози характеризуються високим рівнем латентності та здатністю маскуватися

під легітимну активність користувачів, що ускладнює процеси їх своєчасного виявлення традиційними методами. Використання алгоритмів машинного навчання дозволяє аналізувати поведінкові характеристики користувачів, виявляти нетипову активність у мережі, аналізувати структуру мережевого трафіку та автоматично ідентифікувати потенційно небезпечні дії. У результаті формується інтелектуальне середовище ситуаційної обізнаності, здатне забезпечити оперативне реагування на кіберінциденти та підтримку управлінських рішень у режимі реального часу [2].

Не менш важливим напрямом є використання технологій штучного інтелекту для прогнозування кіберзагроз та моделювання можливих сценаріїв розвитку кіберінцидентів. У сучасних умовах управління кібербезпекою дедалі більше орієнтується на концепцію проактивного захисту, що передбачає не лише реагування на вже реалізовані атаки, але й прогнозування потенційних ризиків та попередження виникнення загроз. Використання предиктивної аналітики, нейронних мереж та системного моделювання дозволяє формувати математичні моделі розвитку кіберзагроз, оцінювати ймовірність реалізації кібератак та прогнозувати потенційні наслідки кіберінцидентів для інформаційної інфраструктури. У межах таких моделей штучний інтелект виконує функцію інтелектуального аналізатора, здатного інтегрувати різнорідні інформаційні потоки та формувати аналітичні рекомендації для суб'єктів управління у сфері кібербезпеки.

Особливу роль технології штучного інтелекту відіграють у процесі підтримки стратегічних управлінських рішень у діяльності правоохоронних органів. Сучасний кримінальний аналіз у сфері кібербезпеки потребує комплексного дослідження великих масивів інформації, інтеграції даних із різних джерел та формування аналітичних моделей, здатних відображати структуру та динаміку розвитку кіберзлочинності. Використання інтелектуальних аналітичних платформ дозволяє автоматизувати процеси збору, структуризації та інтерпретації інформації про кіберінциденти, формувати аналітичні профілі кіберзлочинних угруповань, виявляти закономірності їх діяльності та прогнозувати потенційні напрями розвитку загроз. У результаті правоохоронні органи отримують можливість приймати більш обґрунтовані

управлінські рішення, спрямовані на підвищення ефективності протидії кіберзлочинності [1,3].

У контексті системного аналізу технології штучного інтелекту виступають інструментом дослідження складних динамічних систем, до яких належить сучасний кіберпростір. Системний підхід дозволяє розглядати інформаційну інфраструктуру як багаторівневу систему взаємопов'язаних елементів, функціонування яких супроводжується постійними інформаційними потоками та ризиками виникнення кіберінцидентів. Використання інтелектуальних алгоритмів забезпечує можливість аналізу взаємозв'язків між елементами системи, виявлення слабких місць інформаційної інфраструктури та оцінювання рівня стійкості системи до зовнішніх і внутрішніх загроз. У межах такого підходу штучний інтелект виступає не лише інструментом автоматизації процесів аналізу, але й основою для формування адаптивних механізмів управління кібербезпекою.

Суттєвого значення набуває використання технологій штучного інтелекту у системах Threat Intelligence та інформаційно-аналітичних платформах ситуаційної обізнаності. Сучасні системи кіберрозвідки генерують значні обсяги інформації про кіберзагрози, джерела атак, шкідливе програмне забезпечення та вразливості інформаційних систем. Обробка таких масивів даних у ручному режимі є практично неможливою, що обумовлює необхідність використання інтелектуальних алгоритмів автоматизованого аналізу інформації. Використання штучного інтелекту дозволяє здійснювати автоматизовану кореляцію подій безпеки, виявляти приховані зв'язки між кіберінцидентами та формувати аналітичні прогнози щодо розвитку кіберзагроз.

Водночас активне впровадження технологій штучного інтелекту у сферу кібербезпеки супроводжується низкою складних проблем та викликів. Однією з ключових проблем є забезпечення достовірності та якості даних, які використовуються для навчання інтелектуальних систем. Наявність неповних, суперечливих або маніпулятивних даних може призводити до формування помилкових моделей та прийняття неефективних управлінських рішень. Крім того, значною проблемою залишається інтерпретованість рішень, сформованих інтелектуальними системами. Багато сучасних алгоритмів глибинного навчання функціонують за

принципом «чорної скриньки», що ускладнює процес пояснення логіки прийняття рішень та створює ризики у сфері управлінської діяльності [1].

Не менш актуальною проблемою є забезпечення інформаційної безпеки самих систем штучного інтелекту. Сучасні кіберзлочинці активно використовують механізми атак на моделі машинного навчання, маніпулювання навчальними вибірками та технології обходу систем автоматичного виявлення загроз. У зв'язку з цим особливого значення набуває формування стійких до атак інтелектуальних систем, здатних функціонувати в умовах активної кіберпротидії. Додатково актуалізуються питання етичного та правового регулювання використання штучного інтелекту у сфері кібербезпеки, оскільки автоматизація процесів прийняття рішень нерідко пов'язана із ризиками порушення прав людини, цифрової приватності та принципів інформаційної безпеки.

Перспективним напрямом розвитку технологій штучного інтелекту у сфері кібербезпеки є створення комплексних інтелектуальних платформ підтримки прийняття рішень, здатних інтегрувати функції моніторингу, прогнозування, аналізу ризиків та автоматизованого реагування на кіберінциденти. Використання технологій Big Data, хмарних обчислень, нейронних мереж та цифрових платформ ситуаційної обізнаності створює передумови для формування єдиного інформаційного середовища управління кібербезпекою. У межах такого середовища забезпечується автоматизований аналіз великих масивів інформації, моделювання сценаріїв розвитку кіберзагроз та підтримка стратегічних і тактичних управлінських рішень [2].

Таким чином, використання технологій штучного інтелекту для підтримки прийняття управлінських рішень у сфері кібербезпеки виступає одним із ключових напрямів розвитку сучасної системи забезпечення інформаційної безпеки держави. Інтеграція інтелектуальних алгоритмів у діяльність правоохоронних органів, інформаційно-аналітичних центрів та суб'єктів кіберзахисту дозволяє суттєво підвищити ефективність виявлення, аналізу та прогнозування кіберзагроз, забезпечити оперативність реагування на кіберінциденти та сформувати нову модель управління безпековими процесами в умовах цифрового суспільства. Подальший розвиток зазначеного напряму потребує вдосконалення

нормативно-правового забезпечення, розвитку інформаційної інфраструктури, підготовки висококваліфікованих фахівців у сфері кримінального аналізу та кібербезпеки, а також інтеграції сучасних технологій штучного інтелекту у практичну діяльність правоохоронних органів України.

Список використаних джерел:

1. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень/ за заг. ред. д.т.н., доц. О.А. Балтовського. Одеський держ. унів-т внутр. справ, 2022. 146 с.
2. Історія створення та розвитку систем підтримки прийняття рішень. URL:https://studme.org/212174/informatika
3. Левіна-Костюк М.О., Мельничук О.І., Телічко Н.О. Методи прийняття управлінських рішень в умовах недостатньої інформації URL:https://economyandsociety.in.ua/index.php/j ournal/article/view/1726/1663

THE PRINCIPLE OF CRIMINAL LEGALITY IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

GHERMAN-GRIMAILO Ana-Maria
Phd Student, University Assistant at „Ştefan cel Mare" Academy of the Ministry of Internal Affairs, Republic of Moldova
Department „Private Law"
ana-maria.gherman@mai.gov.md

The rule of legality constitutes a key challenge in the context of the development of artificial intelligence in modern states of law. So, the advancement of technologies, technological progress and the capacity of artificial intelligence to generate unpredictable actions raise major questions as to the applicability of this rule.

Moreover, adapting the rule of law to the new realities requires a rethink of the legal framework, in essence criminal laws need to be drafted that take technological aspects into account without infringing fundamental human rights. A balanced approach is needed, which maintains criminal law as a fundamental guarantee of individual freedom, but which also allows for the criminalization of crimes

committed with or through artificial intelligence. At the same time, technology in our age must remain a tool of justice, not a means of impunity and restriction of certain human rights. Artificial intelligence will never be able to take the place of the human judge.
Keywords: legality, artificial intelligence, accessibility, predictability.

Criminal legality means that no act can be considered a crime and no punishment can be imposed except on the basis of a law passed before the act was committed. This principle is a fundamental guarantee of the rule of law, which ensures predictability, stability and protection of citizens against arbitrary criminal acts and abuse of the law, but also ensures that justice is done fairly. Many authors may wonder what is the link between the legality approach and artificial intelligence, but the legality approach is of major importance in the context of challenges and changes that may arise in the process of justice, since any action, any change in the normative framework and in the procedural aspect must pass through the filter of legality.

We must bear in mind in particular that legality does not only address issues of predictability and clarity, accessibility of the rules as a whole, but also procedural fairness and the fairness of the administration of justice [7].

The progress of both human and artificial intelligence is constantly evolving and changing, and everything that is generated along the way is thanks to human intelligence, whereas artificial intelligence is emerging and progressing thanks to none other than human beings. Obviously, society must be as close as possible to the new challenges and keep pace with performance, but are these things natural in the context of modernizing the justice system of a state? Will this concept be a viable one within the justice system, a relevant and effective one within the state's legal system? Could a mechanism, a robot replace human strength, human thinking and human perception? Will this not eventually lead to a dehumanization of the law? Is this a relevant and unquestionable moment for our society? Will the fairness and legality of the criminalization of the act and the sentencing not be affected and clearly violated? Will the sentencing not constitute an abuse of the law, will the decision not be arbitrary and confusing? Will we not stumble over countless errors in the merits of the case? We are well aware that society will become even more innovative in the near future,

especially in the context of the adoption at European level of the „European Union Regulation on Artificial Intelligence" which recently entered into force, on August 1, 2024 [13]. Moreover, being the first law in the world to regulate Artificial Intelligence, the EU rules could set a global standard for the regulation of artificial intelligence, the world's countries being guided by the provisions of this law, but are all countries ready for this?

We believe that it is an idea that is still a legislative dilemma. However, what is really driving technological development and progress is the fact that artificial intelligence has in the last year become more and more a topic of discussion among young researchers (Stănilă, 2020), practitioners, and a strong point that demonstrated the possibility [15] of the emergence of artificial intelligence in our society was also the Nobel Prizes [10] for innovations in certain areas, which has indeed shown that we are approaching with small but rapid steps towards a change in many areas of life, towards technological progress, towards the embodiment of so-called robotized, automated mechanisms and perhaps sometimes their replacement by human power. However, one thing is certain in addressing this topical issue:

„Justice is for people, with people, for a normal functioning of society, and techniques and technologies will never be able to fully replace the human being, especially in such complex areas as justice".

We have a few issues regarding the emergence and evolution of artificial intelligence as a potential subject of discussion of the criminal law system.

For example, we are referring to the following facts:

1) Carrying out the hacking of the IA system as a result of which a crime has been committed;

2) The creation of an IA device by criminals for the purpose of committing offenses;

3) Admitting a technical error in the creation of the IA system which led to the commission of the offense;

4) The AI device decided to commit a crime, for example a bot, designed to write social media posts, composed a death threat „I want to kill people" and published it using the account of its owner, who was later held responsible for the bot's crime [14] (CLAUSSÉN-KARLSSON, 2017).

We fully agree with the idea that the current criminal codes are „built" for human subjects of criminal liability, being the natural person and the legal person, but not for digital entities, which may lead to impunity or misapplication of rules by analogy, which is inadmissible in the criminal law system.

So, the problem is who will be criminally liable when an automated system commits an unlawful act, the human perpetrator or the user?

With regard to procedural legality, we must say that the judge is the main actor of the justice system, having the role of guaranteeing respect for the law, fundamental rights and freedoms of citizens, [9] maintaining social balance, balance in justice, by resolving concrete and impartial disputes, representing an active, decision-making factor in the realization of justice[8].

The delegation of the judicial function to AI would not only undermine the independence of the judiciary, also will create serious risks in terms of the fairness of decisions, transparency and the right to a fair trial.

Respectively, this would also significantly contravene the fundamental principles of criminal procedure recognized in international law at the global level, not only the principle of legality. In this regard, we refer to the following principles of criminal procedure: the principle of the presumption of innocence, equality before the law and the authorities, respect for human rights, freedoms and dignity, inviolability of the person, independence of judges and their submission to the law, free appraisal of evidence [11].

At the same time, in this regard we refer to the clear violation of fundamental human rights, in the context of the European Convention on Human Rights, the violation of Articles 6 – „the right to a fair trial", 7 - „No punishment without law" [6].

In this sense, in conclusion we may say that automated mechanisms cannot guarantee real human impartiality, especially if the algorithm is influenced by some erroneous data [1].

Moreover, this would also exclusively violate the provisions of the Code of Criminal Procedure, in particular the provisions of the regulations „The administration of justice - exclusive competence of the courts", „Independence of judges and their submission only to the law", „Free appraisal of evidence" [2].

In this context, we deduce that in the era of artificial intelligence, when automated decisions influence more and more areas of life, the

principle of legality faces profound legal and ethical challenges in this respect. Our society is not ready for such a change, in order to confer the attributions of a human judge to a virtual judge. This is due to the blind trust that we, the society still have in technology. An aspect of major importance lies in the fact that the judicial decision implies above all human, transparent, predictable appreciation, it also implies a dose of empathy, balance in the appreciation of thoughts, morality, all those elements that are otherwise inaccessible and imperceptible to an automated system, a robot.

References:

1. BADEA C.A. (2020). Revoluția inteligenței artificiale în sistemul judiciar penal. penalmente relevant, pg. 122-157.

2. Code of Criminal Procedure of the Republic of Moldova, published at 05.07.2013 în MO Nr.248- 251, art.699.- art. 25-27.

3.Constitution of the Republic of Moldova. Constituţia (1994). as amended and supplemented on October 20, 2024. – Chişinău : Moldpres, 2024 (Universul). – 60, [1] p. [2000] ex. ISBN 978-9975-3618-2-8., art. 20.

4. CLAUSSÉN K. (2017). Artificial Intelligence and the External Element of the Crime. An Analysis of the Liability Problem. Final Thesis for the Law Program, Orebro University, p. 17.

