Львівський державний університет внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

26 грудня 2025 року

Львів 2026

УДК 004
І 78
Рекомендовано до розміщення в електронних сервісах ЛьвДУВС Вченою радою Львівського державного університету внутрішніх справ (протокол № 7 від 27.01.2026)

І 78 **Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України**: матеріали Науково-практичної конференції (Львів, 26 грудня 2025) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2026. 346 с.
У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України», що проводилася 26 грудня 2025 року у Львівському державному університеті внутрішніх справ.

УДК 004

Опубліковано в авторській редакції

Абзалов Денис Владиславович

курсант навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, рядовий поліції

Габорець Ольга Андріївна

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

ЦИФРОВІ ЗАГРОЗИ В УМОВАХ ВІЙНИ: РОЛЬ АНАЛІТИЧНИХ ТЕХНОЛОГІЙ У ЇХ НЕЙТРАЛІЗАЦІЇ

Цифровізація сучасних воєн докорінно змінила природу збройних конфліктів, перетворивши кіберпростір, інформаційні канали та мережеві системи на ключові поля протистояння. У контексті російсько-української війни цифрові загрози набули безпрецедентної масштабності та комплексності, поєднуючи кібератаки, інформаційно-психологічні операції, маніпулятивні медіакампанії, використання штучного інтелекту та високотехнологічних автоматизованих платформ. Критичні інфраструктури – енергетика, зв'язок, логістика, державні реєстри – стають мішенями системних атак, спрямованих на дестабілізацію управлінських процесів, дезорганізацію оборони й підрив суспільної довіри. Паралельно здійснюються багаторівневі інформаційні операції, що використовують ботоферми, фейкові наративи, deepfake-контент і таргетовані маніпуляції з метою впливу на громадську думку, політичну волю та міжнародну підтримку України.

Розвиток бойових дій також супроводжується швидким упровадженням автономних систем і безпілотних платформ, які збирають колосальні масиви даних і, водночас, створюють нові цифрові вразливості. Системи керування дронами, канали передавання телеметрії, алгоритми навігації стають об'єктами атак, спрямованих на підміну даних, перехоплення управління, зниження ефективності розвідки та

вогневої підтримки. Таким чином цифрові загрози перетворюються на багатовимірний феномен, що включає технічні, інформаційні та психологічні чинники, які діють одночасно й синергетично. У цій ситуації традиційні інструменти кіберзахисту виявляються недостатніми, оскільки масштаб і динаміка атак вимагають глибшої аналітики, швидкого перехоплення сигналів, прогнозування тенденцій та прийняття рішень у реальному часі.

На цьому тлі особливої ваги набувають аналітичні технології – OSINT, системи великих даних, інструменти машинного навчання та штучного інтелекту, а також платформи кіберзагрозової розвідки. Саме OSINT забезпечує проактивне виявлення підготовки до кібератак, моніторинг діяльності хактивістських і державних кібергруп, аналіз інформаційних потоків і моделювання взаємозв'язків між цифровими об'єктами [1]. Великі дані, накопичені в умовах війни (фронтове відео, сенсорні потоки, логи атаки, комунікаційні метадані), стають фундаментом для формування ситуаційної обізнаності та підтримки стратегічних рішень. Штучний інтелект дозволяє автоматизувати виявлення аномалій, класифікувати наративи дезінформаційних кампаній, оцінювати ризики та прогнозувати поведінку ворожих кіберструктур.

Водночас противник також вдосконалює свої методи, застосовуючи шифрування, анонімізацію, атаки на моделі машинного навчання, ін'єкції «отруєних» даних і гібридні операції, у яких технічні й психологічні інструменти взаємодіють. Саме тому роль аналітичних технологій доповнюється критично важливим людським чинником: здатністю експертів інтерпретувати дані, перевіряти джерела, оцінювати достовірність інформації та приймати етичні й стратегічно виважені рішення. Не менш значущими залишаються міжнародна співпраця, стандарти кіберстійкості, обмін даними та розвиток власних суверенних технологій штучного інтелекту, інтегрованих у національну систему оборони.

У розвитку цифрового протистояння чітко простежується тенденція до переходу від реактивної до прогностичної моделі безпеки. Аналітичні технології дозволяють не лише фіксувати інциденти, а й визначати закономірності їх розвитку, виявляти «слабкі сигнали» майбутніх атак,

прогнозувати цілі противника й будувати сценарії реагування. Війна дедалі більше перетворюється на змагання швидкості обробки даних, точності аналітичних моделей і здатності приймати рішення на основі комплексних інформаційних масивів. Держава, що ефективно інтегрує ці технології, отримує перевагу в інформаційному, кібернетичному та оперативному доменах, а відтак – у загальній системі оборони.

Цифрові загрози в умовах війни становлять складну, багатокомпонентну систему, що охоплює технічні, інформаційні та психологічні впливи. Їх нейтралізація неможлива без аналітичних технологій, які забезпечують перетворення масивів даних на операційно значущі знання, підтримують раннє виявлення атак, прогнозування ризиків та ефективну координацію оборонних дій. Успішна протидія цифровим загрозам вимагає синергії технологічних інновацій, якісної кіберзагрозової розвідки, інституційної та міжнародної співпраці, а також людиноцентричного підходу. Саме ця інтегрована модель забезпечує державі стійкість та адаптивність у гібридній війні XXI століття.

Література

1. Габорець О. А. Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі : робота на здобуття кваліфікаційного ступеня магістра: спец. 125 - Кібербезпека та захист інформації / наук. кер. В. В. Муж. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. 80 с.

Андрусишин Леонтій Богданович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Баб'як Андрій Васильович

завідувач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ

Швидкоплинність розвитку сфери інформаційних технологій та послуг зумовлює потребу безперервної актуалізації своїх знань, вмінь та навичок сучасного оперативника. Умови сьогодення диктують нові, раніше невідомі правила, зумовлені вкрай динамічною імплементацією технологій штучного інтелекту (далі – ШІ) в усі сфери суспільного життя, в тому числі – в оперативно – розшукову діяльність.

Сучасний розвиток інформаційних технологій відкриває нові можливості для підвищення ефективності правоохоронної діяльності. Зокрема, технології штучного інтелекту здатні значно покращити процеси збору, аналізу та інтерпретації даних, що є ключовими в оперативно-розшуковій діяльності та досудовому розслідуванні. Застосування штучного інтелекту в оперативно-розшуковій діяльності передбачає збір та аналіз великого обсягу інформації для виявлення, попередження та розкриття кримінальних правопорушень.

Штучний інтелект може бути використаний для:

– аналізу великих даних, ШІ здатний обробляти великі масиви даних з різних джерел, виявляючи приховані закономірності та зв'язки, що можуть бути корисними для розслідування;

– розпізнавання образів та обличчя, технології комп'ютерного зору дозволяють ідентифікувати підозрюваних на відеозаписах або фотографіях, що прискорює процес їх розшуку;

– прогнозування злочинності, моделі машинного навчання можуть передбачати можливі місця та час вчинення кримінальних правопорушень, що дозволяє правоохоронцям ефективніше планувати патрулювання та інші превентивні заходи [1].

В Україні впровадження ШІ у правоохоронну діяльність знаходиться на початковому етапі. Однак існують значні перспективи для його розвитку. Необхідно створити державну програму розвитку та впровадження ШІ у правоохоронну сферу з урахуванням міжнародного досвіду та національних особливостей. Важливу роль у цьому повинно відігравати Міністерство цифрової трансформації спільно з Міністерством внутрішніх справ. Підготовка фахівців, здатних працювати з технологіями ШІ, є ключовим аспектом успішного впровадження цих технологій. Використання штучного інтелекту (ШІ) у правоохоронній діяльності, зокрема в оперативно-розшуковій діяльності та досудовому розслідуванні, є одним із найбільш перспективних напрямів цифрової трансформації системи правоохоронних органів. ШІ дозволяє не лише реагувати на вже скоєні кримінальні правопорушення, а й працювати на їх випередження. Аналітичні системи, що використовують алгоритми прогнозного поліцейського аналізу (Predictive Policing), можуть визначати райони з підвищеною ймовірністю злочинної активності та допомагати ефективніше розподіляти ресурси правоохоронних органів. Однак цей підхід вимагає додаткових заходів для мінімізації ризиків дискримінації та помилкових висновків [2, с. 36].

Незважаючи на очевидні переваги ШІ, його використання у правоохоронній діяльності викликає серйозні етичні питання. Основними проблемами залишаються можливе порушення права на конфіденційність та захист персональних даних, ризик алгоритмічної дискримінації та упередженості у рішеннях ШІ, відсутність чітких законодавчих норм, що регулюють використання ШІ у кримінальних розслідуваннях, питання відповідальності за рішення, прийняті на основі ШІ. В Україні

використання ШІ в боротьбі зі злочинністю перебуває на початковій стадії розвитку. Однак існує великий потенціал для створення сучасних цифрових систем у правоохоронній сфері. Подальший розвиток у цьому напрямку має включати, удосконалення законодавчої бази, яка регулюватиме застосування ШІ, розробку національних програм цифро-візації правоохоронних органів, впровадження системи етичного та правового контролю за алгоритмами ШІ, навчання спеціалістів, які зможуть ефективно працювати з технологіями штучного інтелекту [3].

Аналізуючи позитивну сторону імплементації досягнень ШІ маємо також згадати і про приховані ризики розповсюдження інформації з обмеженим доступом та такої, що містить таємницю досудового розслідування. Забезпечення захисту такої інформації потребує максимальної уваги та обережності у наданні доступу й опрацюванні криміналістично важливої інформації особами, які проводять досудове розслідування чи розгляд справ у суді. Також варто відмітити, що багато роботи потрібно провести аби напрацювати законодавче врегулювання правомірного використання ШІ в експертній діяльності, розробити стандарти прозорості та аудиту алгоритмів роботи ШІ для оптимізації процесу розслідування злочинів.

ШІ у діяльності правоохоронних органів сьогодні активно використовується під час документування кримінальних правопорушень за допомогою різних інструментів, таких як аналіз даних, машинне навчання, обробка природної мови та розпізнавання образів та ін. При використанні цих інструментів вдається аналізувати великі обсяги даних, виявляти зв’язки та шаблони, що допомагає передбачати майбутні злочинні події та спланувати подальші процесуальні дії. У цьому напрямку використовуються різні інструменти та методи ШІ, включаючи:

1. Аналіз даних: Використання алгоритмів машинного навчання для обробки та аналізу великих обсягів даних, пов’язаних із документуванням кримінальних проваджень, дозволяє виявити тенденції, та, відповідно, вдосконалити організаційно-тактичні форми та методи роботи, спрогнозувати злочинну діяльність та

виявити осіб, які переховуються від органів досудового розслідування та суду. Такий підхід сприяє ефективності документування кримінальних правопорушень а також забезпечує сприятливі умови для оперативно – розшукової діяльності.

2. Геоінформаційні системи (ГІС): ГІС дозволяють аналізувати злочинність на географічному рівні, визначаючи «гарячі точки» та передбачаючи потенційні зони (осередки) злочинності
3. Прогностичне моделювання: із використанням ШІ можна будувати математичні моделі злочинності та передбачати ймовірність вчинення злочинів у певних умовах.
4. Відеоаналітика: Використання комп'ютерного «зору» для аналізу відеоматеріалів дозволяє виявляти кримінальні правопорушення, фіксувати їх та використовувати в якості доказів [4].