5. DESCALUI E. (2022). INTELIGENȚA ARTIFICIALĂ DIN PERSPECTIVA DREPTULUI PENAL. USM Facultatea de drept, pg. 255-258.

6. European Convention for the Protection of Human Rights and Fundamental Freedoms.art.6. art. 7.

7. FLETCHER I, P. D. (2001). Concepte de bază ale justiției penale. Chișinău: Editura Arc.

8. Guide to the Organizational and Administrative Activities of the Courts. Chișinău, 2022.

9. Law No. 544 of July 20, 1995, on the Status of Judges // Official Gazette nr. 59-60 art. 664 din 26.10.1995.

10.On the Use of Artificial Intelligence in the Justice System. Available at: https://www.juridice.ro/758949/despre-utilizarea-.

11. Principiile procesului penal.USM, Note de curs.p. 2-5Available at:

https://moodle.usm.md/pluginfile.php/306774/mod_resource/content/0/Tema%20%20nr.3%20Principiile%20procesului%20%20penal.pdf- .

12. PRISĂCARU. (2012). Drept procesual penal. Partea generală. Chișinău: Tipograia Centrală.

13. Regulation on Artificial Intelligence. Available at: https://www.consilium.europa.eu/ro/policies/artificial-intelligence/ .

14. SAUD A. (2023). Criminal Liability about the Use of Artificial Intelligence: Investigating the Actus Reus Element of AI-driven Technology. American Journal of Law , pg. 1-25.

15. STĂNILĂ. (2020). Inteligența artificială, dreptul penal și sistemul de justiție penală. Amintiri despre viitor. București: Universul Juridic.

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ АВТОМАТИЗАЦІЇ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

Грезіна Олена Миколаївна
доктор філософії в галузі права,
доцент кафедри кримінального аналізу
та інформаційних технологій
Одеський державний університет внутрішніх справ

Динамічний розвиток інформаційно-комунікаційних технологій зумовив фундаментальну трансформацію методів збору, обробки та інтерпретації даних у наукових і прикладних дослідженнях. Ключове місце у цих перетвореннях посідає штучний інтелект (ШІ), що перетворився з вузькоспеціалізованого інструменту автоматизації на повноцінний когнітивний засіб підтримки аналітичної діяльності людини. Сучасні технології ШІ — зокрема методи машинного навчання, глибокі нейронні мережі та великі мовні моделі — уможливлюють опрацювання масивів неструктурованих даних, виявлення прихованих закономірностей і формування аналітичних висновків у режимі, близькому до реального часу, що принципово змінює продуктивність аналітичних процесів.

Дослідження засвідчують, що інтеграція ШІ до аналітичних процесів відбувається найактивніше у сфері управління знаннями та обробки інформаційних потоків. Управління знаннями стало однією з функцій найбільшого задокументованого рівня застосування ШІ. Показовим є те, що серед найпоширеніших практик

виокремлюється автоматизація захоплення, обробки та передачі інформації — тобто саме ті операції, які традиційно становлять основу аналітичної роботи: верифікація джерел, структурування даних, формування зведених звітів. Таким чином, ШІ виступає не лише засобом пришвидшення рутинних процедур, а й повноцінним інструментом підвищення якості аналітичних рішень [2].

Одним із найбільш затребуваних напрямів автоматизації аналітичної діяльності є обробка відкритих джерел інформації (OSINT — Open Source Intelligence). Аналітичні системи, що базуються на ШІ, здатні в автоматизованому режимі збирати, верифікувати та класифікувати відомості з різнотипних відкритих джерел — соціальних медіа, геопросторових баз даних, відкритих реєстрів та мережевих ресурсів. Думчиков М. О. у своєму дослідженні 2025 року обґрунтовує, що технологія AI-assisted OSINT істотно підвищує ефективність аналітичної діяльності завдяки автоматизації алгоритмів перевірки достовірності інформації та формуванню багаторівневих систем збору й верифікації даних [1]. Такі інструменти демонструють особливу ефективність у контексті протидії дезінформаційним кампаніям, де оперативність і точність аналізу набувають критичного значення.

Поряд із практичними здобутками, автоматизація аналітичної діяльності засобами ШІ породжує низку концептуальних і методологічних проблем. Насамперед, постає питання про рівень довіри до автоматизованих аналітичних висновків у порівнянні з результатами експертної діяльності людини. Технології ШІ характеризуються непрозорістю процесів прийняття рішень («чорна скринька»), схильністю до алгоритмічних упереджень і можливими похибками при обробці контекстуально складних або суперечливих даних.

Окремої уваги заслуговує питання автоматизації когнітивних аспектів аналітичної діяльності, що традиційно вважалися прерогативою людського інтелекту. Сучасні агентні системи ШІ здатні самостійно формулювати гіпотези, планувати послідовність аналітичних операцій і адаптувати стратегію дослідження залежно від проміжних результатів. За оцінками галузевих аналітиків, у 2025 році 29 % компаній вже використовують агентний ШІ, тоді як 44 % планують його впровадження протягом найближчого року. Зазнаена тенденція свідчить про поступовий перехід від ШІ як допоміжного інструменту до ШІ як повноправного учасника

аналітичних процесів, що потребує перегляду традиційних моделей організації інтелектуальної праці.

Узагальнюючи викладене, можна стверджувати, що штучний інтелект сформувався як системоутворювальний інструмент автоматизації аналітичної діяльності, що забезпечує якісно новий рівень ефективності роботи з даними. Водночас масштабне впровадження ШІ в аналітичні процеси потребує комплексного підходу, який поєднує технологічні рішення з правовим регулюванням, етичними стандартами та розвитком відповідних компетентностей аналітиків. Перспективним напрямом подальших досліджень є розроблення методологічних основ гібридних аналітичних систем, у яких штучний інтелект і людський експерт функціонують як взаємодоповнювальні компоненти єдиного процесу прийняття обґрунтованих рішень.

Список використаних джерел:

1. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство.* 2025. Т. 2, № 6. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.43

2. Форос Г.В., Калугін В.Ю., Грезіна О.М. Методологія кримінального аналізу в умовах зростання кіберзагроз. Юридичний науковий електронний журнал. № 11/2025.С. 356-359. https://doi.org/10.32782/2524-0374/2025-11/74

ІНТЕГРАЦІЯ OSINT В СИСТЕМУ КІБЕРБЕЗПЕКИ ДЕРЖАВИ: СТРАТЕГІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ

Демедюк Сергій Васильович
кандидат юридичних наук, доцент
Національна академія СБ України
Інститут дослідження кібервійни

Інформаційна відкритість сучасного цифрового середовища відкриває безпрецедентні можливості для збору, аналізу та інтерпретації даних, що формуються у відкритих джерелах. Open Source Intelligence (OSINT) перетворюється на невід'ємний інструмент забезпечення національної безпеки, а його інтеграція в систему кібербезпеки держави – на стратегічне завдання в умовах гібридної війни,

цифрової трансформації та зростання ролі інформаційного простору як арени конфліктів. Для України, яка перебуває у стані збройної боротьби з агресором, ефективне використання OSINT має не лише оперативне, але й екзистенційне значення.

OSINT — це систематизована діяльність із добування, аналізу та інтерпретації інформації з відкритих джерел: інтернету, соціальних мереж, відкритих баз даних, супутникових знімків, засобів масової інформації, форумів, даркнету, офіційної звітності тощо. На відміну від закритих джерел (HUMINT, SIGINT тощо), OSINT не потребує прихованих методів добування інформації, однак вимагає високої експертизи для відсіву фейків, маніпуляцій та дезінформації.

У кібербезпековому вимірі OSINT забезпечує *раннє виявлення загроз* (включаючи ознаки кібератак, витоки даних, активність бот-мереж), *атрибуцію атак* (зокрема через збір даних про групи хакерів, їхні інфраструктури та цифрові відбитки), *оцінку вразливостей* критичної інфраструктури через аналіз відкритих технічних даних, *контррозвідувальне забезпечення* (виявлення дезінформаційних кампаній, фішингових кампаній та елементів інформаційно-психологічних операцій (ІПсО)).

Таким чином, OSINT виступає одночасно як превентивний, аналітичний та доказовий інструмент у системі кібербезпеки.

Для того щоб OSINT був ефективно інтегрований у державну систему кібербезпеки, необхідно сформувати загальнодержавну концепцію, яка б визнавала відкриту розвідку як повноцінний елемент національного безпекового інструментарію. Таке визнання має знайти своє відображення у національних стратегічних документах, у тому числі з оновленою Стратегією кібербезпеки, Національним планом реагування на кіберінциденти та доктриною інформаційної безпеки. Важливо, щоб на рівні державної політики було визначено місце OSINT у структурі забезпечення інформаційної та кібербезпеки, з його використанням для виявлення дезінформаційних кампаній, інформаційно-психологічних операцій, а також у під час розслідування кіберзлочинів.

Важливою передумовою ефективної інтеграції OSINT є створення інституційної основи. В Україні досі не існує єдиного координаційного органу, який би відповідав за розвиток та системну реалізацію політики у сфері відкритої розвідки. Тому доцільним є створення *Національного центру OSINT*, який міг би

функціонувати у структурі Ради національної безпеки і оборони або як окремий міжвідомчий орган у взаємодії з Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, Кіберполіцією, Міністерством оборони та іншими суб'єктами сектору безпеки. Такий центр міг би координувати зусилля різних структур, формувати спільну аналітичну базу, забезпечувати обмін результатами досліджень та забезпечувати відповідну стандартизацію діяльності у сфері OSINT.

Не менш важливою складовою інтеграції є розробка єдиних методологічних стандартів. В умовах великої кількості джерел та високого рівня інформаційного шуму необхідно впровадити критерії перевірки достовірності інформації, методики аналізу достовірності джерел, правила документування та архівування даних. Це також має включати процедури збереження доказової інформації, яка може бути використана у правовому процесі, а також визначення правових і технічних стандартів взаємодії OSINT-аналітиків із правоохоронними та розвідувальними структурами.

Технологічна база є ще одним ключовим чинником. Сучасна аналітика OSINT базується на використанні спеціалізованих програмних засобів, таких як системи автоматизованого збору даних (web crawlers), парсери, інструменти для виявлення цифрових відбитків (digital footprinting), платформи для аналізу соціальних мереж, системи аналізу супутникових знімків, а також інструменти візуалізації та картографування зібраної інформації. Розвиток національної програмної інфраструктури у цьому напрямі потребує залучення інноваційного потенціалу вітчизняних компаній та стартапів, які вже активно працюють у сфері OSINT та кіберрозвідки.

Не менш важливою є підготовка відповідних кадрів. Станом на сьогодні кадровий потенціал у сфері відкритої розвідки є обмеженим. Відсутність спеціалізованих освітніх програм, невизначеність правового статусу OSINT-діяльності, а також недостатня кількість сертифікаційних курсів ускладнює процес формування професійної спільноти аналітиків. Потрібно розробити стандартизовані навчальні програми для студентів ІТ-спеціальностей, права та національної безпеки, ввести обов'язкову підготовку з елементами OSINT для співробітників кіберполіції, СБУ, військових аналітиків, а також запровадити систему післядипломної освіти та підвищення кваліфікації у цій сфері.

Юридичне регулювання є окремим та важливим питанням. Застосування OSINT у кримінальних провадженнях, оперативно-розшуковій та розвідувальній діяльності потребує чіткого врегулювання. На сьогодні законодавство України не визначає повноцінно статус відкритих джерел як доказів у судовому процесі. Це створює певну правову невизначеність. Необхідно внести відповідні зміни до Кримінального процесуального кодексу, закону про оперативно-розшукову діяльність, закону про розвідку, а також до підзаконних нормативних актів, що регулюють роботу спеціальних служб. Важливо забезпечити баланс між правом держави на захист безпеки та правом громадян на захист персональних даних, що є актуальним як у національному, так і в європейському контексті.

Окремої уваги потребує взаємодія держави з громадянським суспільством та волонтерськими ініціативами, які вже довели свою ефективність у сфері відкритої розвідки. Український досвід, зокрема діяльність таких спільнот, як InformNapalm, OSINT-UA, Molfar, Bellingcat та інших, показує, що громадські аналітики здатні оперативно і точно ідентифікувати ворожі угрупування, викривати схеми фінансування окупаційних адміністрацій, а також розкривати злочини, вчинені під час бойових дій. Держава має створити правові механізми залучення таких структур до офіційного процесу реагування на загрози, забезпечити підтримку їх діяльності, включно з технічними ресурсами, правовою допомогою та доступом до відкритих державних реєстрів.

Таким чином, інтеграція OSINT у систему кібербезпеки держави має розглядатися як складова загального реформування сектору національної безпеки. Вона повинна базуватися на чітко визначеній стратегії, інституційному забезпеченні, законодавчій підтримці, розвитку кадрового потенціалу та побудові сучасної технологічної інфраструктури. Лише за таких умов можна забезпечити ефективне використання відкритої інформації для виявлення, попередження та нейтралізації кіберзагроз, які дедалі більше стають ключовими інструментами сучасної війни.

ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНАЛЬНОМУ АНАЛІЗІ: ПРАКТИЧНИЙ ДОСВІД ТА ПРОБЛЕМНІ ПИТАННЯ

Клименко Вячеслав Анатолійович
заступник начальника управління кримінального аналізу
Головного управління Національної поліції
в Одеській області, підполковник поліції

Стрімкий розвиток технологій штучного інтелекту (ШІ) суттєво змінює методи протидії злочинності та організацію аналітичної роботи в органах Національної поліції України. Інструменти автоматизованого розпізнавання обличчя дозволяють суттєво скоротити час ідентифікації осіб, причетних до кримінальних правопорушень, проте їх упровадження супроводжується низкою невирішених правових, технічних і організаційних питань. Метою цієї роботи є узагальнення практичного досвіду застосування ШІ-інструментів в аналітичній діяльності УКА ГУНП в Одеській області та формулювання пропозицій щодо вдосконалення нормативної бази й організаційного забезпечення цього напряму.