Підсумовуючи можемо зробити висновок, що штучний інтелект (ШІ) безперечно й надалі пронизуватиме й інтегруватиметься у оперативно – розшукову діяльність значно підвищуючи ефективність розслідування злочинів і кримінальних правопорушень.Використання ШІ в такій чутливій сфері як оперативно – розшукова діяльність вимагає дотримання суворих юридичних та етичних норм. В Україні існують пропозиції щодо внесення змін до законодавства ,зокрема до Закону України «Про оперативно – розшукову діяльність», аби чітко регламентувати застосування ШІ для обробки оперативнї інформації. Важливо забезпечити захист прав людини, конфіденційність даних та мінімізувати ризики упередженості алгоритмів. Таким чином, ШІ виступає потужним допоміжним інструментом, який значно покращує якість оперативно – розшукової діяльності, але не замінює критичну роль людського судження та прийнятя рішень.

Література

1. Технології штучного інтелекту в документуванні та розслідуванні кримінальних правопорушень. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/479/12832/26799-1?inline=1

2. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. Kriminalistikairteismo ekspertologija: mokslas, studijos, praktika. 2022. Т. 18. С. 31–36.
3. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична: збірник наукових праць. 2023. №3. С.148- 156. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5945/1/19.pdf
4. Концепція розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556-р. URL: https://www.kmu.gov.ua/npas/proshvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 .

Бортник Надія Петрівна

завідувачка кафедри адміністративного та конституційного права Національного кораблебудівного університету імені адмірала Макарова, докторка юридичних наук, професорка

Єсімов Сергій Сергійович

професор кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

МЕТОД АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВНУТРІШНЬОВІДОМЧОГО КОНТРОЛЮ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Правовому регулюванню можуть підлягати не всі суспільні відносини, що складаються в регульованій сфері, а тільки ті, які мають

певні властивості. По-перше, вони повинні бути істотними для досягнення цілей регульованої діяльності. Ігнорування цього принципу часто призводить до перевантаження нормативного акта надмірною кількістю формальних вимог, які не мають вирішального значення для його сутності, але при цьому стають формальними показниками його видимої ефективності. По-друге, вони повинні бути придатними до однозначної формалізації з точки зору виключення вільного тлумачення їх оцінки. По-третє, правове регулювання зберігає призначення, якщо поширює дію на суспільні відносини, що мають властивості повторюваності та систематичності, порушення яких істотно знижує ефективність регульованої діяльності. Однак, вже на цьому загально правовому рівні виявляються різні підходи до визначення правового регулювання.

У теоретичній правовій науці поняття правового регулювання в широкому його значенні прямо не відокремлюють від інших, близьких за змістом понять: правового регулювання у вузькому його значенні, тобто поняття, що відображає процес і організацію правового регулювання конкретної групи суспільних відносин у певному територіальному органі та підрозділі у певний період часу; механізму правового регулювання, тобто поняття, що відображає правове регулювання з інструментальної точки зору: підбору та порядку використання юридичних засобів, адекватних специфіці регульованих суспільних відносин.

Загальнотеоретичне поняття правового регулювання фіксує лише фундаментальні вихідні засади правового регулювання окремих сфер суспільних відносин. Відступ від цих засад знижує ефективність правового регулювання або виключає його. З такого підходу стає зрозумілим, що дослідження правового регулювання зі сфер суспільних відносин у контексті діяльності поліції не може бути успішним без наукової оцінки особливостей суб'єктів правового регулювання, цілей і завдань правового регулювання, предмета правового регулювання, адекватних методів правового регулювання.

Нормативно-правове регулювання внутрішньовідомчого контролю з використанням інформаційних технологій підпорядковане загально-

правовим і галузевим правовим принципам. Однак, воно має ряд особливостей визначених Інструкцією з організації контролю за виконанням документів у Національній поліції України, які пов'язані з функціональним призначенням внутрішньовідомчого контролю [1].

Інструкція з організації контролю за виконанням документів у Національній поліції України передбачає, що облік документів в системі поліції здійснюється з використанням інформаційних технологій відповідно до Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС [2].

Специфіка суспільних відносин, що складаються в процесі організації та здійснення внутрішньовідомчого контролю, дозволяє виділити їх в самостійний предмет правового регулювання, тобто тісно пов'язану групу відносин, що мають однорідність, обумовлену спільністю цілей і завдань. Особливості правовідносин, що утворюють предмет правового регулювання внутрішньовідомчого контролю в системі Національної поліції, повинні мати такі властивості. По-перше, вони повинні бути істотними для досягнення цілей внутрішньовідомчого контролю, по-друге, придатними до однозначної формалізації, по-третє мати властивості повторюваності та систематичності.

Предметом правового регулювання внутрішньовідомчого контролю стає лише та їх частина, яка забезпечує організаційні, процедурні та правозахисні основи стабільності, гарантованості та достовірності цільової інформації про стан і розвиток функціонування поліції та кожного з її територіальних органів, організацій і підрозділів окремо.

Першу частину предмета правового регулювання внутрішньовідомчого контролю складають принципи і цілі організації та реалізації контрольної діяльності, що визначають і конкретизують його місце в системі управлінської діяльності, завдання щодо виявлення недоліків і позитивного досвіду, що істотно впливають на законність і ефективність функціональних завдань поліції.

Другу групу складають відносини, що визначають статус суб'єкта внутрішньовідомчого контролю та його повноваження. Оскільки порядок

організації внутрішньовідомчого контролю покладається на відповідного керівника, його повноваження в цій сфері утворюють два блоки: нормотворчі, що складають нормативно-організаційну діяльність щодо встановлення порядку, цілей і напрямів внутрішньовідомчого контролю підлеглих підрозділів і посадових осіб, і безпосередньо контрольні, що складають діяльність з оцінки результатів внутрішньовідомчого контролю і прийняття на їх основі коригувального управлінського рішення.

До третьої самостійної групи відносин, що складають предмет правового регулювання внутрішньовідомчого контролю, належать відносини, з яких складаються методи та форми здійснення контрольних дій, що забезпечують достовірність і об'єктивність збору цільової інформації, її оперативність і своєчасне вжиття заходів управлінського реагування. Оскільки внутрішньовідомчий контроль є однією з форм управлінської діяльності, помилки в якій можуть спричинити репутаційну та функціональну шкоду діяльності посадових осіб, підрозділів і відомства, важливе значення набуває правове регулювання процесуальних форм здійснення. Сувора регламентація форм внутрішньовідомчого контролю утворює, у зв'язку з цим, самостійне значення як невід'ємна частина предмета правового регулювання.

Класифікація на підставі опосередкованості контрольних функцій виділяє як самостійний вид внутрішньовідомчого контролю – внутрішнє управлінський, характерними рисами якого є: мінімальна нормативна регламентованість; наявність безпосередньої підпорядкованості між суб'єктом і об'єктом контролю; відсутність нормотворчих повноважень у суб'єкта контролю; повсякденність реалізації; основний зміст контролю становить робота з особовим складом, у тому числі й індивідуальна; істотно позначається на результатах усіх інших форм внутрішньовідомчого контролю, будучи фундаментальною передумовою всіх формалізованих показників діяльності всього відомства та підрозділів.

Аналіз порядку правового регулювання системи цілей і принципів організації та реалізації внутрішньовідомчого контролю в поліції показує, що законодавче закріплення принципів внутрішньовідомчого контролю і впровадження принципів комплексної профілактики, спрямованої на

співпрацю контролюючих і підконтрольних суб'єктів в усуненні негативних факторів, що впливають на ефективність і результативність, при його організації мають потенційне перспективне значення для розвитку і організації прозорості та зрозумілості системи внутрішньовідомчого контролю в діяльності органів поліції, а також визначити їх місце в системі принципів організації і здійснення державного управління. У сфері цілепокладання очевидна необхідність поширення спрямованості на використання позитивних контрольних процедур, правовим результатом яких є акт, що містить пропозиції щодо розвитку управлінської діяльності, усунення виявлених порушень, які часто вирішуються шляхом винесення охоронних приписів, щодо усунення порушень.

Метод правового регулювання внутрішньовідомчого контролю відноситься до адміністративно-правового включає всі способи впливу на правовідносини, характерні для нього. До особливостей методу правового регулювання даної сфери суспільних відносин можна було б віднести: використання внутрішньовідомчих нормативно-правових актів як основного джерела норм правового регулювання; певна самостійність контролюючого суб'єкта у виборі засобів, методів і порядку правового регулювання внутрішньовідомчого контролю відповідно до принципів ієрархічності та законності; сувора регламентація форм і засобів внутрішньовідомчого контролю залежно від його виду та напряму; широке використання засобів забезпечення об'єктивності та достовірності методів отримання інформації і оцінки шляхом формування перевірочних комісій з незалежних експертів; сувора процесуальна регламентація взаємодії перевіряючих і підконтрольних суб'єктів; використання відомчої інформаційної системи, де відображаються результати заходів.

Внутрішньовідомчий контроль в Національній поліції – самостійний адміністративно-правовий інститут, що має самостійний предмет і метод правового регулювання. Правове регулювання представляє спеціально організовану внутрішньовідомчу діяльність уповноважених осіб, спрямовану на його вдосконалення, поточний стан правореалізаційної

діяльності в даній сфері, де використання інформаційних технологій утворює окремий напрям правового відомчого регулювання.

Правове регулювання внутрішньовідомчого контролю можна визначити як цілеспрямовану діяльність нормотворчого та правореалізаційного характеру уповноважених посадових осіб та контрольно-наглядових підрозділів Національної поліції щодо впорядкування та реалізації за допомогою інформаційних технологій суспільних відносин у сфері внутрішньовідомчого контролю.

Література

1. Про затвердження Інструкції з організації контролю за виконанням документів у Національній поліції України: Наказ МВС України від 13.06.2016 р. № 503. URL. https://zakon.rada.gov.ua/laws/show/z0944-16#Text
2. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: Наказ МВС України від 20.10.2017 р. № 870. URL. https://zakon.rada.gov.ua/laws/show/z1433-17#n13

Василик Анастасія Василівна

здобувач вищої освіти спеціальності 125 «Системний аналіз» Львівського національного університету імені Івана Франка

Мельничин Андрій Володимирович

доцент кафедри теорії оптимальних процесів Львівського національного університету імені Івана Франка, кандидат технічних наук, доцент

ВИКОРИСТАННЯ ЙМОВІРНІСНИХ ХАРАКТЕРИСТИК ЧАСТОТНОГО СЛОВНИКА ДЛЯ ПОБУДОВИ ТЕМАТИЧНОГО СХОВИЩА ДАНИХ

Упродовж останніх років обсяг текстової інформації зріс настільки, що звичайні методи її опрацювання вже не забезпечують ані потрібної

швидкості, ані достатнього рівня систематизації. Сучасні текстові колекції – це десятки тисяч документів різного стилю й тематики, що суттєво унеможливлює їх ручну класифікацію. Водночас ефективний аналіз таких даних потребує чіткої структури, яка б дозволяла групувати документи за змістом і швидко знаходити необхідний матеріал.

Одним із підходів, що дає змогу сформувати таку структуру, є побудова тематичного сховища на основі статистичних характеристик тексту. Центральним елементом у цьому процесі виступає частотний словник, тобто перелік слів корпусу з вказаною частотою їх появи. Він відображає загальну картину використання лексики, але для більш глибокого аналізу цього недостатньо. У роботі пропонується підхід, у якому частотні характеристики поєднуються з кількома ймовірнісними моделями. Це дозволяє краще описати поведінку різних груп слів і на основі цього будувати тематичну структуру корпусу.

У зв'язку із вищесказаним, маємо задачу проєктування та реалізації тематичного сховища даних на базі достатньо великого текстового корпусу. При цьому повинен забезпечуватися наступний функціонал:

- групування документів за тематичної схожістю;
- можливість оцінювання схожості;
- надання змоги переглядати ключову лексику кожної групи;
- забезпечення зручного пошуку за тематичними ознаками

Також важливо щоб метод побудови не залежав від конкретного типу текстів і міг працювати із загальними корпусами у яких присутні як наукові, так і публіцистичні матеріали.