У практичній діяльності аналітичних підрозділів ГУНП в Одеській області застосовуються три основні системи. Clearview AI демонструє точність розпізнавання 99,6% (за даними NIST) і використовує базу понад 10 млрд фотозображень (з яких близько 2 млрд отримано з ресурсу «ВКонтакте»), що дозволяє ідентифікувати особу навіть за зображенням низької якості; з її допомогою в Україні встановлено особи понад 10 тис. осіб. Кожен запит до системи підлягає обов'язковій реєстрації із зазначенням номера кримінального провадження та мети звернення.

BigData People Artellence формує 360-градусний профіль особи (телефонні номери, акаунти в соціальних мережах, родинні зв'язки), уможливлює пошук за фотографією, номером телефону чи посиланням на профіль, а також виявляє зв'язки особи з державою-агресором; водночас система потребує якісного вхідного зображення.

Face-chek (ІПНП НПУ) — внутрішня система з базою близько 2 млн фотозображень (обліки «Особа», «Розшук», «Безвісти зниклі», «Блокпост», «Сепаратисти», «Зброя»), що забезпечує миттєве розпізнавання з виведенням прізвища, імені та по батькові й не створює додаткових правових ризиків, оскільки є відомчою розробкою.

Робота аналітика з ШІ-системами розпізнавання обличчя реалізується за такою послідовністю: 1) отримання вихідного матеріалу (відеозапису або фотозображення особи); 2) завантаження матеріалу в систему (Clearview AI / BigData / Face-chek); 3) аналіз результатів пошуку — формування переліку найбільш схожих осіб із пріоритетом збігів понад 90%; 4) критичний аналіз — верифікація аналітиком постійних і тимчасових ознак зовнішності; 5) перехресна перевірка отриманих даних за іншими інформаційними системами (ІПНП «Цунамі», НАІС, ДМС, «Гепард» тощо); 6) формування аналітичного продукту — обґрунтованого висновку з доказовою базою.

Принципове значення має четвертий етап: практика свідчить, що збіг на рівні 40–60% подекуди виявляється правильним, тоді як формально високий показник у 90% може бути помилковим. Це підтверджує тезу про незамінність критичного мислення аналітика навіть за використання високоточних автоматизованих систем.

Ключові проблеми застосування ШІ:

1. правова неврегульованість. В Україні відсутнє спеціальне законодавство щодо застосування ШІ правоохоронними органами. Показовим є випадок штрафу компанії Clearview AI у Нідерландах на суму 30,5 млн євро, що актуалізує ризики невідповідності вимогам GDPR у контексті євроінтеграційних процесів;
2. відсутність API-доступу до державних реєстрів. Аналітики змушені вручну опрацьовувати дані з ІПНП, НАІС, ДМС, «Гепард», що призводить до значних витрат часу на структурування інформації замість безпосередньо аналітичної роботи;
3. відставання системи підготовки аналітиків. Дипфейки, кіберфрод, злочини з використанням криптовалют і ШІ-згенерованого контенту з'являються швидше, ніж оновлюються відповідні навчальні програми;
4. відсутність обліку камер приватного сектору. Магазини, підприємства та ОСББ встановлюють камери відеоспостереження без погодження з органами поліції; єдиний реєстр та доступ до таких камер відсутні, що ускладнює проведення розслідувань.

На підставі викладеного пропонується: розробити Положення «Про застосування штучного інтелекту у правоохоронній діяльності» та відомчий наказ МВС, що регламентує роботу з системами розпізнавання, з обов'язковою реєстрацією кожного запиту

(номер справи, мета, посадова особа); забезпечити захищену API-інтеграцію підрозділів кримінального аналізу з ІПНП, НАІС, ДМС через міжвідомчу інтеграційну шину даних НПУ, що автоматизує рутинні запити та вивільнить час аналітика; запровадити практичні курси з ШІ-інструментів у партнерстві з ОДУВС та ГУНП із навчанням на реальних кейсах і міжрегіональним обміном досвідом; ухвалити нормативно-правовий акт про обов'язкове погодження встановлення вуличних камер і створити єдиний реєстр камер із доступом підрозділів кримінального аналізу до відеоматеріалів для оперативного аналізу.

Застосування інструментів штучного інтелекту суттєво підвищує ефективність кримінального аналізу, однак не замінює аналітика — критичне мислення людини залишається визначальним чинником достовірності результатів. Пріоритетним напрямом є нормативно-правове врегулювання застосування ШІ відповідно до європейських стандартів (GDPR). Інтеграція державних реєстрів через захищені API дозволить скоротити рутинне навантаження та збільшити частку часу, що витрачається на власне аналітичну роботу. Підготовка аналітиків потребує системної перебудови навколо ШІ-компетенцій у партнерстві з ОДУВС та ГУНП, а створення єдиного реєстру камер відеоспостереження сформує нову якість аналітичного забезпечення правоохоронної діяльності.

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ МОНІТОРИНГУ ДЛЯ ВИЯВЛЕННЯ ТА АНАЛІЗУ КІБЕРІНЦИДЕНТІВ

Лозовий Олег Володимирович, *аспірант*
Одеського державного університету внутрішніх справ.

Сучасний розвиток цифрової інфраструктури та зростання складності кіберзагроз зумовлюють необхідність переходу від традиційних методів виявлення атак до інтелектуальних систем моніторингу, здатних здійснювати аналіз подій у режимі реального часу. Класичні підходи, що базуються на сигнатурному аналізі, демонструють обмежену ефективність в умовах появи нових,

раніше невідомих типів атак, зокрема цілеспрямованих атак (APT) та атак нульового дня. У цьому контексті особливого значення набувають системи класу SIEM (Security Information and Event Management) та UEBA (User and Entity Behavior Analytics), які інтегрують методи машинного навчання для виявлення аномалій у поведінці користувачів і мережевих об'єктів.

Інтелектуальні системи моніторингу кіберінцидентів ґрунтуються на концепції багаторівневої обробки даних, що включає збір телеметрії, агрегацію журналів подій, кореляційний аналіз та автоматизоване виявлення відхилень. Як зазначається у дослідженні, присвяченому моделі ZenGuard, сучасні SIEM-рішення поєднують механізми Zero Trust, UEBA та алгоритми машинного навчання для підвищення точності ідентифікації загроз та зменшення кількості хибнопозитивних спрацьовувань [1]. Такий підхід дозволяє здійснювати контекстно-залежний аналіз подій, враховуючи не лише сам факт інциденту, але й поведінкові патерни користувачів та сутностей у мережі.

Важливою складовою інтелектуальних систем моніторингу є застосування алгоритмів штучного інтелекту для виявлення аномалій у великих обсягах даних. Використання методів машинного навчання, зокрема нейронних мереж, моделей класифікації та кластеризації, дозволяє адаптивно реагувати на зміну поведінкових патернів у кіберпросторі. У дослідженні UEBA-систем у межах SIEM підкреслюється, що AI-орієнтовані моделі значно підвищують здатність системи до виявлення складних та прихованих атак, які не можуть бути ідентифіковані традиційними методами аналізу логів [2]. Таким чином, інтелектуалізація процесів моніторингу забезпечує перехід до проактивної моделі кіберзахисту.

Архітектурно сучасні системи кібермоніторингу будуються як багатокомпонентні платформи, що включають модулі збору даних, аналітичні ядра та підсистеми автоматизованого реагування. Особливу роль відіграють механізми кореляції подій, які дозволяють об'єднувати окремі сигнали в цілісну картину кіберінциденту. У цьому контексті застосування штучного інтелекту забезпечує не лише виявлення загроз, але й прогнозування їхнього розвитку, що є критично важливим для об'єктів критичної інфраструктури.

Окремої уваги потребує проблема зменшення кількості хибнопозитивних спрацювань, яка традиційно є однією з ключових у

системах SIEM. Інтелектуальні алгоритми дозволяють здійснювати динамічне налаштування порогових значень та адаптацію моделей виявлення відповідно до зміни поведінкових патернів у мережі. Як показано в дослідженнях, інтеграція UEBA та AI-підходів у SIEM-системи сприяє підвищенню точності детекції та оптимізації процесів реагування на інциденти [2].

У практичному аспекті інтелектуальні системи моніторингу кіберінцидентів дедалі частіше використовуються у державному секторі, фінансових установах та критичній інфраструктурі. Це пов'язано з необхідністю обробки великих обсягів гетерогенних даних у режимі реального часу та забезпечення високого рівня кіберстійкості. Застосування моделей машинного навчання в таких системах дозволяє автоматизувати процеси первинного аналізу інцидентів, що суттєво зменшує навантаження на аналітиків кібербезпеки та підвищує швидкість реагування.

Разом із тим, впровадження інтелектуальних систем моніторингу супроводжується низкою викликів, серед яких слід виділити питання захисту даних, забезпечення прозорості алгоритмів прийняття рішень та стійкості моделей до атак на самі системи штучного інтелекту. Додатково актуальною проблемою є необхідність інтеграції різнорідних джерел даних у єдину аналітичну платформу, що вимагає стандартизації форматів обміну інформацією та підвищення сумісності між компонентами кіберінфраструктури.

У перспективі розвиток інтелектуальних систем моніторингу буде пов'язаний із подальшою інтеграцією технологій глибинного навчання, федеративного навчання та автономних агентних систем, здатних не лише виявляти, але й самостійно реагувати на кіберінциденти. Це формує нову парадигму кіберзахисту, в якій людина виступає як стратегічний контролер, тоді як оперативний рівень аналізу та реагування дедалі більше автоматизується.

Таким чином, інтелектуальні системи моніторингу кіберінцидентів є ключовим елементом сучасної архітектури кібербезпеки, що забезпечує підвищення ефективності виявлення загроз, скорочення часу реагування та формування адаптивної моделі захисту інформаційних ресурсів.

Список використаних джерел

1. Hassan A., Rauf A., Shafqat N., Latif R., Khan H. *ZenGuard a machine learning based zero trust framework for context aware*

threat mitigation using SIEM SOAR and UEBA. Scientific Reports, 2025, Vol. 15, Article 35871. URL: https://www.nature.com/articles/s41598-025-20998-4 .

2. Aljumaily M. S., Abd H. K., Majeed E. *Enhancing User and Entity Behavior Analytics in SIEM Systems Using AI-Powered Anomaly Detection: A Data-Driven Simulation Approach*. International Journal of Mechatronics, Robotics, and Artificial Intelligence, 2025, Vol. 1(2). DOI: https://doi.org/ 10.33971 /ijmrai.1.2.11.

АВТОМАТИЗАЦІЯ ОБРОБКИ ВІЗУАЛЬНИХ ДАНИХ У КРИМІНАЛЬНОМУ АНАЛІЗІ: СУЧАСНИЙ ІНСТРУМЕНТАРІЙ ТА АЛГОРИТМИ*

Манжай Олександр Володимирович
к.ю.н., професор, завідувач кафедри
протидії кіберзлочинності ННІ № 4
Харківського національного університету внутрішніх справ
Манжай Ірина Андріївна
старший викладач кафедри
інформаційних систем та технологій ННІ № 4
Харківського національного університету внутрішніх справ

У повсякденній роботі підрозділів кримінального аналізу Національної поліції України регулярно виникають завдання, пов'язані з глибокою обробкою, відновленням та аналізом цифрових зображень. З огляду на стрімкий розвиток технологій штучного інтелекту (ШІ) та комп'ютерного зору, доцільно виокремити шість найбільш перспективних напрямів автоматизації та оптимізації роботи з візуальними даними:

1) *покращення якості фотознімків та відеокадрів для ідентифікації.* Першим напрямом є відновлення розмитих стопкадрів з відеопотоку чи фотографій низької якості з метою ідентифікації зображених на них осіб та предметів. Для досягнення найкращого

* Дослідження виконано в рамках НТР за договором із МОН № ДЗ / 162 - 2025 від 11.02.2025

результату рекомендується застосовувати не поодинокі ШІ-інструменти, а їх послідовні комбінації. Алгоритм комплексного покращення може виглядати так: *первинне покращення* (remini.ai) → *видалення водяних знаків* (watermarkremover.io) → *моделювання потенційного зображення* (replicate.com/ sczhou/ codeformer, imglarger.com/repair, jpghd.com тощо) → *фінальне збільшення без втрати якості* (waifu2x.net). Вибір конкретних інструментів здійснюється експериментальним шляхом залежно від специфіки вихідного файлу (рис. 1) [1, с. 170].

Рис. 1. Приклад зображення обличчя, послідовно удосконаленого двома сервісами

2) *моделювання реалістичного фоторобота за ізороботом*. Другий напрям покликаний підвищити ефективність ідентифікації правопорушників, зовнішність яких відтворена художником зі слів очевидців. Для створення максимально реалістичної фотографії правопорушника застосовується такий алгоритм:

- формування базового зображення за допомогою генеративних ШІ-сервісів (imgtoimg.ai, dreamstudio.stability.ai);
- перенесення рис обличчя на згенероване фото з використанням спеціалізованих інструментів (wapfaces.ai, faceswapper.ai, pixlr.com/express).

Приклад реалізації цього завдання наведено на рис. 2.

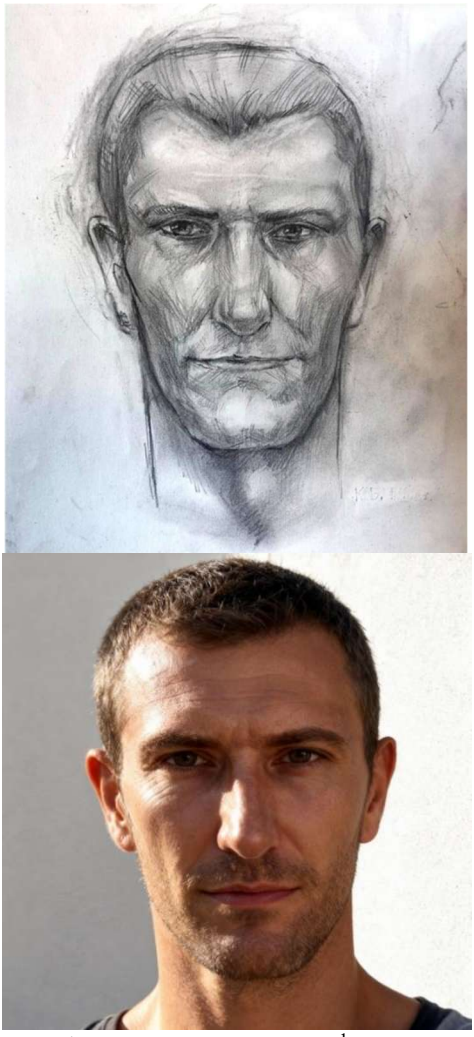

Рис. 2. Ізоробот правопорушника[1] та створена модель фоторобота

[1]. На Харківщині невідомий згвалтував і задушив 15-річну дівчинку. Фоторобот. URL: https://tsn.ua/ukrayina/na-harkivschini-nevidomiy-zgvaltuvav-i-zadushiv-15-richnu-divchinku-fotorobot-1244328.html (дата звернення: 09.04.2026).

3) **Вікове прогресування зовнішності зниклих безвісти осіб** Під час оперативно-службової діяльності виникає потреба ідентифікації безвісти зниклих осіб із урахуванням часу, що минув з моменту їхнього зникнення, та ймовірних умов перебування. За допомогою нейромереж (imgtoimg.ai, dreamstudio.stability.ai) аналітики можуть змоделювати актуальний вигляд особи на основі старих фотографій. Специфічний запит для ШІ може формулюватися так:

Show what will this man look like in a photo four years from now if he is living in difficult conditions, malnourished, and suffering. Make his head bald and remove his beard and mustache. Make his face as similar to the original as possible, not counting the changes I mentioned.

4) *відновлення навмисно спотворених (пікселізованих) зображень*. Четвертий напрям передбачає розкриття облич чи об'єктів, які були навмисно спотворені. Оскільки методи спотворення різняться, способи їх відновлення також потребують індивідуального підходу. Якщо, наприклад, була виконана пікселізація фотографії особи, то для відновлення її обличчя можна скористатися послідовним застосуванням декількох інструментів. Спершу відкрити саме зображення у редакторі. Для цього можна скористатися, наприклад, редактором GIMP (gimp.org). У згаданій програмі потрібно активувати Фільтри → Розмиття → Розмиття за Гаусом… та збільшувати рівень розмиття, доки не зникнуть квадрати пікселізації. Після цього за необхідності можна створити дублікат шару (Shift+Ctril+D) та надати зображенню більшої чіткості, для чого за допомогою меню Фільтри → Виявлення меж відобразити Градієнт зображення… і потім з використанням Колір → Яскравість-контрастність… збільшувати контрастність до набуття контурами обличчя прийнятного рівня (рис. 3). Після цього у правому фреймі слід обрати режим «Лише освітлення яскравості». Відновлене таким чином зображення можна спробувати покращити далі за допомогою інших інструментів, наприклад, на базі штучного інтелекту, або одразу подати на вхід інформаційно-пошукової системи чи програми розпізнавання облич.

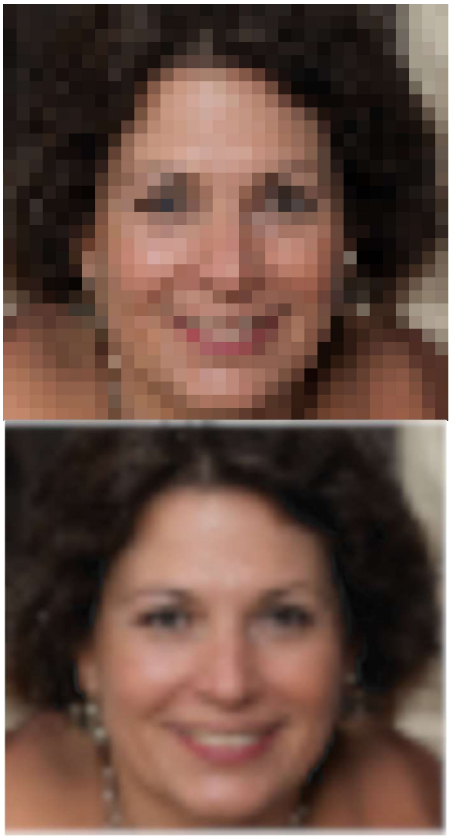

Рис. 3. Зображення до відновлення[2] та після відновлення

5) *ідентифікація нерозбірливих державних номерних знаків*. П'ятим напрямом є розпізнавання номерних знаків автотранспорту з камер відеоспостереження у випадках, коли традиційні ШІ-засоби покращення різкості виявляються безсилими. Для цього доцільно використовувати спеціалізоване ПЗ, таке як Forensic Plate (sourceforge.net/projects/forensic-plate). Ця програма використовує математичний підхід. Замість візуального усунення розмитості вона генерує всі можливі комбінації символів з алфавіту і

[2]. Оригінальне зображення згенеровано за допомогою ресурсу thispersondoesnotexist.com та пікселізовано з використанням Paint Net.

обчислює їхню кореляцію з наявними розмитими кадрами. Це дозволяє суттєво звузити масив можливих номерів для оперативної перевірки (рис. 4).

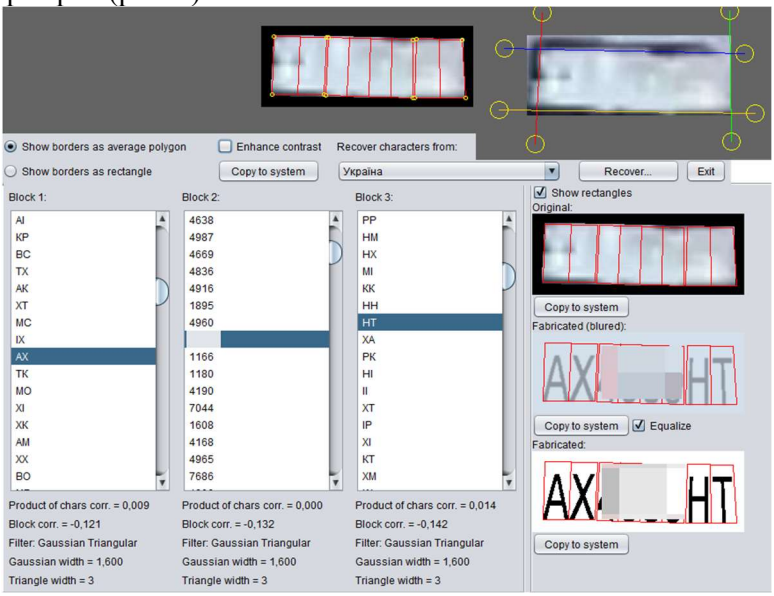

Рис. 4. Відновлення даних номеру з використанням Forensic Plate

Як видно по розташуванню повзунків, шуканий номер було ідентифіковано досить успішно, тому що по суті масив можливих номерів для перевірки було суттєво звужено. Також слід зважати, що дане розпізнавання було виконано на основі одного знімку.

6) *уніфікація та стандартизація масивів фотоданих*. Останнім напрямом є приведення великої кількості неоднорідних фотографій до єдиного формату (наприклад, для завантаження в бази даних чи системи машинного навчання). На практиці аналітики часто стикаються з фотографіями різних ракурсів, освітлення, або навіть зі знімками документів (паспортів, прав), де обличчя розташоване під кутом. Завдання полягає в автоматизованому вилученні облич, їх вирівнюванні та збереженні у стандартизованому вигляді. Ефективний алгоритм розв'язання цієї проблеми докладно описаний авторами в попередньому дослідженні «Solving

specific tasks of face image processing and analysis using artificial intelligence based tools» [2].

Отже, застосування сучасних інструментів обробки зображень суттєво розширює аналітичні можливості правоохоронних органів. Як свідчить практика, відмова від використання ізольованих програм на користь комплексних багатокрокових алгоритмів із поєднання генеративного штучного інтелекту, математичної кореляції та класичних графічних редакторів дає змогу ефективно вирішувати найскладніші оперативні завдання: від ідентифікації осіб за пікселізованими кадрами до розшуку зниклих безвісти та деобфускації номерних знаків. Подальша алгоритмізація цих процесів є ключовою умовою підвищення результативності підрозділів кримінального аналізу.

Список використаних джерел:

1. Манжай О. В. Поліцейська діяльність у кіберсфері : підручник / О. В. Манжай ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2024. 188 с. URL: https://dspace.univd.edu.ua/handle/123456789/23140.

2. Sokurenko V., Rusyn B., Manzhai O., Nosov V., Luchyk S., Luchyk V. Solving specific tasks of face image processing and analysis using artificial intelligence based tools. *Proceedings of the International Workshop on Applied Intelligent Security Systems in Law Enforcement (AISSLE-2025)* (Vinnytsia, Ukraine, October 30–31, 2025). Vinnytsia : KNUIA, 2025. P. 186–203. URL: https://ceur-ws.org/Vol-4126/paper13.pdf.

ЦИФРОВІ ПЛАТФОРМИ КРИМІНАЛЬНОГО АНАЛІЗУ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Моргунова Тетяна Іванівна
к.т.н., доцент, доцент кафедри
кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ

Сучасна система забезпечення правопорядку вже давно не виглядає такою простою, як її іноді намагаються описати в підручниках. Кримінальні загрози ніби розповзаються у різні боки, стають складнішими, переплітаються між країнами, і все це ще й

активно підживлюється цифровими технологіями. Іноді складається враження, що швидкість змін тут навіть вища, ніж у бізнес-середовищі, хоча це різні сфери. За таких умов звичні підходи до кримінального аналізу починають виглядати дещо застарілими, навіть якщо формально вони працюють.

Тому поступово виникає потреба переходити до більш гнучких і «розумних» інструментів, зокрема цифрових платформ, які здатні не просто накопичувати дані, а щось із ними робити в режимі, близькому до реального часу.

Якщо говорити про самі ці платформи, то їх складно звести до якогось одного визначення. Це швидше набір взаємопов'язаних рішень, які одночасно і збирають інформацію, і обробляють її, і намагаються показати аналітику певну картину подій. Причому мова не лише про факти, а й про зв'язки між людьми, повторювані моделі поведінки, інколи навіть такі речі, які не лежать на поверхні. У традиційних системах зазвичай все обмежувалося фіксацією інформації, тоді як тут з'являється елемент «домислення», якщо так можна сказати, хоча це, звісно, алгоритми, а не інтуїція. Втім, іноді результат виглядає дуже схоже.

Штучний інтелект у цьому контексті використовується доволі широко, хоча не завжди це помітно на перший погляд. Машинне навчання, наприклад, дозволяє виявляти певні закономірності, які людина могла б і пропустити, особливо коли даних багато. Обробка текстів теж відіграє роль, бо значна частина інформації існує у вигляді звітів, повідомлень, пояснень. Десь поруч і комп'ютерний зір, який аналізує відео з камер, хоча якість цих даних буває різною, і це теж проблема. Усе це разом поступово змінює саму логіку аналітичної роботи, скорочує час на прийняття рішень, але повністю виключити людський фактор все одно не виходить, та й навряд чи це потрібно.

Окремо варто згадати про різні джерела інформації, які ці платформи намагаються об'єднати. Дані з внутрішніх баз, відкриті джерела, відеоспостереження, інформація з мобільних пристроїв або фінансових операцій – усе це збирається в одному місці, хоча на практиці не завжди ідеально стикується. Іноді виникають труднощі з сумісністю форматів або з якістю даних, але загальна тенденція очевидна: формується певний єдиний інформаційний простір, у якому можна дивитися на ситуацію ширше, ніж раніше.

Хоча це теж не панацея, бо надлишок інформації іноді створює нові складнощі.

Структура таких платформ теж не є чимось абсолютно чітким і раз і назавжди заданим. Вона змінюється під потреби конкретних органів або навіть під окремі завдання. Зазвичай можна говорити про певні базові елементи, але їх межі досить умовні, і в реальній роботі вони часто перетинаються. Тому функціональні можливості таких систем краще розглядати не як жорстко визначений перелік, а як набір інструментів, який постійно доповнюється і трохи змінюється залежно від ситуації. І, мабуть, саме ця гнучкість і є однією з ключових їх характеристик, навіть якщо про це не завжди прямо говорять.

У цьому контексті доцільно підкреслити, що саме платформний підхід у поєднанні з інструментами штучного інтелекту формує якісно новий рівень кримінального аналізу. Йдеться не просто про автоматизацію окремих функцій, а про створення єдиного середовища, у якому дані, аналітичні алгоритми та управлінські рішення взаємодіють у межах узгодженої логіки. Штучний інтелект у таких системах виступає не допоміжним елементом, а центральним механізмом, що забезпечує адаптивність, здатність до самооновлення моделей і підвищення точності аналітичних висновків. Завдяки цьому цифрові платформи набувають ознак динамічних систем, які можуть не лише відображати поточний стан криміногенної ситуації, але й активно впливати на процеси прийняття рішень у правоохоронній діяльності.

Важливою перспективою розвитку є застосування ШІ для предиктивного аналізу злочинності та створення профілів потенційних злочинців. Алгоритмічні моделі ШІ активно використовуються для ідентифікації та відстеження серійних злочинців шляхом виявлення спільних рис у різних кримінальних епізодах, підвищуючи рівень громадської безпеки. Завдяки прогностичним можливостям ШІ правоохоронні структури отримують інструменти для формування обґрунтованих прогнозів щодо часових, територіальних та якісних характеристик злочинності, що дозволяє більш ефективно розподіляти патрульні сили, слідчі групи та інші ресурси [1].

Застосування штучного інтелекту в криміналістичній діяльності є перспективним напрямом, що відкриває нові можливості для підвищення ефективності розкриття злочинів, автоматизації

рутинних завдань, прогнозування злочинності та аналізу великих обсягів даних [2].

Звернемо увагу на ключові складові цифрових платформ кримінального аналізу, які визначають їх ефективність (табл. 1).

Якщо дивитися на ці всі компоненти не окремо, а разом, то поступово стає зрозуміло, що вся ця історія з цифровими платформами тримається не стільки на самих технологіях, скільки на тому, як вони між собою «домовляються».

Слід відзначити, що можна мати доволі потужні модулі, але якщо вони працюють уривчасто або дані заходять із помилками, то результат виходить, м'яко кажучи, не дуже. Іноді проблема навіть не в складності алгоритмів, а в банальній якості інформації на вході, яка тягне все вниз.