Основні викладки. Першим кроком у роботі є побудова частотного словника. Після очищення текстів та лематизації підраховуються частоти слів, а далі вони впорядковуються за спаданням. Уже на цьому етапі можна побачити характерну структуру словника: перші позиції займають службові слова, далі поширена лексика, а наприкінці – рідкісні та спеціалізовані терміни. Далі визначається закон розподілу звертання до слів. Серед найвідоміших законів розглядатимемо наступні:

– **Закон Зіпфа.** описує залежність між рангом слова та його частотою. У більшості природних текстів ця закономірність виконується досить добре, частота зменшується швидко, а більшість слів має дуже низькі значення. Така поведінка дає змогу визначати групи слів, що з одного боку не несуть корисної смислової інформації, а з іншого, – навпаки, можуть бути індикаторами теми.

– **Розподіл Пуасона.** Рідкісний словник часто містить найбільш цінні слова з точки зору тематики. Вони трапляються нерегулярно, а їхні частоти добре описуються пуассонівським розподілом. Завдяки цьому можна автоматично відокремлювати слова, які зустрічаються випадково від тих, що слугують маркерами окремих тематичних напрямів.

– **Експоненційний та нормальний розподіли.** Аналітичні дослідження показують, що ймовірності появи середньочастотних слів спадають приблизно експоненційно. Нормальний розподіл добре моделює деякі стилістичні показники, наприклад, варіації середньої довжини слова або частота вживання певних лексичних груп. Ці моделі дозволяють більш точно визначати межі між тематичними кластерами та допомагають уникати надмірної чутливості до окремих текстів.

Тематичне групування документів проводиться методами кластеризації (*K-Means* – дає можливість отримати фіксовану кількість тем, *Ієрархічний метод* – забезпечує побудову дерева, яке відображає вкла/-деність тем). Як основна міра подібності слів застосовується косинусна відстань, оскільки вона краще враховує семантичний напрямок векторів. Отримані кластери формують основу тематичного сховища. Для кожного кластера визначаються такі елементи: перелік документів, ключові слова (терміни, що найбільше вплинули на кластеризацію), зв'язки з іншими темами, внутрішня структура (підтематика).

Паралельно формується матриця ознак подібності документів, що дає змогу швидко знаходити близькі за змістом тексти. Здійснюється це на базі обчислених значень TF – IDF. Така матриця дає змогу оцінювати важливість слова не лише в окремому документі, а й у порівнянні з іншими текстами. У результаті кожен документ перетворюється на вектор великої розмірності. Попередній статистичний аналіз лексики дозволяє

видалити малозначущі високочастотні слова, згладити вплив випадкових рідкісних лексем, уточнити ваги інформативних слів і в кінцевому результаті сформувати стабільну основу для кластеризації

Аналіз показав кілька очевидних і важливих тенденцій. Частоти слів у корпусі розподілилися саме так, як зазвичай буває у природних текстах: найбільш вживані слова трапляються дуже часто, а далі їхня частота швидко падає. Це добре узгоджується із законом Зіпфа і підтверджує, що корпус достатньо різноманітний.

Рідкісні слова проявили себе очікувано: більшість із них трапляється один або кілька разів. Таку поведінку добре описує пуасонівська модель. Саме ця група слів виявилася найбільш корисною під час визначення тем, оскільки серед них часто зустрічаються терміни та специфічні поняття.

Також спостерігалося поступове зменшення частот середньочастотних слів, що нагадує експоненційний спад. Це підтвердило, що можна обмежувати словник певним порогом і не втрачати при цьому важливої інформації.

Щодо кластеризації, то отримані групи документів виявилися досить чіткими. Кожен кластер має свою логічну тему і ці теми легко інтерпретувалися. Побудована дендрограма додатково допомогла побачити, як окремі теми об’єднуються у ширші групи.

У результаті створено тематичне сховище, що значно полегшило роботу з текстами: потрібні документи тепер знаходяться швидше, а переміщення між темами стало набагато зручнішим.

Висновки. Представлений підхід демонструє, що використання ймовірнісних характеристик частотного словника дає можливість набагато точніше визначати структуру текстового корпусу. Поєднання кількох статистичних моделей дозволяє збалансувати вплив різних груп слів та отримати стійкі ознаки для тематичної класифікації.

У результаті формується тематичне сховище, яке є зручним у використанні, забезпечує логічну структуру документів та може бути

застосоване в інформаційних системах різного призначення – від наукових бібліотек, до систем аналітичної обробки великих текстових даних.

Література

1. Moreno-S´anchez I, Font-Clos F, Corral A. Large-scale analysis of Zipf's law in English texts // PLOS ONE. – 2016. – Vol. 11, No. 1. – Article e0147073.
2. Бакуменко О. І. Методи інтелектуального аналізу текстових даних: класифікація та кластеризація документів. // О. І. Бакуменко / Київ: НАУ. – 2017. – 142 с.
3. Кириченко О. В. Методи та моделі інформаційного пошуку: тематична класифікація та індексація текстів. // О. В. Кириченко / Київ: КПІ ім. Ігоря Сікорського. – 2019. – 156 с.

Веселовська Тетяна Сергіївна

ГУНП у Львівській області, доктор філософії

ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Нині науково-технічний прогрес розвивається стрімкими темпами і однією з найпомітніших інновацій є безпілотні літальні апарати (далі – БпЛА). БпЛА – це повітряне судно без пілота, екіпажу чи паса жирів на борту, управління яким здійснюється автоматично чи/або дистанційно за допомогою безпілотної авіаційної систем (безпілотного авіаційного комплексу), що є невід'ємною складовою БпЛА та включає в себе наземний контроль і систему зв'язку із БпЛА [1, с.195].

Так, наприклад, одна з головних причин, чому поліцейські сили Великої Британії почали використовувати дрони – це можливість

забезпечити посилене спостереження. Дрони дають офіцерам можливість оглянути великі території з висоти пташиного польоту, які може бути важко контролювати за допомогою інших традиційних методів. Чи то моніторинг протесту, відстеження підозрюваного чи огляд місця злочину, дрони дозволяють збирати дані в режимі реального часу, що дозволяє поліції приймати більш обґрунтовані рішення [2].

Понад 1500 відділень поліції у США використовують їх у тій чи іншій ролі. Їх використання правоохоронними органами зростає з року в рік [3]. NV Techno повідомляв, що в США правоохоронці за допомогою дронів зафіксували момент зламу кількох автівок і затримали злочинця [4].

Тому, у поліцейській діяльності вони знайшли своє особливе місце, забезпечуючи правоохоронні органи новими можливостями у виконанні оперативно-розшукових завдань [5, с.408].

До основних переваг використання БпЛА Національною поліцією України належать:

– мобільність комплексів БпЛА.

– можливість спостереження за місцями скоєння злочинів (правопорушень).

– можливість доставки та скидання малогабаритних вантажів (як правило, масою до 3 кг) до зони проведення спеціальних заходів.

– можливість після польотного аналізу та обробки отриманої інформації.

– використання мінімального штату для запуску БПЛА, а також доступна можливість підготовки (перепідготовки) персоналу.

– забезпечення безпеки співробітників, які беруть участь у спеціальних заходах, з урахуванням наземної оперативної обстановки, що складається.

– не складна система управління БПЛА, дозволить швидко підготовити оператора безпілотника.

– використання БпЛА для огляду місця події з метою виявлення доказів та їх подальшої фіксації під час проведення розслідування.

– непомітність і малошумність, можливість застосування в умовах міської забудови, оперативність розгортання.

– координації підрозділів поліції з повітря в різних умовах складної обстановки.

– документування злочинів та отримання оперативної інформації (негласне документування дій, спостереження та контроль у важкодоступних місцях і т. д.) [6, с.99-100].

– значно нижчі витрати на експлуатацію порівняно з використанням традиційних авіаційних засобів, таких як гелікоптери [5, с.409].

До проблемних питань використання БпЛА у оперативно-розшуковій діяльності вчені виділяють:

– правові обмеження, які впливають на можливості їх застосування. Відсутність чіткої регламентації щодо того, коли, як і де можуть бути задіяні дрони, спричиняє правові колізії та обмежує оперативні можливості правоохоронців.

– потреба в спеціалізованих знаннях та підготовці персоналу, високі вимоги до експлуатації та обслуговування обладнання.

– обмежена тривалість польоту БпЛА є суттєвими факторами, що впливають на ефективність їх використання.

– необхідність значних фінансових вкладень для закупівлі сучасних дронів та обладнання, а також інтеграції їх у загальну систему оперативно-розшукових дій додає викликів для правоохоронних структур, що ставить перед українським суспільством завдання створення нових підходів та стандартів у цій сфері [7, с.164-165].

– застосування технологій відеофіксації може відбуватися лише за наявності відповідного дозволу, особливо коли це стосується приватної території або особистих даних громадян [7, с.166]. Тобто є питання приватності та етичних норм [5, с.408].

– високу витратність на впровадження та обслуговування безпілотних систем, що впливає на можливість їх широкого використання [7, с.166].

– залежність від погодних умов [5, с.408].

– побоювання значної частини суспільства щодо потенційного зловживання цими технологіями. Ці побоювання не є безпідставними, оскільки такі технології можуть бути використані для створення баз

даних, що містять чутливу інформацію про громадян, а також для застосування надмірних заходів контролю. Це питання вимагає чітких та жорстких правових рамок, які б регулювали використання дронів, забезпечуючи прозорість і підзвітність правоохоронних органів [7, с.168].

– захист від зловживання дронами з боку самих злочинців, які можуть використовувати БпЛА для своїх незаконних цілей. Наприклад, дрони можуть використовуватися для шпигунства, незаконної відеозйомки або доставки заборонених предметів до місць позбавлення волі. Правоохоронним органам необхідно розробити ефективні заходи проти/-дії таким злочинним діям, що включають не лише технічні засоби нейтралізації дронів, але й удосконалення нормативно-правової бази [7, с.169].

Використання БпЛА на сьогоднішній день, з урахуванням прогре/-сивних напрямків науки і техніки, є звичайним явищем, а спектр їх застосування є досить широким. В оперативно-розшукової діяльності надає правоохоронним органам України нові можливості у розслідуванні злочинів. Так, впровадження новітніх технологій завжди супроводжується як позитивними, так і негативними наслідками. Однак, незважаючи на свої недоліки у застосуванні та використанні, БпЛА завдяки своїм можливостям, не тільки швидко та ефективно фіксують правопорушення, а й збирають докази (фото- та відеоматеріали). Тому використання БпЛА в оперативно-розшуковій діяльності Національної поліції має свої подальші перспективи для розвитку (нормативно-правове регулювання, вдосконалення та впровадження новітніх технологій та ін.).

Література

1. Саковський А.А., Мировська А.В., Бистрицький Б.Ю. Окремі питання класифікації безпілотних літальних апаратів. Науковий вісник публічного та приватного права. Випуск 1. 2025. С.194-201.
2. UK Police Forces and Drones: 10 Years On. URL: https://eeinnovationsltd.com/training/uk-police-forces-and-drones-10-years-on/. (дата звернення 02.12.2025).
3. The future is here. In the US, drones will work as police and rescue workers. URL: https://techno.nv.ua/ukr/innovations/v-ssha-droni-pracyuvatimut-yak-policiya-i-ryatuvalniki-50437448.html (дата зв-я 02.12.2025).