Таблиця 1

Ключові компоненти цифрових платформ кримінального аналізу на основі штучного інтелекту

Компонент платформи	Зміст та функціональне призначення
Модуль збору даних	Забезпечує інтеграцію даних із внутрішніх і зовнішніх джерел, включаючи бази даних, сенсори, соціальні мережі
Аналітичний модуль	Використовує алгоритми машинного навчання для виявлення закономірностей, кластеризації та прогнозування
Модуль обробки природної мови	Дозволяє аналізувати текстову інформацію (заяви, протоколи, повідомлення в мережі)
Візуалізаційний модуль	Забезпечує графічне представлення результатів аналізу (карти, графи зв'язків, дашборди)
Модуль прийняття рішень	Формує рекомендації для правоохоронних органів на основі аналітичних висновків
Система безпеки даних	Гарантує захист інформації, контроль доступу та відповідність нормативним вимогам

У підсумку прогнози виглядають переконливо лише формально, а рішення, які на них спираються, можуть не давати очікуваного ефекту.

Досить часто згадують машинне навчання, особливо коли мова заходить про прогнозування кримінальної активності. І воно справді дає цікаві результати, дозволяє побачити певні «гарячі точки», часові періоди, коли ризики зростають, або навіть виділити людей, які можуть бути дотичними до правопорушень. Але тут не все так однозначно. Є нюанси, про які інколи говорять неохоче: алгоритми можуть відтворювати старі перекоси, підсилювати їх, якщо дані були упередженими. Це вже виходить за межі техніки і заходить у площину етики, прав людини, і загалом довіри до таких систем. Без цього моменту вся «розумність» платформи виглядає трохи під питанням.

Ще один напрям, який останнім часом активно використовують, пов'язаний з аналізом соціальних мереж. Через ці інструменти намагаються розплутати структури груп, зрозуміти, хто з ким взаємодіє, хто відіграє ключову роль. Інколи це справді допомагає швидше вийти на організовані групи або побачити те, що раніше залишалося поза увагою. Хоча знову ж таки, не все так гладко: інформація з відкритих джерел буває суперечливою, і її інтерпретація може змінюватися залежно від контексту.

Разом із тим, впровадження таких платформ не обмежується лише технічними рішеннями. Тут одразу виникає цілий набір практичних моментів – фінанси, підготовка спеціалістів, питання безпеки даних. Іноді складається враження, що організаційна складова навіть складніша за технологічну. Додається ще й правове поле, яке не завжди встигає за розвитком технологій, особливо коли йдеться про штучний інтелект. Це створює певну невизначеність, яку доводиться якось обходити в реальній практиці.

В українських умовах усе це відчувається ще гостріше. Війна, кіберзагрози, нестабільність – ці фактори ніби підштовхують до швидшого впровадження нових рішень, але водночас ускладнюють сам процес. Іноді доводиться працювати з тим, що є, паралельно намагаючись модернізувати систему. Тут цифрові платформи могли б стати корисним інструментом, хоча їх ефективність напряму залежить від того, наскільки грамотно вони інтегровані у вже існуючі процеси.

Цікаво, що в інших країнах, особливо в Європі, подібні системи вже використовуються доволі активно. Там тестують різні підходи – від прогнозної аналітики до розпізнавання облич і аналізу поведінки. Це дозволяє економити ресурси, швидше реагувати, хоча й там не обходиться без дискусій щодо меж допустимого. Певною мірою ці приклади можна брати до уваги, але повністю копіювати їх, мабуть, не вийде.

Зрештою, все впирається в баланс. З одного боку – ефективність, швидкість, аналітика, яка дає нові можливості. З іншого – права людини, етичні обмеження, відповідальність за рішення, які приймаються на основі алгоритмів. Якщо цей баланс порушується, довіра до системи швидко зникає, навіть якщо вона технічно працює добре.

У підсумку можна сказати, що ці цифрові платформи виглядають перспективно, але їх розвиток не є прямолінійним. Це скоріше поступовий процес із великою кількістю нюансів, де технічні, організаційні та правові речі переплітаються між собою. І саме від того, як це все поєднається, залежить, чи дадуть вони реальний ефект, чи залишаться більше теоретичною перевагою.

Список використаних джерел:

1. Яровий К. Штучний інтелект як інструмент протидії злочинності. *Юридичний вісник. Повітряне і космічне право*. 2024. № 2. С. 68-76.

2. Черваньова Д.А., Курман О.В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство*. 2025. Т. 3, № 3. С. 211-216. DOI: https://doi.org/10.24144/2788-6018.2025.03.3.31

МІЖНАРОДНИЙ ДОСВІД РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ БЕЗПЕКИ

Моргунова Тетяна Іванівна
к.т.н., доцент, доцент кафедри
кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ
https://orcid.org/0000-0002-3512-2425
М'ясоєдова Анастасія Григорівна
здобувач першого (бакалаврського)
рівня вищої освіти спеціальності 081 «Право»
Одеського державного університету внутрішніх справ

Розвиток цифрової економіки супроводжується інтенсивним впровадженням передових цифрових технологій, зокрема штучного інтелекту та аналітики великих даних (Big Data), що спричиняє глибокі трансформаційні зміни в різних галузях [1].

Сучасний етап розвитку цифрових технологій супроводжується стрімким впровадженням систем штучного інтелекту (ШІ) у сферу безпеки, що охоплює як державні, так і приватні структури.

Штучний інтелект не лише моделює людське мислення та аналізує великі обсяги даних, а й активно впроваджується в різні сфери діяльності. Зокрема, він забезпечує ідентифікацію ризиків і шахрайських схем,оптимізацію портфелів інвестицій та автоматизацію процесів прийняття рішень на основі машинного навчання [2].

Використання різних інструментів на базі штучного інтелекту, включно з машинним навчанням, розпізнаванням облич чи аналітикою прогнозів, вже давно перестало бути чимось суто експериментальним. Це поступово змінює підходи до безпеки – і громадської, і національної, і навіть кіберпростору. Деякі рішення ухвалюються швидше, ніж раніше, інколи навіть занадто швидко, і не завжди зрозуміло, як саме вони були сформовані. Тут і виникають певні сумніви, бо поряд із зручністю з'являються ризики – від порушення приватності до не зовсім прозорих алгоритмів, які працюють ніби «всередині чорної скриньки». Власне, через це тема регулювання штучного інтелекту на міжнародному рівні почала звучати значно частіше, ніж ще кілька років тому.

Якщо подивитись на різні країни, стає помітно, що єдиного підходу тут так і не сформувалося. Кожен рухається у свій спосіб, іноді

навіть досить суперечливо. Це залежить і від економічних інтересів, і від політичних традицій, і від того, наскільки взагалі країна готова до таких технологій. Хоча в цілому проглядається спільна логіка – знайти якийсь баланс між розвитком і безпекою, щоб не загальмувати інновації, але й не втратити контроль над ситуацією.

Європейський варіант виглядає більш формалізованим, якщо так можна сказати. Тут робиться акцент на правах людини, і це відчувається майже у всіх документах. Системи ШІ оцінюються через призму ризиків, і залежно від цього до них застосовуються різні вимоги. З одного боку, це створює певну чіткість, але з іншого – іноді виглядає надто складно і бюрократично. Особливо коли мова заходить про такі речі, як прозорість алгоритмів або відповідальність розробників. У сфері безпеки це означає обережне ставлення до масового спостереження, хоча на практиці все не завжди так однозначно.

У Сполучених Штатах підхід інший, більш гнучкий, навіть трохи хаотичний на перший погляд. Там більше покладаються на саморегулювання і галузеві стандарти, що дає змогу швидше впроваджувати нові рішення. У сфері безпеки технології ШІ використовуються досить активно, зокрема правоохоронними структурами. Але водночас виникають дискусії про те, де проходить межа між ефективністю і втручанням у приватне життя. І ці дискусії часом заходять у глухий кут.

Китайська модель виглядає ще інакше. Там держава відіграє ключову роль, фактично задає напрям розвитку і контролює його. Системи відеоспостереження, соціальні рейтинги – усе це вже стало частиною повсякденності. Такий підхід дозволяє досить ефективно управляти процесами, хоча питання приватності тут відходить на другий план. І це викликає неоднозначну реакцію, особливо з боку інших країн.

Не можна обійти увагою і міжнародні організації, які намагаються хоча б частково узгодити підходи. Наприклад, Організація економічного співробітництва та розвитку пропонує певні принципи відповідального використання ШІ – прозорість, підзвітність, безпека. Подібні ініціативи з'являються і в рамках Організація Об'єднаних Націй, де більше уваги приділяється етичним аспектам. Хоча іноді ці документи виглядають більше як рекомендації, ніж реальні механізми впливу.

Окремо варто згадати військову сферу, де штучний інтелект починає відігравати все помітнішу роль. Автономні системи викликають багато суперечок, особливо через питання контролю. Ідея збереження людського фактора звучить логічно, але реалізувати її не так просто. Міжнародні обговорення тривають, але чіткої позиції досі немає, і це, мабуть, теж показник того, наскільки складною є ця тема. Іноді здається, що технології рухаються швидше, ніж здатність суспільства домовитися про правила їх використання.

Аналізуючи різні підходи до регулювання штучного інтелекту, доцільно узагальнити їх ключові характеристики, що відображено у табл. 1.

Таблиця 1

Порівняльна характеристика моделей регулювання штучного інтелекту у сфері безпеки

Країна/регіон	Основний підхід	Рівень державного контролю	Особливості у сфері безпеки
ЄС	Ризик-орієнтований, нормативний	Високий	Обмеження масового спостереження, захист прав людини
США	Гнучкий, ринковий	Середній	Активне використання ШІ правоохоронними органами
Китай	Централізований, державний	Дуже високий	Масштабні системи цифрового контролю
ОЕСР / ООН	Рекомендаційний	Низький	Формування етичних стандартів та принципів

Якщо дивитись на це трохи простіше, то видно, що жодна модель не є ідеальною сама по собі. У кожної є свої сильні сторони, але й свої слабкі місця, і вони якось природно випливають із того, що саме для держави важливіше в конкретний момент. Європейський варіант більше «про правила» і захист прав, інколи навіть занадто обережний, через що розвиток технологій може трохи гальмуватися. Американський підхід виглядає більш живим, швидшим, але при цьому не завжди встигає за власними наслідками,

тому питання контролю постійно повертається в дискусіях. Китайська модель, навпаки, показує ефективність у сенсі організації й безпеки, хоча ціна цього іноді здається занадто високою, особливо якщо говорити про свободи.

Для України ця тема виглядає трохи інакше, бо контекст все ж складніший, і безпековий фактор тут відчувається значно сильніше. Просто взяти одну з моделей і скопіювати її навряд чи спрацює. Швидше, мова йде про певне поєднання різних підходів, навіть якщо це звучить не дуже чітко. Логічно виглядає варіант, де європейська ідея з оцінкою ризиків якось поєднується з американською гнучкістю, плюс додається більш стратегічне бачення, яке часто згадують у контексті Китаю. Хоча на практиці це, напевно, буде виглядати зовсім не так акуратно, як у теорії.

При цьому ключові речі залишаються доволі очевидними, навіть трохи банальними: безпека, права людей і розвиток технологій. Інша справа, що між ними постійно виникає напруга, і баланс тримати складніше, ніж це зазвичай описують у підручниках. Іноді здається, що рішення приймаються вже «по ситуації», а не за якоюсь чіткою моделлю, і це, мабуть, теж частина реальності.

Важливо враховувати, що сучасний міжнародний досвід регулювання штучного інтелекту у сфері безпеки поступово переходить від фрагментарних рішень до формування комплексних підходів, які поєднують правові, технологічні та інституційні механізми. У цьому контексті дедалі більшого значення набуває гармонізація нормативно-правових вимог між країнами, зокрема щодо використання ШІ в правоохоронній діяльності, кібербезпеці та оборонному секторі. Практика свідчить, що ефективне регулювання неможливе без встановлення чітких процедур оцінки ризиків, визначення меж допустимого застосування автономних систем і забезпечення прозорості алгоритмів. Крім того, міжнародна координація дозволяє уникнути регуляторних прогалин, які можуть бути використані для зловживань, і водночас сприяє формуванню спільного безпекового простору, в якому інновації розвиваються без критичних загроз для суспільства.

Таким чином, міжнародний досвід регулювання штучного інтелекту у сфері безпеки демонструє різноманітність підходів і необхідність їх адаптації до національних умов. Формування ефективної системи регулювання потребує комплексного врахування технологічних, правових та етичних аспектів, а також активної

участі держави, бізнесу та громадянського суспільства. У перспективі подальший розвиток міжнародного співробітництва у цій сфері може сприяти створенню узгоджених стандартів, які забезпечать безпечне та відповідальне використання штучного інтелекту на глобальному рівні.

Список використаних джерел:

1. Ying J., Wan Y. The development trend of artificial intelligence in the big data environment. *2022 3rd International Conference on Electronic Communication and Artificial Intelligence (IWECAI)*. Zhuhai, China, 2022. https://doi.org/10.1109/ IWEC AI5531 5.2022.00064

2. Цегельник Н.І., Гладков Д.А. Big Data та штучний інтелект в обліку інвестицій: вплив на економічну безпеку підприємств. *Актуальні питання економічних наук*. 2025. № 9. DOI: https://doi.org/10.5281/zenodo.15108352

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ ТА КІБЕРБЕЗПЕЦІ У КОНТЕКСТІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ: АНАЛІТИЧНІ, ТЕХНОЛОГІЧНІ ТА ПРАВОВІ АСПЕКТИ

Поляков Євген Валентинович
доцент кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України, кандидат юридичних наук, доцент
Мотрюк Максим Дмитрович
курсант 201 взводу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України

Оперативно-розшукова діяльність (ОРД) є важливим інструментом протидії злочинності, що забезпечує отримання, обробку та аналіз інформації з метою попередження, виявлення та розкриття кримінальних правопорушень. У сучасних умовах цифровізації суспільства та зростання кіберзагроз особливого значення набуває використання технологій штучного інтелекту (ШІ) у

поєднанні з методами кримінального аналізу, що дозволяє значно підвищити ефективність діяльності оперативних підрозділів [1]. Відповідно до Закону України «Про оперативно-розшукову діяльність», ОРД визначається як система гласних і негласних заходів, спрямованих на захист прав і свобод людини, власності та безпеки держави [2]. У цьому контексті впровадження технологій штучного інтелекту виступає як складова інформаційно-аналітичного забезпечення ОРД, що дозволяє автоматизувати процеси збору, обробки та аналізу інформації.

Кримінальний аналіз є одним із ключових елементів аналітичної діяльності оперативних підрозділів, який спрямований на виявлення закономірностей у злочинній діяльності, встановлення зв'язків між особами та прогнозування криміногенної ситуації. Як зазначає І. А. Федчак, кримінальний аналіз дозволяє ефективно обробляти великі масиви інформації та приймати обґрунтовані управлінські рішення [3, с. 64]. Використання технологій штучного інтелекту значно розширює можливості кримінального аналізу, зокрема за рахунок застосування машинного навчання, обробки природної мови (NLP) та автоматичного виявлення аномалій. У сфері кібербезпеки штучний інтелект використовується для виявлення кіберзагроз, аналізу шкідливого програмного забезпечення, моніторингу мережевої активності та запобігання кібератакам. Для оперативних підрозділів це має важливе значення, оскільки значна частина злочинної діяльності перемістилася у цифровий простір. Застосування ШІ дозволяє виявляти підозрілу активність у режимі реального часу та оперативно реагувати на загрози [4]. Аналітичний аспект застосування штучного інтелекту полягає у можливості автоматизованого аналізу великих обсягів даних, включаючи інформацію з відкритих джерел (OSINT), баз даних, соціальних мереж та інших інформаційних ресурсів. ШІ здатний виявляти приховані закономірності, встановлювати зв'язки між об'єктами аналізу та формувати аналітичні прогнози. Це значно підвищує ефективність оперативного пошуку та оперативної розробки.

Технологічний аспект полягає у використанні спеціалізованих програмних продуктів та систем, які забезпечують аналіз даних, візуалізацію зв'язків та автоматизацію аналітичних процесів. До таких систем належать платформи кримінального аналізу, системи аналізу соціальних мереж, а також інструменти

кіберрозвідки. Їх інтеграція в діяльність оперативних підрозділів дозволяє підвищити швидкість та якість обробки інформації. Правовий аспект застосування штучного інтелекту в ОРД є одним із найбільш складних. Конституція України гарантує дотримання прав і свобод людини, зокрема права на приватність [5]. У зв'язку з цим використання ШІ повинно здійснюватися з дотриманням принципів законності, пропорційності та обґрунтованості. Відповідно до Кримінального процесуального кодексу України, доказами є лише ті дані, які отримані у законний спосіб [6]. Це означає, що результати, отримані за допомогою ШІ, повинні бути належним чином перевірені та задокументовані. У межах оперативно-розшукової діяльності результати кримінального аналізу із застосуванням ШІ можуть використовуватися як підстава для проведення негласних слідчих (розшукових) дій. Зокрема, відповідно до статей 246 та 260 КПК України, такі дії проводяться з метою отримання доказів та перевірки інформації [6]. Таким чином, штучний інтелект виступає як допоміжний інструмент, що підвищує ефективність ОРД.

Разом із тим існують певні ризики використання ШІ у правоохоронній діяльності. До них належать: можливість помилок алгоритмів, упередженість моделей, відсутність прозорості прийняття рішень, а також загроза порушення прав людини. У зв'язку з цим необхідним є розроблення чітких правових механізмів регулювання використання штучного інтелекту у діяльності правоохоронних органів. Перспективи розвитку застосування ШІ у кримінальному аналізі та ОРД пов'язані з подальшою автоматизацією аналітичних процесів, інтеграцією різних інформаційних систем, а також розвитком міжнародного співробітництва у сфері кібербезпеки. Важливим є також підвищення рівня підготовки працівників правоохоронних органів у сфері використання сучасних інформаційних технологій. Таким чином, використання технологій штучного інтелекту у кримінальному аналізі та кібербезпеці є перспективним напрямом розвитку оперативно-розшукової діяльності. Воно дозволяє підвищити ефективність збору та аналізу інформації, однак потребує належного правового регулювання та дотримання прав людини.

Список використаних джерел:

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2021.

2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII.
3. Федчак І. А. Основи кримінального аналізу. Львів : ЛьвДУВС, 2020.
4. ENISA. Artificial Intelligence Cybersecurity Challenges. 2023.
5. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР.
6. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.

ДОПОВНЕНІ ОПЕРАЦІЇ БЕЗПЕКИ ЯК СУЧАСНИЙ ЗАСІБ ЗАСТОСУВАННЯ ШІ У КІБЕРБЕЗПЕЦІ

Пядишев Володимир Георгійович
доктор юридичних наук, професор, професор кафедри кримінального аналізу та інформаційних технологій, Одеський державний університет внутрішніх справ
Волошко Олексій Вікторович
начальник Управління кримінального аналізу, ГУНПУ в одеській області

Сьогодні штучний інтелект (ШІ) у кібербезпеці включає застосування машинного навчання, глибокого навчання та обробку природної мови для автоматизації виявлення загроз, аналізу величезних наборів даних та реагування на інциденти в режимі реального часу. Він діє як множник сили для команд безпеки, забезпечуючи проактивний захист, а не лише реактивне виявлення на основі сигнатур.

При цьому, до найважливіших аспектів застосування ШІ в кібербезпеці належать наступні.

а. Виявлення загроз та ідентифікація аномалій

Поведінкова аналітика (UEBA). ШІ встановлює базову лінію для нормальної мережевої активності та поведінки користувачів, негайно позначаючи відхилення, що вказують на внутрішні загрози, захоплення облікових записів або горизонтальне переміщення [1, с. 1-2].

Виявлення шкідливого програмного забезпечення. Захист кінцевих точок на базі ШІ (EDR) класифікує файли та блокує шкідливе програмне забезпечення, включаючи загрози нульового дня, не покладаючись на відомі сигнатури [2, с. 3].

Безпека електронної пошти. ШІ аналізує вміст, контекст та тон електронних листів для виявлення спроб фішингу [3, с. 4].

б. Автоматизоване реагування та управління інцидентами

Інтеграція SOAR. ШІ інтегрується з платформами оркестрації, автоматизації та реагування безпеки (SOAR - Security Orchestration, Automation, and Response) для автоматичної ізоляції заражених пристроїв, блокування шкідливих IP-адрес та скасування скомпрометованих облікових даних користувачів [4, с. 8].

Автономне виправлення: Системи можуть самостійно ініціювати виправлення або зміни конфігурації безпеки для усунення вразливостей.

в. Управління вразливостями [5, с. 12].

Прогнозна оцінка ризиків: ШІ оцінює інвентаризацію IT-активів та інформацію про загрози, щоб передбачити, де найімовірніше відбудеться порушення, що дозволяє командам пріоритезувати зусилля з виправлення (за допомогою CVSS) [6, с.].

Автоматизований аналіз коду: ШІ сканує програмне забезпечення на наявність вразливостей під час розробки [7, с. 14]..

г. Доповнення операцій безпеки (SecOps)

Зменшення втоми від сповіщень тривоги: ШІ сортує, пріоритезує та співвідносить тисячі сповіщень, зменшуючи кількість хибнопозитивних результатів, щоб аналітики могли зосередитися на критичних загрозах.

Генеративні помічники ШІ: помічники ШІ, такі як Microsoft Security Copilot, дозволяють аналітикам запитувати складні журнали, використовуючи природну мову, для швидшого розслідування інцидентів [8, с. 3].

Кожен зі зазначених аспектів заслуговує на окрему увагу. Проте сьогодні ми зосередимось на одному з них, а саме на так званому «доповненні операцій безпеки».

Отже, доповнення операцій безпеки (SecOps) за допомогою ШІ [9, с. 3]. – це інтеграція штучного інтелекту, включаючи машинне навчання (ML), обробку природної мови (NLP) та генеративний ШІ, до Центру операцій безпеки (SOC) – для покращення,

але не для повної заміни аналітиків-людей. З 2026 року доповнення ШІ переходить зі стану конкурентної переваги до стану необхідності, дозволяючи командам переходити від реактивного (тобто після виявлення події) ручного сортування тривог до проактивного (тобто попереджуючого подію) пошуку загроз та стратегічного управління ризиками. Цей підхід, який часто називають «SecOps на основі ШІ» або «Agentic SOC» (центр операцій з безпеки на основі застосування спеціалізованих програм), діє як «множник сили», що підсилює людським судження швидкістю ШІ.

Отже, ШІ у складі операцій з безпеки покращує наступні критично важливі функції.

Інтелектуальне сортування та зменшення втоми від опрацювання тривог. ШІ обробляє величезні набори даних, корелюючи сигнали між інструментами (наприклад, SIEM, EDR, NDR), щоб розрізняти доброякісну активність та справжні загрози. Це зменшує кількість хибнопозитивних результатів більш ніж на 90% та значно скорочує час розслідування.

Поведінковий аналіз та виявлення аномалій. ШІ постійно контролює мережі, пристрої та поведінку користувачів, щоб виявляти відхилення від встановлених базових рівнів, які вказують на шкідливу активність.

Генеративна допомога з боку ШІ. Помічники ШІ дозволяють аналітикам використовувати природну мову для запитів до платформ безпеки, узагальнення складних інцидентів та пропонування кроків щодо усунення наслідків.

Автономне розслідування та реагування. Агентний ШІ може самостійно досліджувати сповіщення, відстежувати ланцюжки атак у гібридних середовищах та рекомендувати або виконувати дії щодо стримування, як підкреслюють такі інструменти, як FortiSOC від Fortinet.

Зазначене забезпечує наступні переваги.

Більш швидкі виявлення загроз та реагування. Платформи на базі ШІ можуть аналізувати та реагувати за лічені секунди, значно скорочуючи час витримки.

Підвищені ефективність та масштабованість. Автоматизуючи повторювані завдання (наприклад, збагачення даних), аналітики можуть зосередитися на завданнях високої цінності.

Подолання розриву в навичках. ШІ надає покрокові інструкції, дозволяючи менш досвідченим аналітикам обробляти складні інциденти.

Що ж очікується протягом 2026 року?

Перехід до агентних операцій з безпеки. Очікується, що у 2026 рокці ШІ вийде за рамки простої автоматизації – з переходом до автономних, керованих агентами робочих процесів, які підключатимуться до інструментів безпеки через такі фреймворки, як Model Context Protocol (MCP) [10, с. 2-3].. При цьому основні гравці галузі зосередяться на наступному.

Microsoft Security. Пропонування уніфікованих платформ SecOps на базі штучного інтелекту, які об'єднують виявлення, розслідування та реагування.

Fortinet FortiAI. Використання штучного інтелекту для забезпечення агентних робочих процесів для пошуку загроз та реагування на інциденти

Google Cloud SecOps. Використання агентів, які підключаються до різних інструментів, щоб забезпечити на 50% швидший середній час реагування

ВИСНОВКИ

Хоча при здійсненні операцій з кібербезпеки штучний інтелект забезпечує високу швидкість, нагляд людини має вирішальне значення для контексту, стратегії та прийняття рішень на високому рівні. Отже, для забезпечення високої ефективності застосування штучного інтелекту потрібна високоякісна, комплексна інтеграція даних у всьому IT-середовищі. Одночасно важливим аспектом постає гостра необхідність забезпечувати захист власних моделей штучного інтелекту від атак ухилення та отруєння з боку деструктивних систем штучного інтелекту.

Список використаних джерел:

1. What is user and entity behavior analytics (UEBA)? *IBM.Com*. 29 April 2026. 16 p. Site. URL: https://www.ibm.com/think/topics/ ueba

2. What is the Role of AI in Endpoint Security? *Palo Alto Networks*. 2026. 16 p. Site. URL: https://www.paloaltonetworks.com/ cyberpedia/ what-is-ai-in-endpoint-security

3. Eze, Ch. S., Shamir, L. Analysis and Prevention of AI-Based Phishing Email Attacks. Electronics 2024, 13, 1839. 13 p. URL:

https://www.researchgate.net/publication/380475287_Analysis_and_Prevention_of_AI-Based_Phishing_Email_Attacks

4. Blacet, B. How SOAR and AI Are Reshaping Cybersecurity in Real Time. anomali.com. June 9, 2025. 12 p. Site. URL: https://www.anomali.com/blog/how-soar-and-ai-are-reshaping-cybersecurity Blacet, B. How SOAR and AI Are Reshaping Cybersecurity in Real Time. anomali.com. June 9, 2025. 12 p. Site. URL: https://www.anomali.com/blog/how-soar-and-ai-are-reshaping-cybersecurity

5. Aramide, O. AI-Driven Automated Incident Response and Remediation in Networks. May 2025. 25 p. DOI:10.21590/ijtmh.11.02.00. Site. URL: https://www.researchgate.net/publication/393743988_ AI-Driven_Automated_Incident_ Response_and_ Remediation_ in_Networks

6. Kalogiannidis, S., Papaevangelou, O., Giannarakis, G., Chatzitheodoridis, F. The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *MDPI.Com*. 23 January 2024. 57 p. Site. URL: https://www.mdpi.com/2227-9091/12/2/19

7. AI-driven code analysis: The new frontier in code security. *GitLab Inc*. 2026. 33 p. Site. URL: https://about.gitlab.com/topics/agentic-ai/ai-code-analysis/

8. Bono, J., Grana, J., Xu, A. Generative AI and Security Operations Center Productivity: Evidence from Live Operations. *ResearchGate*. November 2024. 8 p. DOI:10.48550/arXiv. 2411.03116. Site. URL: https://www.researchgate.net/ publication/ 385560290_ Generative_AI_and_Security_Operations_Center_Productivity_Evidence_from_Live_Operations

9. Gillett, M. How AI Can Reshape Security Operations Through Augmentation, Not Automation. *ESENTIRE.Com*. May 28, 2025. 8 p. Site. URL: https://www.esentire.com/blog/how-ai-can-reshape-security-operations-through-augmentation-not-automation

10. What is the Model Context Protocol (MCP)? *Model Context Protocol*. 2026. 4 p. Site. URL: https://modelcontextprotocol.io/docs/getting-started/intro

ДОКАЗОВЕ ЗНАЧЕННЯ РЕЗУЛЬТАТІВ КРИМІНАЛЬНОГО АНАЛІЗУ, СФОРМОВАНИХ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ, В МАТЕРІАЛАХ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Павлова Н.В., *к.ю.н., доцент,*
доцент кафедри правоохоронної діяльності, УМСФ
Розгон О.Г., *к.ю.н., доцент,*
доцент кафедри правоохоронної діяльності, УМСФ

Цифровізація правоохоронної діяльності та технологічне ускладнення злочинних практик перетворили кримінальний аналіз із допоміжного методу обробки інформації на самостійний напрям інформаційно-аналітичного забезпечення оперативно-розшукової діяльності (далі - ОРД). В умовах воєнного стану до аналітичної роботи дедалі активніше долучаються інструменти на основі штучного інтелекту (далі - ШІ) - алгоритми машинного навчання, моделі обробки природної мови, інструменти зв'язкового аналізу великих даних. Утім КПК України та Закон України «Про оперативно-розшукову діяльність» залишаються нейтральними щодо самого факту застосування таких технологій. Звідси постає невирішене питання: чи можуть результати кримінального аналізу, отримані за допомогою ШІ й оформлені як матеріали ОРД, набувати доказового значення у кримінальному провадженні, і за яких саме умов така трансформація є правомірною.