4. California police have arrested a car thief who was spotted by a camera mounted on a drone. URL: https://techno.nv.ua/ukr/innovations/dron-dopomig-zatrimati-zlochincya-video-z-miscya-podiji-50435845.html (дата звернення 03.12.2025).
5. Єфімова І.В., Розгон О.Г. Використання безпілотних літальних апаратів у оперативно-розшуковій діяльності Національної поліції України. Юридичний науковий електронний журнал. №7/2024. С.407-410. DOI https://doi.org/10.32782/2524-0374/2024-7/98.
6. Лизогубенко Є.В. Актуальні аспекти використання безпілотних літальних апаратів Національною поліцією України в умовах воєнного стану. Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану: матеріали наук.-практ. конф. 30 березня 2023 року. Київ. 2023. С. 98-101.
7. Єфімов В., Асламов О. Використання дронів в оперативно-розшуковій діяльності: практичні аспекти та правові обмеження. Здобутки та досягнення прикладних та фундаментальних наук XXI століття: збірник наукових праць з матеріалами VIII Міжнародної наук. конф. 22 листопада 2024 року. м.Біла Церква. 2024. С. 164-171.

Войтюк Олеся Романівна

здобувач вищої освіти освітнього ступеня «бакалавр» спеціальності «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Зачек Олег Ігорович

кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій Львівського державного університету внутрішніх справ

МЕТОДОЛОГІЯ ТА ТЕХНОЛОГІЇ OPEN SOURCE INTELLIGENCE У СУЧАСНІЙ ІНФОСФЕРІ

Інформаційне суспільство XXI століття характеризується стрімким зростанням обсягів відкритих даних, зумовленим діджиталізацією та

формуванням глобального інформаційного простору. Це сприяло трансформації розвідувальної діяльності й становленню OSINT як розвідки з відкритих джерел. Із вузькоспеціалізованого інструменту спецслужб OSINT перетворився на загальнодоступну аналітичну методологію, що застосовується в науковій, журналістській та безпековій сферах. Водночас зростання інформаційних загроз актуалізує потребу в усвідомленні можливостей і меж використання OSINT.

OSINT (Open Source Intelligence) є напрямом інформаційно-аналітичної діяльності, що передбачає аналіз даних з відкритих джерел для отримання обґрунтованих висновків. OSINT має міждисциплінарну природу, поєднуючи аналітику розвідки, інформаційні технології, кібербезпеку, цифрову криміналістику та соціальні науки. Його ключовою особливістю є використання виключно відкритих і легально доступних джерел, що відрізняє OSINT від інших видів розвідки та забезпечує дотримання прав людини [1].

Стрімке зростання цифрового контенту в інтернеті, співмірне із закономірністю закону Мура, призводить до швидкого подвоєння обсягів відкритих даних, створюючи водночас можливості й виклики для OSINT-аналітиків. Методологія OSINT поєднує класичний аналіз із сучасними цифровими інструментами, що забезпечує ефективну обробку великих масивів інформації з дотриманням вимог законодавства України [2].

Джерельна база OSINT охоплює широкий спектр відкритих ресурсів – від традиційних ЗМІ, наукових і офіційних матеріалів до соціальних медіа, відкритих баз даних, мультимедійного контенту, метаданих, даних Інтернету речей і супутникових зображень. Джерела класифікуються за доступністю та правовим статусом, виокремлюючи відкриті, публічні та легітимні ресурси. Також використовується поділ інформації на первинну та вторинну залежно від способу її створення й обробки [1].

Розвиток інформаційно-комунікаційних технологій зумовив еволюцію OSINT і появу спеціалізованих напрямів, таких як SOCMINT, FININT, GEOINT і DIGMINT, що нині функціонують у межах єдиної аналітичної екосистеми відкритих джерел. Зростання цифрових слідів посилює аналітичний потенціал OSINT, водночас ускладнюючи відбір, перевірку та

інтеграцію релевантної інформації в умовах інформаційного надлишку. Методологічну основу сучасного OSINT становлять мультимодальні підходи та принципи системного збору, критичної оцінки, тріангуляції й верифікації даних, що забезпечують комплексний аналіз різнорідної інформації [3].

Юридичне регулювання OSINT охоплює норми інформаційного, кримінально-процесуального права, законодавства про захист персональних даних, приватність та інтелектуальну власність. В Україні правову основу OSINT становлять положення Конституції України та спеціальні закони у сфері інформації, доступу до публічних даних, кібербезпеки, розвідувальної й оперативно-розшукової діяльності [4]. Конституційне право на інформацію поєднується з можливими законними обмеженнями, а Закон України «Про інформацію» формує базові принципи відкритості й доступності даних [5]. Водночас використання OSINT зумовлює необхідність балансу між відкритістю інформації та захистом приватності: обробка персональних даних має відповідати меті їх оприлюднення, принципу цільового обмеження та підвищеним вимогам до чутливих категорій даних [6]. На міжнародному рівні нормативні рамки OSINT визначаються, зокрема, GDPR і ключовими конвенціями у сфері прав людини та кіберзлочинності, які встановлюють суворі умови правомірної обробки персональної інформації [7].

Складність правового регулювання OSINT зумовлена транскордонністю інформаційного простору, коли дані зберігаються в різних юрисдикціях із відмінними правовими режимами, що ускладнює застосування національного законодавства та зумовлює використання доктрини екстратериторіальності. Водночас OSINT-діяльність має виразний етичний вимір, пов’язаний із межами приватності, ризиками деанонімізації, можливим завданням шкоди гідності та репутації осіб у разі використання неточної чи неповної інформації. У цьому контексті ключового значення набувають деонтологічні принципи, зокрема мінімізація збирання даних, забезпечення їх точності та актуальності, а також обмеження строків зберігання персональної інформації [8].

Дезінформація та маніпулятивний контент створюють для OSINT серйозні етичні виклики, зокрема відповідальність за використання перевірених даних і дотримання суворих стандартів верифікації. Особливої уваги потребують розслідування щодо вразливих груп, де професійна етика OSINT вимагає пропорційності, мінімізації шкоди, захисту приватності та усвідомлення соціальної відповідальності за оприлюднені результати [9].

Методологія OSINT розслідувань є циклічним і поетапним процесом, що поєднує формулювання дослідницького запиту, визначення меж аналізу та ідентифікацію релевантних джерел. Подальші етапи охоплюють систематичний збір даних з відкритих ресурсів, їх обов'язкову верифікацію шляхом перехресної перевірки й аналізу метаданих, а також комплексну аналітичну обробку із застосуванням контентного, мережевого та просторово-часового аналізу. Завершальною стадією є синтез і візуалізація результатів [10].

Пошукові системи загального призначення, такі як Google, Bing, Yahoo, DuckDuckGo та Baidu, є ключовими інструментами в арсеналі OSINT-аналітика. Для їх ефективного використання необхідно володіти специфічними синтаксичними конструкціями та операторами, які отримали назву «дорки» (dorks). Відмінності в алгоритмах пошукових систем зумовлюють інформаційну асиметрію, тому OSINT-аналітики застосовують диверсифікацію інструментів, розширені запити й фільтри для повнішого доступу до релевантних даних. Для наукової верифікації використовують спеціалізовані академічні пошукові платформи та бібліометричні показники оцінки джерел, а метапошукові й технічні системи дають змогу агрегувати результати та аналізувати цифрову інфраструктуру. Архівні сервіси забезпечують дослідження історичних версій вебконтенту, що є ключовим для виявлення змін, видалень і спроб приховування інформації [2].

Публічні реєстри, технічні, фінансові та криптографічні бази даних формують ключову джерельну основу OSINT, забезпечуючи доступ до офіційної, інфраструктурної й корпоративної інформації, у тому числі для

транскордонного аналізу. Соціальні мережі доповнюють цю базу масивами структурованих і неструктурованих даних, що дозволяють формувати «цифрові портрети» осіб і організацій, реконструювати соціальні графи, часові та просторові патерни активності. Використання мережевого аналізу, метаданих і крос-платформної тріангуляції дає змогу виявляти приховані зв'язки, центри впливу та спроби маскування цифрових слідів [10].

Професійні OSINT-розслідування вимагають застосування спеціалізованого програмного забезпечення, яке забезпечує автоматизацію рутинних операцій збору та обробки даних, дозволяє інтегрувати інформацію з різнорідних джерел і використовувати складні аналітичні алгоритми для виявлення прихованих взаємозв'язків між об'єктами розслідування. Технологічна екосистема OSINT-інструментів відзначається високою швидкістю розвитку, регулярним оновленням функціональних можливостей, розширенням набору аналітичних модулів та здатністю адаптуватися до змін в інформаційному ландшафті, а також до нових вимог законодавства [11].

Автоматизація є ключовим напрямом розвитку OSINT, оскільки дозволяє масштабувати розслідування, зменшити рутинне навантаження та подолати інформаційну надмірність, з якою не справляється ручна обробка даних. Вона реалізується у вигляді централізованих або розподілених систем і потребує поєднання алгоритмічної ефективності з людським контролем, насамперед на етапах верифікації та інтерпретації результатів. Технічно автоматизація базується на програмних інструментах збору даних (веб-скрапінг, API), їх фільтрації й аналізу в межах єдиного OSINT-pipeline, який забезпечує масштабованість, модульність, безпеку та зручність роботи аналітиків [1].

Використання штучного інтелекту та машинного навчання суттєво розширює можливості OSINT-автоматизації, забезпечуючи автоматичний аналіз текстового й візуального контенту, класифікацію даних і формування аналітичних висновків на основі різнорідних джерел. Трансформерні моделі та комп'ютерний зір підвищують точність семантичного аналізу, розпізнавання об'єктів і встановлення контексту, а

федеративні архітектури дозволяють масштабувати та координувати розслідування в розподілених середовищах. Загалом OSINT постає як легальна, міждисциплінарна методологія системного аналізу відкритих даних, що поєднує технологічну автоматизацію з правовими та етичними обмеженнями, спрямованими на захист приватності й забезпечення соціальної відповідальності аналітичної діяльності [12].

Перспективним напрямом розвитку OSINT є інтеграція технологій штучного інтелекту, обробки природної мови, комп'ютерного зору та мережевого аналізу для підвищення аналітичного потенціалу та масштабування процесів збору даних. Концепція OSINT-pipeline, що передбачає систематизований підхід до автоматизації розслідувань, демонструє можливості подолання інформаційної надмірності та оптимізації аналітичних процесів.

Комплексний аналіз OSINT-методології виявляє подвійний характер цифрової відкритості: вона одночасно надає унікальні можливості дослідникам та створює ризики для приватності, інформаційної безпеки та соціальної стабільності. Ефективне використання OSINT-інструментарію потребує врівноваження технологічних можливостей із етично-правовими обмеженнями, а також постійного підвищення професійних компетенцій фахівців для адаптації до динамічного інформаційного середовища.

Результати дослідження свідчать, що у контексті гібридних загроз, інформаційних протистоянь та кіберзлочинності OSINT набуває стратегічного значення як інструмент забезпечення інформаційної безпеки, протидії дезінформації та захисту національних інтересів у кіберпросторі.

Література

1. What is OSINT (Open Source Intelligence)? URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/ (дата звернення: 10.12.2025).
2. Bazzell, M. (2023). OSINT Techniques: Resources for Uncovering Online Information (10th ed.). IntelTechniques.com.

3. Tal, L. (n.d.). Threat Intelligence Lifecycle: Phases & Best Practice Explained. URL: https://snyk.io/articles/threat-intelligence/threat-intelligence-lifecycle/ (дата звернення: 10.12.2025).
4. Конституція України від 28.06.1996. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/ 254%D0%BA/96-%D0%B2%D1%80 .
5. Закон України «Про інформацію» від 02.10.92 № 2658-XII // Відомості Верховної Ради України, 1992, № 48, ст.650.
6. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.
7. Regulation (EU) 2016/679 (GDPR). General Data Protection Regulation. Official Journal of the European Union L119/1–88, 2016. URL: https://gdpr-info.eu/?utm_source=data-act-law.eu (дата звернення: 10.12.2025).
8. Tools information struggle: OSINT, IPSO andopposition misinformation. URL: https://infolight.in.ua/wp-content/uploads/2023/02/brochure-2.pdf (дата звернення: 10.12.2025).
9. Van Puyvelde, D., & Tabárez Rienzi, A. (2025). The rise of open-source intelligence. European Journal of International Security. URL: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586 (дата звернення: 10.12.2025).
10. Intelligence from open sources (Open-sourceintelligence - OSINT). URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ (дата звернення: 10.12.2025).
11. RAWiT. (n.d.). OSINT: Understanding your digital footprint. URL: https://rawit.ca/osint-understanding-your-digital-footprint/ (дата звернення: 10.12.2025).
12. What is threat intelligence? URL: https://nordvpn.com/uk/features/threat-protection/threat-intelligence/ (дата звернення: 10.12.2025).