Доказове значення матеріалів ОРД у кримінальному провадженні досліджували М. А. Погорецький, Д. Б. Сергєєва, С.С. Чернявський, О. М. Бандурка та інші українські вчені, які сформували традицію розгляду оперативно-розшукової інформації крізь призму належності, допустимості й достовірності [1; 2]. Методологію власне кримінального аналізу системно розкрито у працях О. Є. Користіна, С. В. Албула, Б. І. Бараненка [3; 4]. Правовий режим ШІ у правоохоронній діяльності в українському дискурсі лише оформлюється й переважно відштовхується від європейських стандартів - Регламенту ЄС про штучний інтелект і документів Ради Європи [5; 6]. На стику цих трьох ліній і залишається дискусійний простір, якому присвячено цю розвідку.

Кримінальний аналіз, у значенні, якого йому надають європейська модель і підходи Європолу, є циклічним процесом виявлення прихованих зв'язків між особами, подіями та об'єктами інформації з метою формування орієнтуючих висновків для прийняття управлінських і тактичних рішень [3, с. 47]. ОРД, відповідно до ст. 2 Закону України «Про оперативно-розшукову діяльність», має самостійну мету - пошук і фіксацію фактичних даних про протиправні діяння [7]. Отже, ці категорії не є тотожними: кримінальний аналіз постачає інформаційний продукт, ОРД - процесуально значущі дані. Без такого розмежування неможливо коректно описати правовий статус ШІ-аналітики.

Сучасні системи кримінального аналізу - як комерційні (i2 Analyst's Notebook, Palantir Gotham), так і відомчі - все частіше використовують ШІ-компоненти: кластеризацію, рекомендаційні моделі, автоматичне розпізнавання сутностей у текстах, виявлення аномалій у транзакційних масивах. Їхня особливість - непрозорість процесу формування висновку: аналітик бачить кінцевий результат, але не може відтворити покрокову логіку моделі. Цей феномен у літературі позначається як проблема «чорної скриньки» (black box) і, на нашу думку, він має не лише технологічну, а й виразну кримінально-процесуальну природу.

Відтак постає ключове питання: у якому статусі результат ШІ-аналітики потрапляє до матеріалів ОРД. Ст.10 Закону України «Про оперативно-розшукову діяльність» допускає використання таких матеріалів як приводів і підстав для початку досудового розслідування, а також як доказів у порядку, передбаченому КПК України [7]. Натомість статті 84 і 99 КПК України закріплюють, що доказами є фактичні дані, отримані у передбаченому Кодексом порядку, а документ підлягає перевірці щодо походження та змісту [8]. Звідси - вузький, але важливий висновок: аналітичний продукт ШІ-системи у «сирому» вигляді не відповідає вимогам ст. 99 КПК України, оскільки не може бути перевірений у частині походження (алгоритмічної логіки) і змісту (внутрішніх вагових коефіцієнтів моделі).

Ми вважаємо, що результат кримінального аналізу зі ШІ-компонентом за своєю правовою природою не є доказом і не повинен використовуватися як такий безпосередньо. Він має статус орієнтуючої інформації, що окреслює перспективні напрями

оперативно-розшукових заходів і слідчих (розшукових) дій, у межах яких формуються власне процесуальні докази. Інакше кажучи, ШІ-аналітика виконує функцію не доказу, а навігаційного інструменту, який вказує оперативному працівникові або слідчому, де саме слід шукати фактичні дані. Водночас не можемо повністю погодитися з позицією, висловленою у частині наукової літератури, відповідно до якої ШІ-висновок у принципі не може бути легалізований у кримінальному провадженні: на наш погляд, така категоричність ігнорує реальні потреби протидії організованій злочинності та кіберзлочинам у воєнний період.

Видається обґрунтованим виокремити три обов'язкові умови, за яких ШІ-аналітика може правомірно опосередковано впливати на формування доказової бази: технологічна верифікованість моделі (можливість реконструкції джерел даних, ознак та рівня впевненості); документальна простежуваність (протокол із фіксацією вхідних даних, версії моделі, оператора-аналітика, часу формування висновку); персональна відповідальність аналітика за зміст продукту й рішення про передачу матеріалів. Останнє є визначальним, бо усуває спокусу «знеособлення» рішень через посилання на «висновок системи». Окремої уваги потребує і ризик упередженості (algorithmic bias) навчальних даних: якщо модель навчалася на історичних масивах із непропорційно представленими категоріями осіб або територій, її висновки відтворюватимуть це викривлення, концентруючи оперативно-розшукові заходи на «зручних» для алгоритму групах, що порушує закріплений у ст. 24 Конституції України принцип рівності перед законом [9]. Регламент ЄС 2024/1689 відносить такі системи до категорії високого ризику й вимагає спеціальних процедур верифікації [5]; українське законодавство аналогічних вимог не містить.

Це дає підстави стверджувати, що чинна нормативна модель є недостатньою. Видається доцільним доповнити Закон України «Про оперативно-розшукову діяльність» окремою статтею (умовно - ст. 8-1), яка б закріпила: визначення автоматизованих і ШІ-інструментів кримінального аналізу; обов'язковий стандарт верифікації аналітичного продукту перед його включенням до матеріалів ОРД; вимогу до протоколювання, що забезпечує можливість перевірки походження та змісту в порядку ст. 99 КПК України. Паралельно у ст. 99 КПК України, на наш погляд, доцільно

передбачити, що документ, який містить результати автоматизованої аналітичної обробки, оцінюється з урахуванням специфіки методу його отримання. Такий підхід дозволив би уникнути ситуації, за якої практика випереджає закон, а суди змушені формувати стандарти допустимості ad hoc.

Підсумовуючи, зазначимо таке. По-перше, у роботі обґрунтовано, що результати кримінального аналізу, сформовані засобами ШІ, у своєму первинному вигляді не відповідають вимогам ст. 84 і ст. 99 КПК України й не можуть розглядатися як самостійне джерело доказів; їхня правова природа - орієнтуюча інформація, що легалізується через подальші оперативно-розшукові заходи та слідчі (розшукові) дії. По-друге, відсутність у Законі України «Про оперативно-розшукову діяльність» і КПК України спеціального стандарту верифікації ШІ-аналітики створює ризики як для допустимості доказів, так і для дотримання конституційного принципу рівності перед законом. По-третє, наукова й практична цінність дослідження полягає у запропонованому триелементному стандарті (верифікованість - простежуваність - персональна відповідальність) як мінімальній моделі правомірного застосування ШІ у кримінально-аналітичній роботі оперативних підрозділів. Перспективними напрямами подальших розвідок видаються розроблення методичних рекомендацій щодо процесуального оформлення матеріалів ОРД, що базуються на ШІ-аналітиці, та порівняльно-правове дослідження європейських практик у цій сфері.

Список використаних джерел:

1. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі : монографія. Харків : Арсіс ЛТД, 2007. 576 с.

2. Сергєєва Д. Б. Результати негласних слідчих (розшукових) дій: проблеми використання в кримінальному провадженні. Вісник кримінального судочинства. 2017. № 3. С. 81-89.

3. Користін О. Є., Албул С. В. Кримінальний аналіз: методологічні засади та практика впровадження в діяльність правоохоронних органів України : монографія. Одеса : ОДУВС, 2019. 268 с.

4. Бараненко Б. І. Оперативно-розшукова психологія : навч. посіб. Луганськ : РВВ ЛДУВС, 2009. 480 с.

5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial

intelligence (Artificial Intelligence Act). Official Journal of the European Union. L series, 12.07.2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 10.05.2026).

6. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law : CETS No. 225, 17 May 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (дата звернення: 10.05.2026).

7. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303 (зі змінами).

8. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України. 2013. № 9-10, № 11-12, № 13. Ст. 88 (зі змінами).

9. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. Відомості Верховної Ради України. 1996. № 30. Ст. 141 (зі змінами).

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ ТРАНЗАКЦІЙ ПРИ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ЗЛОЧИННИХ ДОХОДІВ

Світличний Віталій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності
Харківського національного університету внутрішніх справ

Вступ. Глобальна трансформація суспільних відносин у цифрову площину зумовила виникнення нових викликів для системи фінансової безпеки держави. Кіберпростір, забезпечуючи транскордонність, анонімність та високу швидкість транзакцій, став основним середовищем для легалізації (відмивання) доходів, одержаних злочинним шляхом. Традиційні методи фінансового моніторингу, засновані на статичних алгоритмах та порогових сумах, виявляються малоефективними проти динамічних методів обфускації фінансових потоків [1].

Сучасна парадигма протидії кіберзлочинності вимагає переходу від реактивних методів (фіксація наслідків) до проактивних стратегій, що базуються на використанні інтелектуальних систем аналізу даних. Актуальність дослідження зумовлена необхідністю розробки концептуальних підходів до автоматизації виявлення складних схем легалізації доходів, що реалізуються з використанням віртуальних активів та децентралізованих фінансових протоколів.

Аналіз сучасних механізмів анонімізації злочинних доходів. Еволюція технологій блокчейн створила інструментарій, який активно експлуатується кіберзлочинцями для розриву зв'язку між джерелом походження коштів та їх кінцевим бенефіціаром [2]. Основними технічними викликами для правоохоронних органів є:

1. Алгоритмічні методи змішування (Mixing services): Використання протоколів типу CoinJoin дозволяє об'єднувати вхідні дані багатьох незалежних транзакцій в єдину операцію. Це унеможливлює встановлення детермінованого зв'язку між конкретними суб'єктами, фактично руйнуючи цілісність «ланцюжка володіння» активами [3].

2. Конфіденційні цифрові активи на базі Zero-Knowledge Proofs: Інтеграція протоколів zk-SNARKs у віртуальні активи дозволяє підтверджувати валідність транзакції без розкриття інформації про суму переказу, адресу гаманця та баланс сторін. Такі механізми створюють умови для функціонування «сліпих зон» у системі глобального фінмоніторингу [4].

3. Технології міжмережевої взаємодії (Cross-chain Bridges): Застосування децентралізованих мостів для швидкої конвертації активів між різними блокчейн-реєстрами (наприклад, з публічного реєстру Bitcoin до конфіденційного реєстру Monero) дозволяє зловмисникам маскувати переміщення активів, ускладнюючи наскрізний аудит [5].

Застосування інтелектуальних систем у процесах моніторингу. Для підвищення ефективності виявлення вищеописаних загроз необхідне впровадження штучного інтелекту (ШІ) та глибокого машинного навчання у практику діяльності підрозділів кіберполіції та суб'єктів моніторингу [6]. Перспективними напрямами є:

- Графові нейронні мережі (GNN): Оскільки фінансові транзакції за своєю структурою є мережевими графами, використання GNN дозволяє аналізувати нелінійні зв'язки та виявляти специфічні топологічні патерни, характерні для «розпилення» (smurfing) або кільцевих схем відмивання коштів [7].
- Динамічна детекція аномалій на основі поведінкових профілів: ШІ забезпечує побудову багатовимірного цифрового портрета користувача, аналізуючи не лише параметри транзакцій, а й технічні атрибути (fingerprinting пристроїв, геопросторові аномалії IP-адрес, часові інтервали активності). Будь-яке відхилення від індивідуального паттерна автоматично підвищує індекс ризику операції [8].
- Прогностична аналітика та автоматизований Risk Scoring: Використання моделей, навчених на історичних даних про вже розкриті злочини, дозволяє в реальному часі оцінювати ймовірність залучення транзакції до злочинної діяльності. Це забезпечує можливість превентивного блокування операцій з критично високим рівнем ризику [9].

Правові та організаційні аспекти реалізації стратегії протидії. Технологічна модернізація повинна супроводжуватися відповідною адаптацією правового поля. Закон України «Про віртуальні активи» став важливим етапом у регулюванні цієї сфери [5], проте залишається потреба у деталізації механізмів вилучення віртуальних активів та визнання результатів автоматизованого криптоаналізу як належної доказової бази в кримінальному провадженні [2].

Ефективна стратегія попередження легалізації доходів має базуватися на:

1. Технологічному суверенітеті: Розробці національних аналітичних систем для моніторингу блокчейн-мереж та ідентифікації сервісів-міксерів [8].
2. Міжнародній інституційній взаємодії: Наскрізному обміні даними про «заплямовані» активи через мережі Європолу та FATF, оскільки цифрові злочини не мають фізичних кордонів [3, 4].
3. Публічно-приватному партнерстві: Взаємодії правоохоронних органів з VASP (провайдерами послуг віртуальних активів) для оперативного обміну інформацією про підозрілі транзакції.

Висновки. Протидія легалізації доходів у цифрову епоху — це безперервний процес вдосконалення методів аналізу та

регулювання. Тільки через інтеграцію передових досягнень у сфері графового аналізу, штучного інтелекту та міжнародної кооперації можливо створити ефективний бар'єр проти складних схем відмивання коштів у кіберпросторі. Майбутнє успішної боротьби з кіберзлочинністю полягає у синергії людського досвіду та потужності інтелектуальних алгоритмів.