Волобоєва Злата Олегівна

студентка навчально-наукового інституту права та соціального менеджменту Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

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

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В умовах гібридної війни кіберзлочинність трансформується з переважно економічно мотивованої протиправної діяльності у складовий елемент системного деструктивного впливу на національну безпеку, державне управління та суспільну стабільність. Цифровий простір використовується не лише як середовище вчинення злочинів, а й як інструмент реалізації інформаційно-психологічних операцій, саботажу критичної інфраструктури, підриву довіри до органів влади та правоохоронної системи. За таких умов ефективна протидія кіберзлочинності неможлива без розвиненої інформаційно-аналітичної підтримки, здатної забезпечити випереджувальне виявлення загроз, глибоке осмислення їх природи та обґрунтоване прийняття управлінських і процесуальних рішень.

Інформаційно-аналітична підтримка протидії кіберзлочинності в умовах гібридної війни набуває міждисциплінарного характеру, поєднуючи інструменти кримінального аналізу, кібербезпеки, цифрової криміналістики, розвідки з відкритих джерел та аналітики великих даних [1]. Її сутність полягає у системному зборі, верифікації, інтеграції та інтерпретації різнорідної інформації з метою формування цілісної картини кіберзагроз, ідентифікації суб'єктів протиправної діяльності, їх інфраструктури, мотивації та зв'язків. На відміну від традиційного аналізу кіберінцидентів, сучасна аналітична діяльність повинна враховувати гібридну

природу загроз, коли межі між кримінальними угрупованнями, хактивізмом і керованими ззовні кібератаками стають дедалі більш розмитими.

Особливе значення в цьому контексті має перехід від реактивної моделі реагування до проактивної аналітики, орієнтованої на прогнозування та попередження кіберзлочинних проявів. Аналіз поведінкових патернів зловмисників, кореляція технічних індикаторів компрометації з фінансовими, комунікаційними та соціальними слідами дозволяють виявляти підготовчі стадії атак, оцінювати потенційні наслідки та визначати найбільш уразливі об'єкти впливу. У цьому аспекті інформаційно-аналітична підтримка виконує не лише допоміжну, а стратегічну функцію, формуючи підґрунтя для розроблення державної політики у сфері кібербезпеки та кримінальної юстиції.

Важливою складовою аналітичного забезпечення є використання стандартизованих моделей опису кіберзлочинної діяльності, що забезпечують уніфікацію підходів до фіксації, аналізу та інтерпретації даних. Формалізація тактик, технік і процедур зловмисників підвищує якість міжвідомчої взаємодії, спрощує міжнародний обмін інформацією та сприяє підвищенню доказової спроможності матеріалів кримінальних проваджень. Водночас у гібридній війні аналітика має виходити за межі суто технічного аналізу, доповнюючись оцінкою інформаційного ефекту кібератак, їх впливу на громадську думку, соціальні настрої та легітимність державних інститутів.

Додатковим викликом для інформаційно-аналітичної підтримки стає активне використання штучного інтелекту та автоматизованих інструментів у кіберзлочинній діяльності. Масштабування фішингових кампаній, створення переконливого синтетичного контенту, автоматизований підбір жертв і адаптація сценаріїв соціальної інженерії суттєво ускладнюють виявлення та атрибуцію злочинів. У відповідь аналітичні підрозділи змушені впроваджувати методи поведінкового аналізу, графових моделей взаємозв'язків, контент-аналізу та машинного навчання, поєднуючи технологічні можливості з правовими гарантіями захисту прав і свобод людини.

Не менш важливим є організаційно-правовий вимір інформаційно-аналітичної підтримки, який передбачає чітке регламентування доступу до даних, забезпечення цілісності та допустимості цифрових доказів, а також налагодження стійкої взаємодії між правоохоронними органами, спеціальними службами та приватним сектором. Умови гібридної війни об'єктивно зумовлюють необхідність міжнародної координації, оскільки кіберзлочинні екосистеми мають транснаціональний характер, а їх інфраструктура часто розміщується поза межами однієї юрисдикції.

Узагальнений науковий висновок полягає в тому, що інформаційно-аналітична підтримка протидії кіберзлочинності в умовах гібридної війни є ключовим інструментом забезпечення національної безпеки, який інтегрує технологічні, аналітичні та правові механізми у єдину систему протидії. Її ефективність визначається здатністю трансформувати великі обсяги різнорідних даних у науково обґрунтовані аналітичні продукти, орієнтовані на прогнозування, превенцію та доказове реагування, що в сукупності дозволяє зменшити деструктивний вплив кіберзлочинності та підвищити стійкість держави в умовах гібридного протистояння.

Література

1. Габорець О. А., Пекарський С. П. Кіберзлочини як об'єкт правової класифікації. Українська поліцеїстика: теорія, законодавство, практика. 2025. № 2 (серп.). С. 100-105. DOI: https://doi.org/10.32782/2709-9261-2025-2-14-18

Olha Haborets
Associate Professor of the Department of Operational-Search Activities and Information Security Educational and Scientific Institute for Training Specialists for Criminal Police Units named after E.O. Didorenko Donetsk State University of Internal Affairs PhD, Associate Professor

FORMATION OF ANALYTICAL DIGITAL COMPETENCIES OF FUTURE LAW ENFORCEMENT OFFICERS IN THE CONTEXT OF EDUCATIONAL DIGITALIZATION

The contemporary trajectory of civilizational development is characterized by pervasive digitalization across all spheres of social life, which fundamentally reshapes the functioning of social institutions, alters the nature of communication, and generates a multidimensional information environment saturated with vast amounts of data. For law enforcement agencies, this means the necessity to reconsider the very essence of professional activity, as crime is rapidly shifting into the digital domain, acquiring a networked and technologically sophisticated character, while counteracting it requires the use of advanced electronic tools and a high level of analytical culture. Under these conditions, the formation of analytical digital competencies among future law enforcement officers becomes not merely an element of professional training but a crucial factor in ensuring the national security of the state.

These competencies must be viewed as a multi-level, integrated construct that encompasses cognitive, technological, operational, legal, and ethical dimensions. Analytical digital competence is defined as the ability to operate effectively with data in a digital environment, including the processes of collection, processing, critical analysis, interpretation of results, and application of the acquired information within professional activities. This refers to the development of a specific type of professional thinking oriented toward the identification of patterns, construction of logical analytical structures, forecasting the development of events, and making decisions based on objective evidence. For a law enforcement officer, this entails the ability to efficiently use OSINT-technologies, intelligent monitoring systems,

criminal analysis methodologies, crime-mapping tools, digital trace analysis, social media analytics, and various technical sources of information.

In an environment where digital crime exhibits a high degree of latency, and criminal groups actively employ anonymization techniques, cryptographic tools, and complex concealment strategies, a law enforcement officer must be capable not only of establishing the fact of an offense but also of reconstructing the digital footprint of the crime, restoring the logic of the offender's behavior, identifying indicators of interference with digital infrastructure, and determining the origins of information flows. It is precisely analytical digital competencies that provide the intellectual foundation necessary for deep data analysis, which in turn ensures operational accuracy and timely decision-making.

The digitalization of education significantly expands the possibilities for developing these competencies. Modern technologies allow the modeling of situations that closely approximate real-world scenarios, the application of case-based learning built on actual crime patterns, the use of interactive platforms, online simulators of investigative and operational activities, digital laboratories, and artificial intelligence systems for forensic analysis. Importantly, the digital educational environment offers learners the opportunity not merely to passively perceive information but to actively engage with it: to conduct experiments, test hypotheses, analyze variable datasets, and adapt digital tools to specific professional contexts [1].

One of the fundamental advantages of educational digitalization lies in the ability to develop learners' skills in independent information management and data-driven decision-making. This is particularly essential for future law enforcement officers who often operate under conditions of uncertainty, limited time, and increased risk. The ability to navigate information flows swiftly, identify relevant sources, and utilize digital tools effectively minimizes errors and enhances the quality of operational measures.

At the same time, digitalization necessitates updating the content of educational programs. Traditional approaches focusing solely on legal knowledge no longer meet contemporary requirements. Law enforcement training becomes inherently interdisciplinary, incorporating elements of

cybersecurity, forensic cybernetics, psychology of digital behavior, information analytics, digital law, big data methodologies, and foundational concepts of machine learning. Only such an integrated model can produce competencies aligned with the real needs of professional practice.

Pedagogical interaction also plays a pivotal role in forming analytical digital competencies. In the digital environment, the instructor is no longer a conventional transmitter of knowledge but rather a facilitator, analyst, designer of the pedagogical process, and consultant on the use of technological tools. The instructor's professionalism determines whether future law enforcement officers acquire not only technical proficiency but also the culture of critical analytical thinking that forms the basis of professional effectiveness in the security sector.

Equally important are the legal considerations associated with digital competence. Law enforcement activity in the digital environment inevitably involves the processing of personal data, access to confidential information, use of specialized technical means, and compliance with procedural requirements governing the collection and preservation of digital evidence. Future specialists must possess a deep understanding of legislation, international standards, ethical constraints, and principles establishing the legality of digital interventions. Analytical competence cannot be reduced to technical skill; it must incorporate legal literacy and professional responsibility.

The formation of analytical digital competencies among future law enforcement officers is a systematic, long-term, and consistent process. It must be grounded in modern pedagogical approaches, innovative technologies, adaptive teaching methods, and close cooperation with practical police units capable of providing real data, operational scenarios, incident analyses, and access to technological tools. Only such collaboration ensures the development of a comprehensive skill set necessary for effective work in the digital domain.

In summary, the formation of analytical digital competencies among future law enforcement officers represents one of the key prerequisites for successful modernization of Ukraine's internal security sector. In a world where digital technologies constitute the foundation of social communication

and serve simultaneously as an instrument of criminal activity, the law enforcement officer of a new generation must be a technologically proficient professional capable of applying sophisticated analytical tools, working with large datasets, predicting criminal dynamics, and making informed decisions under conditions of significant informational complexity. The effectiveness of the national law enforcement system in the digital era – and, consequently, the level of national security – depends on how successfully higher education institutions develop these competencies within their educational programs.

References

1. Волобоєв А.О., Лунгол О.М., Габорець О.А. Розвиток цифрової компетентності майбутніх фахівців юридичного спрямування: практичні аспекти. Вісник науки та освіти: журнал. 2022. № 5(5) 2022. С. 193-204.

Габорець Ольга Андріївна

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

Чумаченко Максим Денисович

курсант навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, рядовий поліції

ФОРМУВАННЯ АНАЛІТИЧНИХ ЦИФРОВИХ КОМПЕТЕНТНОСТЕЙ МАЙБУТНІХ ПРАВООХОРОНЦІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ОСВІТИ

Цифрова трансформація суспільства та стрімкий розвиток інформаційно-комунікаційних технологій зумовлюють якісні зміни у характері правоохоронної діяльності, де ключовим ресурсом стає цифрова

інформація, а базовою професійною вимогою – здатність до її глибокого аналітичного опрацювання. У цих умовах система вищої освіти, що здійснює підготовку майбутніх правоохоронців, стикається з необхідністю цілеспрямованого формування аналітичних цифрових компетентностей, які виходять за межі елементарної цифрової грамотності та передбачають інтеграцію технологічних, когнітивних, правових і ціннісних компонентів. Цифровізація освіти виступає не лише інструментом модернізації освітнього процесу, а й середовищем, у якому відбувається професійна соціалізація здобувачів освіти відповідно до викликів цифрової реальності.

Аналітичні цифрові компетентності майбутніх правоохоронців доцільно розглядати як здатність здійснювати цілеспрямований пошук, критичну оцінку, інтерпретацію, систематизацію та доказово орієнтоване використання цифрових даних з метою прийняття обґрунтованих управлінських і процесуальних рішень [1]. Вони формуються на основі поєднання інформаційно-аналітичного мислення, навичок роботи з цифровими середовищами, розуміння алгоритмічних процесів та усвідомлення правових і етичних обмежень використання інформації. На відміну від загальних цифрових компетентностей, аналітичний компонент акцентує увагу не на володінні інструментами, а на здатності вибудовувати логіку аналізу, формулювати гіпотези, виявляти приховані зв'язки між даними та оцінювати рівень достовірності отриманих результатів.

Цифровізація освітнього процесу створює передумови для переходу від репродуктивних моделей навчання до діяльнісно-аналітичних, у межах яких цифрові технології стають не об'єктом вивчення, а засобом професійного мислення. Освітні платформи, симуляційні середовища, навчальні кейси на основі цифрових даних, елементи аналізу відкритих джерел інформації та моделювання реальних службових ситуацій дозволяють формувати у здобувачів освіти досвід роботи з інформаційною невизначеністю, надлишковістю даних та ризиком маніпуляцій. У цьому контексті особливого значення набуває розвиток критичного ставлення до цифрових джерел, уміння виявляти дезінформацію, фальсифікований контент і алгоритмічні викривлення, що є характерними ознаками сучасного інформаційного простору.

Важливим аспектом формування аналітичних цифрових компетентностей є їх нормативно-правова детермінованість. Майбутній правоохоронець повинен усвідомлювати, що будь-яка аналітична діяльність у цифровому середовищі має здійснюватися в межах законності, із дотриманням прав і свобод людини, принципів пропорційності та мінімізації втручання у приватне життя. Це вимагає інтеграції у зміст освітніх програм знань про правовий режим цифрових даних, електронні докази, захист персональної інформації та кібербезпеку, а також формування відповідальних професійних установок щодо використання аналітичних інструментів. Таким чином, аналітичні цифрові компетентності набувають не лише функціонального, а й світоглядного значення.

Не менш суттєвим є педагогічний вимір цифровізації освіти, оскільки ефективність формування аналітичних компетентностей безпосередньо залежить від готовності викладачів проєктувати навчальний процес у логіці цифрової аналітики. Це передбачає використання проблемно-орієнтованих завдань, міждисциплінарних кейсів, формувального оцінювання та рефлексивних практик, спрямованих на усвідомлення здобувачами освіти власних аналітичних рішень і помилок. У такому підході цифрові технології виступають каталізатором розвитку професійного мислення, а не самоціллю освітнього процесу.

Отже, формування аналітичних цифрових компетентностей майбутніх правоохоронців в умовах цифровізації освіти є комплексним і багатоаспектним процесом, який потребує поєднання сучасних цифрових освітніх середовищ, аналітично зорієнтованого змісту навчання, правової та етичної регламентації діяльності й високого рівня педагогічної майстерності. Саме така інтегрована модель підготовки забезпечує здатність майбутніх фахівців ефективно діяти в умовах цифрових викликів, приймати обґрунтовані рішення та виконувати правоохоронні функції на належному професійному й суспільно значущому рівні.

Література

1. Волобоєв А.О., Лунгол О.М., Габорець О.А. Розвиток цифрової компетентності майбутніх фахівців юридичного спрямування: практичні аспекти. Вісник науки та освіти: журнал. № 5(5) 2022. С. 193-204.

Галайко Наталія Володимирівна

старший викладач кафедри інформаційних технологій Львівського державного університету внутрішніх справ

Шевченко Наталія Володимирівна

доцент кафедри менеджменту та економічної безпеки, к.е.н., доцент Львівського державного університету внутрішніх справ

СУЧАСНІ ПІДХОДИ ДО МОДЕЛЮВАННЯ ДИНАМІКИ ДЕРЖАВНОГО БОРГУ

Державний борг є одним із ключових макроекономічних показників, що характеризує фінансову стійкість держави та її здатність забезпечувати стабільний соціально-економічний розвиток. Рівень і динаміка державного боргу істотно впливають на інвестиційний клімат, довіру внутрішніх і зовнішніх кредиторів, а також на позиції країни у міжнародних фінансових рейтингах. Надмірне боргове навантаження призводить до обмеження фіскальних можливостей уряду, зростання витрат на обслуговування боргу, підвищення податкового тиску та посилення соціально-економічних ризиків. Особливої гостроти проблема управління державним боргом набуває в умовах економічних криз, глобальних фінансових потрясінь, пандемій і воєнних дій, коли держава змушена активно залучати внутрішні та зовнішні запозичення для фінансування бюджетного дефіциту та підтримки економіки.

За таких умов актуалізується потреба не лише в оцінюванні поточного обсягу державного боргу, а й у прогнозуванні його динаміки з урахуванням ключових макроекономічних чинників. Саме математичне моделювання дає змогу формалізувати складні взаємозв'язки між державним боргом, темпами економічного зростання, процентними ставками, рівнем інфляції, валютним курсом і параметрами бюджетної політики. Використання моделей дозволяє ідентифікувати критичні умови, за яких борг може набути нестійкого або вибухового характеру, а також оцінити наслідки альтернативних сценаріїв фіскальної та боргової політики.

Сучасні наукові дослідження у сфері державних фінансів дедалі частіше зосереджуються на розробці моделей, здатних відображати як короткострокову динаміку боргових показників, так і довгострокові наслідки бюджетних рішень. Зокрема, у вітчизняних дослідженнях активно застосовується системно-динамічний підхід, який дає змогу моделювати взаємодію державного боргу з ключовими макроекономічними змінними у довгостроковій перспективі та оцінювати наслідки структурних змін економіки [1]. Такий підхід є особливо актуальним для країн із підвищеним рівнем невизначеності економічного розвитку.

Глобальна економіка нині характеризується високим рівнем боргового навантаження, що створює значні виклики для фінансової стабільності. За оцінками аналітиків Міжнародного валютного фонду, до кінця 2025 року сукупний борг усіх країн світу досягне 95,1% від обсягу світового ВВП, а до завершення десятиліття цей показник може зрости до 99,6%. Для порівняння, у 2020 році, під час пандемічної кризи, рівень глобального боргу становив 98,9% ВВП, що свідчить про поступове повернення до критичних меж [2].

Зростання державного боргу зумовлюється уповільненням економічного зростання, посиленням геополітичної напруги, нестабільністю фінансових ринків і підвищенням процентних ставок. За таких умов особливо важливим є використання кількісних методів аналізу, які дозволяють оцінювати вплив окремих макроекономічних чинників на боргову динаміку. Економетричні моделі, зокрема моделі векторної авторегресії, широко застосовуються для дослідження взаємозалежності між державним боргом, темпами зростання ВВП та бюджетним дефіцитом [3].

Базою більшості моделей динаміки державного боргу є бюджетне обмеження держави, яке описує зміну обсягу боргових зобов'язань залежно від первинного бюджетного дефіциту, процентної ставки за запозиченнями та темпів економічного зростання. У межах аналітичних підходів ця залежність формалізується за допомогою різницевих або диференціальних рівнянь, що дозволяє визначити умови стабілізації боргу відносно валового внутрішнього продукту. Подібні динамічні моделі

демонструють, що боргова стійкість досягається за умови, коли темпи економічного зростання не є нижчими за ефективну процентну ставку обслуговування боргу [4].

Поряд з аналітичними моделями дедалі більшого поширення набувають економіко-математичні моделі оптимізації обсягу та структури державного боргу. Вони дозволяють оцінювати доцільність різних варіантів співвідношення внутрішніх і зовнішніх запозичень, а також вплив строкової структури боргу на загальний рівень боргового навантаження [5]. Такі моделі є важливим інструментом формування ефективної боргової політики, оскільки дають змогу мінімізувати ризики та витрати на обслуговування боргу в середньо- та довгостроковій перспективі.

Для адекватного моделювання динаміки державного боргу необхідно враховувати низку макроекономічних параметрів, серед яких ключовими є темпи зростання валового внутрішнього продукту, середня процентна ставка за борговими зобов'язаннями, рівень інфляції та обсяг первинного бюджетного дефіциту. Прискорення економічного зростання, як правило, сприяє зменшенню боргового навантаження відносно ВВП, тоді як високі процентні ставки та тривалий дефіцит бюджету призводять до його зростання. У цьому контексті використання системно-динамічних та економетричних моделей дозволяє комплексно оцінювати можливі траєкторії боргу та ризики втрати боргової стійкості [1, 3].

Отже, сучасні підходи до моделювання динаміки державного боргу є важливим інструментом аналізу та прогнозування боргових процесів у складних і нестабільних економічних умовах. Поєднання аналітичних, чисельних і стохастичних моделей дозволяє комплексно оцінювати боргову стійкість, визначати потенційні ризики та формувати ефективні стратегії управління державними фінансами. Подальший розвиток математичних моделей з урахуванням національної специфіки та глобальних викликів є необхідною передумовою забезпечення фінансової стабільності та сталого економічного розвитку.

Література

1. Григор'єв Г. С. Державний борг і післявоєнне економічне зростання України: системно-динамічний підхід. Наукові записки НаУКМА. Економічні науки. № 8(1), 32–39. https://doi.org/ 10.18523/2519-4739.2023.8.1.32-39
2. Світовий державний борг наблизиться до 100% до 2030 року – МВФ. https://weukraine.tv/ekonomika/svitovij-derzhavnij-borh-nablizitsja-do-100-do-2030-roku-mvf/
3. Пілько А., Чепига Б. Моделі аналізу взаємозв'язків між макроекономічними показниками та показниками державного боргу. Економіка та суспільство. 2022. №45. https://doi.org/10.32782/ 2524-0072/2022-45-60
4. Di Guilmi C., Gallegati M., Landini S. Public debt dynamics: the interaction with national income and fiscal policy. Journal of Economic Structures. 2021. https://link.springer.com/article/10.1186/s40008-021-00238-4
5. Коляда О. В., Кірієнко Д. В. Моделювання оптимізації обсягу та структури державного боргу України в умовах євроінтеграції. Міжнародний науковий журнал «Інтернаука». 2019. № 13 (75). С. 17–20.

Георгієш Владлен В'ячеславович

здобувач вищої освіти освітнього ступеня «бакалавр» спеціальності 126 Інформаційні системи та технології Львівського державного університету внутрішніх справ

Огірко Ольга Ігорівна

кандидат технічних наук, професор кафедри інформаційних технологій Львівського державного університету внутрішніх справ

ІНСТРУМЕНТИ ДЛЯ OSINT-РОЗСЛІДУВАНЬ

В умовах збройної агресії проти України, гібридних загроз та стрімкого розвитку цифрового інформаційного простору інформаційно-

аналітичне забезпечення діяльності органів сектору безпеки і оборони набуває ключового значення. Своєчасне отримання, обробка та інтерпретація інформації з відкритих джерел стають важливими чинниками прийняття управлінських рішень, протидії інформаційним операціям, виявлення загроз національній безпеці та забезпечення стійкості державних інституцій.

Open Source Intelligence (OSINT) як складова інформаційно-аналітичної діяльності дозволяє ефективно використовувати потенціал відкритого інформаційного середовища для моніторингу цифрової інфраструктури, аналізу соціально-мережевих взаємозв'язків, виявлення ознак кіберзагроз, витоків інформації та інших ризиків, що впливають на безпеку і обороноздатність держави. Використання сучасних OSINT-інструментів забезпечує інтеграцію технічного, аналітичного та візуалізаційного компонентів у межах єдиного інформаційно-аналітичного контуру.