Список використаних джерел:

1. Кіберзлочинність в умовах цифровізації економіки: монографія / О. М. Литвинов, О. О. Бакумов, П. С. Корнієнко та ін.; за заг. ред. О. М. Литвинова ; Харків. нац. ун-т внутр. справ. Харків: Панов, 2022. 312 с.
2. Методичні рекомендації щодо виявлення та розслідування злочинів, пов'язаних із використанням віртуальних активів / С. В. Демедюк, Л. В. Тимченко, М. В. Корнієнко та ін.; Департамент кіберполіції Національної поліції України. Київ: НПУ, 2023. 84 с. (Серія «Практикум правоохоронця»).
3. Anonymity-Enhanced Cryptocurrencies and Money Laundering Risks : Europol Spotlight Report. 2022. URL: https://www.europol.europa.eu/publications-events/publications/.
4. Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs : FATF Guidance. Paris : FATF, 2021.
5. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20.
6. Artificial Intelligence in Financial Services : Joint report by FSB and OECD. 2023. URL: https://www.oecd.org/finance/financial-markets/ai-in-financial-services.htm.
7. Носов В.В. Практична оцінка реалізації розподіленого криптоаналізу в умовах обмежених ресурсів / В.В Носов, В.Є.Лучик, Т.П.Колісник, С.В.Калякін, В.А.Світличний // Захист інформації, том 25, № 1, січень-березень 2023 URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/17596
8. Звіт про проведення національної оцінки ризиків у сфері запобігання та протидії легалізації доходів... : Держфінмоніторинг. Київ, 2023. URL: https://fiu.gov.ua/.
9. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом... : Закон України від 06.12.2019 № 361-IX : станом на 01.01.2024.

КРИМІНАЛЬНИЙ АНАЛІЗ У ЦИФРОВОМУ СЕРЕДОВИЩІ: СУЧАСНІ ПІДХОДИ ДО ВИЯВЛЕННЯ КІБЕРЗЛОЧИННОСТІ ТА ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Сіфоров Олександр Іванович
кандидат технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ.
Іванченко Валерія Сергіївна
викладач кафедри кримінального аналізу та інформаційних технологій

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням ролі цифрових технологій у функціонуванні державних інституцій, економічних систем, соціальних комунікацій та безпекового сектору. Цифровізація суспільних процесів, інтеграція інформаційно-комунікаційних технологій у всі сфери життєдіяльності, поширення хмарних платформ, систем штучного інтелекту, великих даних, інтернету речей та кіберфізичних систем формують принципово нове середовище функціонування сучасної держави. Разом із беззаперечними перевагами цифрової трансформації відбувається суттєве ускладнення структури криміногенних загроз, що набувають транснаціонального, латентного, високотехнологічного та адаптивного характеру. Кіберзлочинність у сучасних умовах перестає бути окремим сегментом кримінальної діяльності, поступово трансформуючись у комплексний багаторівневий феномен, який інтегрується у фінансову, соціальну, політичну, інформаційну та безпекову сфери [2].

Формування цифрового середовища як простору взаємодії суб'єктів суспільних відносин спричинило появу нових форм кримінальної активності, що характеризуються високим рівнем анонімності, складністю технічної ідентифікації, використанням розподілених інформаційних інфраструктур та активним застосуванням технологій приховування цифрових слідів. У цих умовах традиційні механізми правоохоронної діяльності виявляються недостатньо ефективними, оскільки орієнтувалися переважно на фізичний простір вчинення правопорушень, лінійні моделі аналізу та реактивний характер прийняття управлінських рішень. Саме тому особливого значення набуває кримінальний аналіз як

інтегрований міждисциплінарний напрям, що поєднує методологію системного аналізу, інструменти інтелектуального аналізу даних, технології OSINT, засоби кіберрозвідки, математичне моделювання ризиків, прогнозування поведінкових сценаріїв та інформаційно-аналітичне забезпечення процесів управління у сфері протидії злочинності.

У сучасному науковому дискурсі кримінальний аналіз дедалі частіше розглядається не лише як окрема функція правоохоронної діяльності, а як стратегічний механізм підтримки управлінських рішень, спрямований на формування доказово обґрунтованої системи реагування на криміногенні процеси. Цифрове середовище значно змінює природу кримінального аналізу, оскільки основним об'єктом дослідження стають інформаційні потоки, цифрові комунікації, поведінкові патерни користувачів, мережеві взаємозв'язки, електронні транзакції, лог-файли, телекомунікаційні метадані, цифрові артефакти та інші структуровані й неструктуровані дані. У таких умовах аналітична діяльність набуває ознак високотехнологічної інтелектуальної системи, яка базується на комплексному застосуванні методів data science, штучного інтелекту, машинного навчання та адаптивного прогнозування ризиків [3].

Кіберзлочинність як складний соціотехнічний феномен характеризується динамічністю, високою швидкістю трансформації та здатністю до самоадаптації. Сучасні кіберзлочинні угруповання активно використовують технології автоматизації атак, шкідливе програмне забезпечення, фішингові механізми, соціальну інженерію, криптовалютні платформи, анонімні мережі, бот-мережі та елементи штучного інтелекту для здійснення деструктивної діяльності. Це суттєво ускладнює процеси виявлення, ідентифікації та прогнозування кіберзагроз. Традиційні підходи до аналізу криміногенної ситуації втрачають ефективність через значний обсяг даних, багатовимірність інформаційних взаємозв'язків та високу швидкість виникнення нових форм кіберризиків.

У контексті цифрового середовища особливого значення набуває системний підхід до організації кримінального аналізу. Системний аналіз дозволяє розглядати кіберзлочинність як складну адаптивну систему, що складається з великої кількості взаємопов'язаних елементів, між якими існують нелінійні зв'язки, зворотні інформаційні потоки та механізми самоорганізації. Застосування принципів системності, ієрархічності, цілісності, багаторівневого моделювання та адаптивного управління забезпечує

можливість комплексного дослідження кіберзагроз, виявлення прихованих закономірностей та формування ефективних управлінських рішень у сфері забезпечення інформаційної безпеки [1].

Важливою особливістю сучасного кримінального аналізу є інтеграція технологій інтелектуального аналізу даних у процес обробки криміналістично значущої інформації. Інтелектуальний аналіз даних дозволяє автоматизувати процес виявлення аномалій, класифікації поведінкових моделей, прогнозування ризиків та встановлення прихованих взаємозв'язків між суб'єктами кримінальної діяльності. Алгоритми машинного навчання, нейронні мережі, кластеризація, дерева рішень, байєсівські моделі, методи асоціативних правил та інші інструменти data mining суттєво розширюють можливості правоохоронних органів у сфері виявлення складних кіберзлочинних схем [4].

Особливу роль у сучасному кримінальному аналізі відіграють технології OSINT, які забезпечують отримання, структуризацію та інтерпретацію інформації з відкритих джерел. В умовах цифровізації значна частина криміналістично важливої інформації міститься у соціальних мережах, форумах, відкритих реєстрах, месенджерах, вебресурсах, телекомунікаційних сервісах та інших елементах цифрового простору. Використання OSINT-технологій дозволяє здійснювати моніторинг інформаційного середовища, аналізувати поведінкові характеристики суб'єктів, встановлювати комунікаційні зв'язки, прогнозувати потенційні ризики та формувати аналітичні профілі об'єктів дослідження. У поєднанні з методами системного аналізу та інтелектуального моделювання OSINT перетворюється на потужний інструмент інформаційно-аналітичного забезпечення управлінської діяльності.

Суттєвого значення у процесі кримінального аналізу набувають питання обробки великих даних. Сучасні інформаційно-аналітичні системи правоохоронних органів функціонують в умовах надзвичайно великих обсягів інформації, що надходить із різноманітних джерел у реальному масштабі часу. Технології Big Data забезпечують можливість інтеграції, агрегації, фільтрації та аналітичної обробки інформаційних потоків із подальшим формуванням прогнозних моделей ризиків. Аналіз великих даних дозволяє виявляти приховані закономірності злочинної діяльності, встановлювати часові та просторові взаємозв'язки між подіями, формувати ризик-орієнтовані профілі та визначати критичні вузли кіберзлочинної активності [3].

Важливим напрямом розвитку кримінального аналізу у цифровому середовищі є використання технологій штучного інтелекту для автоматизації процесів підтримки прийняття управлінських рішень. Системи штучного інтелекту забезпечують можливість адаптивного аналізу інформації, прогнозування сценаріїв розвитку криміногенної ситуації, моделювання ризиків та формування рекомендацій для суб'єктів управління. Використання інтелектуальних аналітичних платформ дозволяє значно скоротити час обробки інформації, підвищити точність прогнозування та забезпечити своєчасне реагування на кіберзагрози.

У сучасних умовах підтримка прийняття управлінських рішень у сфері протидії кіберзлочинності повинна базуватися на ризик-орієнтованому підході. Такий підхід передбачає оцінювання ймовірності виникнення загроз, визначення потенційних наслідків реалізації ризиків та формування пріоритетів управлінського реагування. Системи кримінального аналізу повинні забезпечувати не лише фіксацію фактів протиправної діяльності, а й прогнозування можливих сценаріїв розвитку подій, виявлення тенденцій та формування стратегічних рішень щодо нейтралізації загроз.

Особливого значення набуває інтеграція кримінального аналізу у структуру інформаційно-аналітичних систем правоохоронних органів. Сучасні аналітичні платформи повинні забезпечувати міжвідомчу взаємодію, обмін інформацією, синхронізацію баз даних, підтримку колективного аналізу та формування єдиного інформаційного простору безпеки. В умовах цифрового середовища ефективність управлінських рішень значною мірою залежить від швидкості отримання достовірної інформації, рівня інтеграції інформаційних ресурсів та здатності системи здійснювати адаптивне реагування на динамічні загрози [1].

У контексті сучасних безпекових викликів особливого значення набувають питання кіберстійкості інформаційно-аналітичних систем. Зростання кількості кібератак на державні інформаційні ресурси, критичну інфраструктуру та правоохоронні системи актуалізує необхідність формування комплексної системи кіберзахисту. Кримінальний аналіз у цифровому середовищі повинен враховувати не лише кримінологічні аспекти кіберзлочинності, а й технічні характеристики інформаційних систем, архітектуру мережевих взаємодій, особливості функціонування цифрової інфраструктури та механізми забезпечення кібербезпеки.

Одним із перспективних напрямів розвитку кримінального аналізу є застосування технологій предиктивної аналітики. Предиктивні моделі дозволяють прогнозувати ймовірність виникнення кіберінцидентів на основі аналізу історичних даних, поведінкових характеристик та поточних інформаційних потоків. Використання алгоритмів прогнозування забезпечує можливість переходу від реактивної моделі правоохоронної діяльності до проактивної системи управління безпекою, орієнтованої на попередження загроз.

Не менш важливим аспектом є етичний та правовий вимір використання цифрових технологій у кримінальному аналізі. Активне застосування систем штучного інтелекту, автоматизованого моніторингу, біометричних технологій та масового аналізу даних потребує забезпечення балансу між безпекою та дотриманням прав людини. У сучасних умовах формування інформаційно-аналітичних систем повинно здійснюватися з урахуванням принципів законності, пропорційності, прозорості, відповідальності та захисту персональних даних.

Сучасний кримінальний аналіз поступово трансформується у складну інтегровану систему підтримки управлінських рішень, що функціонує на основі цифрових технологій, алгоритмів штучного інтелекту та міждисциплінарних методологій. Ефективність протидії кіберзлочинності значною мірою залежить від здатності правоохоронних органів здійснювати комплексний аналіз інформації, прогнозувати ризики, адаптуватися до динамічних загроз та забезпечувати високий рівень координації управлінських процесів [2].

Таким чином, кримінальний аналіз у цифровому середовищі виступає одним із ключових елементів сучасної системи забезпечення безпеки держави. Його розвиток безпосередньо пов'язаний із впровадженням інноваційних інформаційних технологій, інтеграцією системного аналізу, штучного інтелекту, OSINT, Big Data та методів інтелектуального прогнозування. Удосконалення інформаційно-аналітичного забезпечення правоохоронної діяльності створює передумови для формування проактивної моделі протидії кіберзлочинності, підвищення ефективності управлінських рішень та забезпечення належного рівня кібербезпеки в умовах цифрової трансформації суспільства [3].

Список використаних джерел:

1. Балтовський О.А., Ісмайлов К.Ю., Сіфоров О.І., Форос Г.В., Заєць О.М. Теорія систем і системний аналіз: навч. посібник. Одеський держ. унів-т внутр. справ, 2020. 156 с.

2. Гончарук О. М. Зародження та еволюція формування кримінального аналізу в світовій парадигмі правоохоронної діяльності. Південноукраїнський правничий часопис. 1. 2023 р. С. 130-137

3. Шинкаренко І. Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 1. С. 5

4. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень: навчальний посібник. Одеса: РВВ ОДУВС. 2022. 176 с.

ЗМІСТ

СЕКЦІЯ 2.
РОЗВИТОК СИСТЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

СЕКЦІЯ 3.
ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

СЕКЦІЯ 4.
OSINT-ТЕХНОЛОГІЇ У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ

СЕКЦІЯ 5.
ІНСТРУМЕНТИ, МЕТОДИ ТА АЛГОРИТМИ ЗАСТОСУВАННЯ OSINT У АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ

СЕКЦІЯ 6.
ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ ТА КІБЕРБЕЗПЕЦІ АНАЛІТИЧНІ, ТЕХНОЛОГІЧНІ ТА ПРАВОВІ АСПЕКТИ

КРИМІНАЛЬНИЙ АНАЛІЗ І КІБЕРБЕЗПЕКА: ОБ'ЄДНАННЯ ЗУСИЛЬ ДЛЯ НОВИХ ВИКЛИКІВ

Матеріали
науково-практичної конференції

22 травня 2026 року

Підписано до друку 22.05.2026. Формат 60х84/16. Папір офсетний.
Гарнітура «TimesNewRoman»/ Друк цифровий.
Ум. друк .арк. 21,62.
Наклад 5 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.