Екосистема спеціалізованих OSINT-платформ представлена широким спектром онлайн-сервісів, які автоматизують та оптимізують процеси збору, структурування та аналізу інформації з відкритих джерел. Технологічна диверсифікація Як показано на рис. 1, сучасні OSINT-інструменти формують багаторівневу екосистему, що охоплює технічний, пошуковий та аналітичний рівні. [1].

Shodan позиціонується як пошукова система для Інтернету речей та промислових систем управління, індексуючи пристрої, підключені до мережі – від вебкамер, маршрутизаторів, серверів до промислових контролерів, медичного обладнання та систем «розумного» будинку. Технічна архітектура Shodan базується на систематичному скануванні IPv4 та IPv6-адресного простору з метою виявлення пристроїв, доступних через інтернет, та збору інформації про їхні сервіси, порти, банери, використовувані протоколи та версії програмного забезпечення [2].

Функціональність Shodan дозволяє виявляти вразливі або неналежно захищені пристрої через цілеспрямований пошук за конкретними портами, сервісами, географічною локацією, операційними системами або специфічними банерами сервісів. Дослідницькі можливості Shodan

розширюються через спеціалізовані фільтри – port: (для пошуку конкретних відкритих портів), os: (для фільтрації за операційною системою), country: (для географічної локалізації), hostname: (для пошуку за доменним ім'ям), org: (для пошуку за назвою організації), що дозволяє здійснювати точні запити для виявлення специфічних технічних вразливостей або конфігурацій [3].

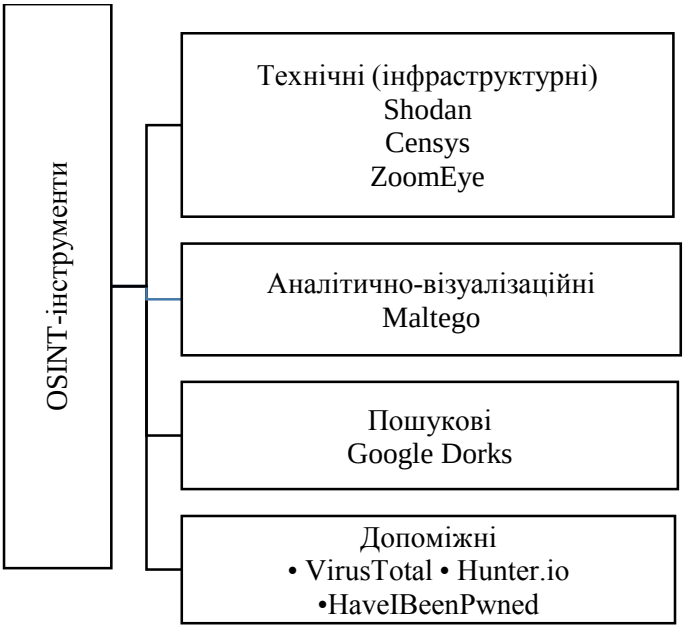

Рис. 1. Класифікація сучасних інструментів OSINT-розслідувань

Maltego представляє інтерактивну платформу для візуалізації взаємозв'язків та проведення мережевого аналізу, що дозволяє через графічний інтерфейс інтегрувати дані з різних джерел та візуалізувати складні взаємозв'язки між об'єктами розслідування. Концептуальною основою Maltego виступає теорія графів, де інформаційні сутності (домени, IP-адреси, електронні адреси, особи, організації, акаунти в соціальних мережах) представлені як вузли, а взаємозв'язки між ними – як ребра [4].

Архітектура Maltego побудована на концепції «трансформацій» – автоматизованих запитів до різних джерел даних, які перетворюють початкову інформацію (наприклад, домен) у пов'язані сутності (IP-адреси, електронні адреси, особи, організації тощо). Технологічна реалізація трансформацій відбувається через TDS (Transform Distribution Server), який забезпечує централізоване управління доступом до різних OSINT-джерел та стандартизацію форматів даних [5]. Система підтримує інтеграцію з численними OSINT-джерелами через API-трансформації, включаючи WHOIS-бази даних, соціальні мережі, пошукові системи, геолокаційні сервіси та спеціалізовані бази загроз. Функціональні можливості Maltego для OSINT-розслідувань включають автоматизований збір інформації з множинних джерел, виявлення прихованих зв'язків між різними типами даних, візуалізацію складних мережевих структур, проведення часових аналізів та генерацію аналітичних звітів [6]. Google Dorks (також відомі як Google Hacking Database) являють собою колекцію спеціалізованих пошукових запитів, які використовують розширений синтаксис Google для виявлення специфічної інформації, яка зазвичай залишається прихованою від стандартних пошукових методів. Методологічна сутність Google Dorks полягає у використанні комбінацій спеціальних операторів для обходу стандартних обмежень пошукових алгоритмів та отримання доступу до чутливої інформації, яка випадково або через неправильну конфігурацію стала доступною в інтернеті [7].

Censys та ZoomEye функціонують як спеціалізовані пошукові системи для інтернет-пристроїв та вебсервісів, надаючи детальну інформацію про цифрову інфраструктуру, сертифікати SSL/TLS, відкриті порти та конфігурації серверів. На відміну від Shodan, Censys фокусується на більш детальному аналізі вебсервісів, включаючи вичерпну інформацію про криптографічні протоколи, цифрові сертифікати та конфігурації безпеки. ZoomEye спеціалізується на розширеному аналізі веб-додатків, детально досліджуючи фреймворки, бібліотеки та компоненти, які використовуються на вебсайтах [8].

Hunter.io, Phonebook.cz, Email-Format спеціалізуються на виявленні корпоративних електронних адрес, дозволяючи ідентифікувати структуру іменування електронних скриньок організацій та знаходити контакти конкретних співробітників. Технологічний підхід цих сервісів базується на аналізі патернів електронних адрес у конкретних доменах, вилученні контактів з публічних джерел (сайти організацій, профілі в соціальних мережах, публікації) та агрегації доступної контактної інформації [9].

VirusTotal, незважаючи на первинну функцію антивірусної перевірки, становить цінний OSINT-інструмент завдяки агрегації інформації про домени, URL, IP-адреси та файли, включаючи історію їх виявлення, пов'язані індикатори компрометації та репутаційні метрики. Інтеграція даних від понад 70 антивірусних рушіїв, систем безпеки та аналітичних платформ робить VirusTotal унікальним ресурсом для дослідження потенційно шкідливих об'єктів та зв'язків між ними [10].

HaveIBeenPwned надає можливість перевірки електронних адрес на предмет витоку в результаті відомих порушень даних, що дозволяє встановити, чи були скомпрометовані облікові дані об'єкта розслідування. База даних сервісу містить інформацію про понад 10 мільярдів скомпрометованих облікових записів з більш ніж 500 різних витоків даних, що робить його цінним ресурсом для оцінки ризиків, пов'язаних з конкретними електронними адресами або доменами [11].

Проведений аналіз інструментів для OSINT-розслідувань свідчить про високий рівень розвитку сучасної екосистеми відкритої розвідки та її орієнтацію на комплексний підхід до збору й аналізу інформації. Розглянуті платформи демонструють різні методологічні підходи – від технічного сканування мережевої інфраструктури до соціально-мережевого аналізу та виявлення цифрових слідів користувачів і організацій.

Shodan, Censys і ZoomEye забезпечують глибоке дослідження інтернет-інфраструктури та дозволяють ідентифікувати вразливі або неправильно сконфігуровані пристрої й сервіси. Maltego виступає потужним аналітичним інструментом для виявлення прихованих взаємозв'язків між об'єктами розслідування шляхом графової візуалізації та автоматизованих трансформацій. Google Dorks, у свою чергу, залишаються

ефективним методом пошуку чутливої інформації, що стала доступною внаслідок людського фактору або помилок конфігурації.

Допоміжні сервіси, такі як Hunter.io, VirusTotal та HaveIBeenPwned, розширюють можливості OSINT-аналізу за рахунок роботи з контактними даними, індикаторами компрометації та витоками облікових записів. Їх використання у поєднанні з базовими OSINT-платформами дозволяє формувати цілісну картину інформаційного середовища об'єкта дослідження.

Таким чином, ефективність OSINT-розслідувань досягається не за рахунок використання окремого інструменту, а через інтеграцію різних сервісів у єдину аналітичну модель. Подальший розвиток OSINT-інструментарію пов'язаний з автоматизацією аналітичних процесів, застосуванням методів штучного інтелекту та розширенням можливостей міжплатформної інтеграції.

Література

1. Ісмайлов К., Пєфтієв Д. Розділ 16. Цифрові технології та аналітичні засоби аналізу воєнних злочинів в Україні. 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: «ВАЙТ», 2024. 504 с. С. 253–267.
2. Dincelli E., Van Slyke C., Yayla A. Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. Communications of the Association for Information Systems. 2023. Vol. 53, № 1. P. 1052–1071. DOI: 10.17705/1cais.05345.
3. The Current Epoch Unix Timestamp. URL: https://www.unixtimestamp.com/
4. How does OSINT affect the war in Ukraine? URL: https://itedu.center/ua/blog/articles/osint/

5. OSINT in Ukraine: how does it help the front during the war? URL: https://the-news.com.ua/single/osint-v-ukrayini-iak-dopomagaie-frontu-pid-chas-viini
6. Tools information struggle: OSINT, IPSO and opposition misinformation. URL: https://infolight.in.ua/wp-content/uploads/2023/02/brochure-2.pdf
7. How To Use The Threat Intelligence Cycle To Secure Your Brand? URL: https://www.groupsense.io/resources/how-to-use-the-intelligence-cycle-to-secure-your-brand
8. Intelligence from open sources (Open-source intelligence - OSINT). URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/
9. Sidorenko V. V. The Schuchart-Deming Cycle (Pdca) for the Organization of Continuing Professional Development of Specialists. VI International Scientific and Practical Conference «CONTINUOUS EDUCATION OF THE NEW CENTURY: ACHIEVEMENTS AND PROSPECTS». 2020.
10. What is OSINT (Open Source Intelligence)? URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/
11. OSINT, digital footprint and how to reduce it? URL: https://euprostir.org.ua/practices/133410

Германчук Юрій Іванович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ СПІВРОБІТНИЦТВА ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ З ІНСТИТУЦІЯМИ МІЖНАРОДНОГО ПРАВОПОРЯДКУ ЩОДО ВИКРИТТЯ ТРАНСНАЦІОНАЛЬНОЇ ЗЛОЧИННОСТІ

Сучасні виклики безпеки, зокрема посилення транснаціональної злочинності, потребують від Національної поліції України удосконалення інформаційно-аналітичного забезпечення співробітництва з міжнародними інституціями правопорядку. Це пояснюється необхідністю оперативного обміну розвідувальною інформацією, аналізу транскордонних зв'язків та фінансових потоків, що дозволяє своєчасно виявляти організовані злочинні мережі й запобігати їхній діяльності. Актуальність теми зумовлена поглибленням інтеграційних процесів України у світову систему безпеки та потребою адаптації національних механізмів протидії злочинності до міжнародних стандартів.

Під інформаційно-аналітичним забезпеченням слід розуміти комплекс заходів, спрямованих на збирання, обробку, аналіз, систематизацію й передачу інформації, що має оперативно-розшукове, розвідувальне або криміналістичне значення для протидії злочинності. Стаття 25 Закону України «Про Національну поліцію» визначає, що поліція має право створювати та використовувати інформаційні системи, проводити аналітичну діяльність для виконання завдань із захисту прав і свобод громадян, протидії злочинності та підтримання публічної безпеки [1].

Відповідно до цього, інформаційно-аналітична діяльність є одним із ключових напрямів оперативного співробітництва з міжнародними структурами.

Особливу роль у забезпеченні такого співробітництва відіграє Департамент міжнародного поліцейського співробітництва Національної поліції України, який координує взаємодію України з INTERPOL, Європолом та іншими правоохоронними структурами [2]. Угода між Україною та Європолом про оперативне та стратегічне співробітництво 2016 року заклала правові підстави для обміну аналітичною інформацією, використання захищеного каналу зв'язку SIENA та формування спільних аналітичних продуктів [3]. Це дозволяє українським оперативним підрозділам долучатися до міжнародних операцій, спрямованих на виявлення мереж, які займаються торгівлею людьми, зброєю, наркотиками чи здійснюють фінансові шахрайства.

У практичному контексті інформаційно-аналітичне забезпечення співробітництва реалізується через інтеграцію національних баз даних із системами INTERPOL, EUROPOL та FRONTEX. Так, у межах проєкту INTERPOL I-FORCE, започаткованого у 2023 році, українські правоохоронці отримали доступ до аналітичних ресурсів для виявлення каналів незаконного переміщення зброї та фінансування злочинних угруповань [4]. Європол, зі свого боку, здійснює аналітичну підтримку через платформу SOCTA, яка надає стратегічні оцінки стану організованої злочинності в ЄС і суміжних регіонах [5, с. 2-3].

Важливою складовою інформаційно-аналітичного забезпечення є використання методів кримінального аналізу – мережевого аналізу зв'язків, лінк-чартингу, аналізу фінансових транзакцій та відкритих джерел (OSINT). Ці методи дозволяють не лише виявляти структуру організованих злочинних груп, а й визначати їхні фінансові та логістичні канали, прогнозувати ризики злочинної діяльності. У цьому контексті набуває значення співпраця між підрозділами кіберполіції, аналітичними службами Міністерства внутрішніх справ та міжнародними центрами боротьби з кіберзлочинністю, оскільки значна частина транснаціональних злочинів сьогодні має цифровий вимір.

Підвищення ефективності інформаційно-аналітичної роботи потребує розвитку спільних стандартів обміну інформацією, уніфікації термінології, впровадження протоколів безпеки та дотримання вимог захисту персональних даних. Координаційні механізми співпраці – створення міжнародних спільних слідчих груп, Їх діяльність дає змогу подолати обмеження, пов'язані з процедурою надання міжнародної правової допомоги, та забезпечити більш тісну координацію зусиль у сфері збору доказів, проведення слідчих дій, обміну інформацією та забезпечення процесуальної присутності представників кількох держав у розслідуванні [6].

Варто наголосити, що сучасні тенденції транснаціональної злочинності характеризуються зрощенням кримінальних структур з економічними та політичними інтересами, використанням штучного інтелекту, криптовалют, а також мереж даркнету. У зв'язку з цим Європол та Рада ЄС у своїх аналітичних документах відзначають необхідність посилення обміну інформацією та розвитку аналітичних спроможностей держав-членів і партнерів, серед яких і Україна [7].

Підсумовуючи, інформаційно-аналітичне забезпечення співробітництва оперативних підрозділів Національної поліції України з міжнародними інституціями правопорядку є ключовим чинником у протидії транснаціональній злочинності. Його ефективність визначається рівнем інтеграції інформаційних систем, якістю аналітичної роботи, відповідністю міжнародним стандартам та здатністю правоохоронних органів швидко адаптуватися до нових загроз. Розвиток аналітичної інфраструктури, навчання працівників та розширення міжнародної взаємодії створюють умови для підвищення спроможності України у сфері забезпечення безпеки та верховенства права.

Література

1. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40–41. – Ст. 379.

2. Національна поліція України. Департамент міжнародного поліцейського співробітництва : офіц. сайт. – Режим доступу: https://www.npu.gov.ua (дата звернення: 23.10.2025).
3. Угода між Україною та Європолом про оперативне та стратегічне співробітництво від 14 груд. 2016 р. // Законодавство України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_016#Text (дата звернення: 23.10.2025).
4. INTERPOL. Project I-FORCE : Supporting law enforcement in response to threats arising from the war against Ukraine. – Режим доступу: https://www.interpol.int (дата звернення: 23.10.2025).
5. Europol. EU SOCTA 2025: European Union Serious and Organised Crime Threat Assessment. – The Hague, 2025.
6. Лук'янчук Ю. Л. Адміністративно-правові основи діяльності міжнародних спільних слідчих груп //Редакційна колегія. – 2025. – С. 154.
7. Reuters. Europol warns of AI-driven crime threats, 18 March 2025. – Режим доступу: https://www.reuters.com (дата звернення: 23.10.2025).

Гладій Дмитро Іванович,

здобувач вищої освіти освітнього ступеня «бакалавр» спеціальності «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Галайко Наталія Володимирівна,

старший викладач кафедри інформаційних технологій Львівського державного університету внутрішніх справ

ВИКЛИКИ ПРОТИДІЇ DEEPFAKE-ТЕХНОЛОГІЯМ У КРИМІНАЛЬНОМУ СУДОЧИНСТВІ

У сучасному світі стрімкий розвиток штучного інтелекту відкриває нові можливості для суспільства, водночас породжуючи низку серйозних загроз. Однією з найбільш дискусійних і потенційно небезпечних для

правоохоронної системи є технологія Deepfake, яка створює принципово нові інструменти маніпуляції цифровою реальністю.

Технологічний прорив у створенні реалістичного синтетичного контенту відбувся у 2014 році з появою алгоритмів машинного навчання, відомих як генеративні змагальні мережі (Generative Adversarial Networks, GAN). Даний тип архітектури нейронних мереж здатний генерувати нові дані, що відповідають вивченим шаблонам. Активне використання GAN дозволяє створювати високореалістичний аудіо- та відеоконтент, який без застосування спеціалізованого програмного забезпечення практично неможливо відрізнити від автентичного.

На сьогодні потенціал використання технології Deepfake ще не повною мірою усвідомлений ані суспільством загалом, ані представниками злочинного середовища. Це дає підстави стверджувати, що кількість та різновиди кримінальних правопорушень, пов'язаних із використанням Deepfake-технологій, у найближчій перспективі лише зростатимуть.

Однією з ключових тенденцій сучасної кіберзлочинності є поступовий перехід від викрадення даних до викрадення цифрової особистості. Традиційна кіберзлочинність тривалий час ґрунтувалася на незаконному доступі до конфіденційної інформації з метою прямого фінансового збагачення або шантажу. Натомість сучасні цифрові технології дозволяють не лише викрадати персональні дані, а й повністю імітувати присутність конкретної особи у цифровому просторі.

У результаті з'являються нові форми злочинної діяльності, зокрема:

1. Синтетична крадіжка ідентичності: шахраї створюють фальшиві особистості та відкривають нові кредитні рахунки, поєднуючи викрадену реальну ідентифікаційну інформацію з фальшивою; або використовуючи фальшиву інформацію, наприклад, вигаданих дітей – практика, яка називається «вирощуванням особистостей» (identity farming).

2. Компроментація робочої електронної пошти (Business Email Compromise, BEC): це складний вид кіберзлочинності, спрямований на компанії та приватних осіб, які здійснюють банківські перекази та мають доступ до конфіденційної фінансової інформації. На відміну від традиційних фішингових атак, BEC передбачає використання тактики соціальної інженерії, щоб обманом змусити жертв розкрити конфіденційну інформацію або здійснити несанкціоновані фінансові операції.
3. Маніпуляція свідченнями та дискредитація: у правоохоронній сфері це створює ризик появи «синтетичних свідків» або дискредитації реальних посадових осіб. Якщо можна підробити відео, на якому офіцер поліції наче приймає хабар, це руйнує довіру до всієї системи правосуддя.

У зв'язку з викладеним, правоохоронні органи об'єктивно потребують упровадження автоматизованих систем перевірки цифрового контенту за принципом «AI-vs-AI», оскільки традиційні методи візуальної або експертної оцінки вже не забезпечують належного рівня достовірності. Людське око більше не може виступати універсальним фільтром істинності в умовах стрімкого розвитку синтетичних медіа.

Ефективність таких систем зумовлена тим, що сучасні алгоритми створення дипфейків працюють на рівні мікротекстур шкіри, мікроміміки, рухів очей та акустичних характеристик голосу – тобто в площині, що перебуває поза межами чутливості людських органів чуття. Як наслідок, навіть експерти-криміналісти у значній частині випадків не здатні відрізнити дипфейк від автентичного відео під час звичайного перегляду. За таких умов створення спеціалізованого штучного інтелекту, орієнтованого на виявлення цифрових аномалій, фактично стає єдиним ефективним інструментом протидії деструктивному використанню ШІ.

Водночас упровадження подібних технологічних рішень має відбуватися з урахуванням фундаментальної ролі правоохоронної діяльності у сучасному суспільстві. Правоохоронні органи щоденно виконують функцію гаранта безпеки та справедливості, формуючи простір довіри, законності та правопорядку. У цьому контексті застосування автоматизованих систем аналізу контенту не може підміняти собою правову

оцінку, а має слугувати допоміжним інструментом для прийняття зважених рішень із дотриманням балансу між інтересами держави, суспільства та окремої особи.

Окремим викликом залишається транснаціональний характер використання дипфейк-технологій. Інструменти створення синтетичного контенту не мають територіальних обмежень, а сучасний кіберпростір фактично стирає державні кордони. Це суттєво ускладнює застосування традиційних правових механізмів, зокрема визначення юрисдикції, збору та допустимості цифрових доказів.

Кіберзлочини, пов'язані з дипфейками, часто мають багаторівневу географію: зловмисник може перебувати в одній державі, використовувати інфраструктуру іншої, тоді як наслідки правопорушення виникають у третій. За таких умов ефективне розслідування стає неможливим без налагодженої міжнародної взаємодії та уніфікованих підходів.

У зв'язку з цим актуалізується необхідність розвитку міжнародної співпраці правоохоронних органів, зокрема шляхом створення спільних протоколів автентифікації цифрового контенту, уніфікованих стандартів експертного аналізу та глобальних баз «цифрових відбитків» синтетичних медіа.

Таким чином, поширення технологій Deepfake суттєво трансформує сучасну кіберзлочинність і створює нові виклики для системи кримінального судочинства та правоохоронної діяльності. Протидія цим загрозам неможлива без поєднання технологічних і правових рішень, зокрема впровадження автоматизованих систем виявлення синтетичного контенту та розвитку міжнародної співпраці. Лише комплексний підхід здатний забезпечити довіру до цифрових доказів, належний захист прав людини та ефективне функціонування правосуддя в умовах цифрової трансформації.

Література

1. Штучний інтелект у правоохоронній практиці: ризики та юридичні межі. Юридична Газета. URL: [https://yur-gazeta.com/dumka-

eksperta/shtuchniy-intelekt-u-pravoohoronniy-praktici-riziki-ta-yuridichni-mezhi.html] (дата звернення: 19.12.2025).
2. Що таке генеративно-змагальна мережа (GAN)? Unite.ai. URL: [https://www.unite.ai/uk/what-is-a-generative-adversarial-network-gan/] (дата звернення: 19.12.2025).
3. Крадіжка синтетичної особистості (Synthetic Identity Theft). KnowledgeFlow. URL: [https://knowledgeflow.org/uk/ресурс/synthetic-identity-theft/] (дата звернення: 19.12.2025).
4. Business E-mail Compromise (BEC): як захистити бізнес від кібершахрайства. SPAN. URL: [https://www.span.eu/ua/інсайти/business-e-mail-compromise-ua/] (дата звернення: 19.12.2025).
5. Використання технологій штучного інтелекту у діяльності правоохоронних органів : аналітичний огляд / Харківський нац. ун-т внутр. справ. URL: [https://dspace.univd.edu.ua/server/api/core/bitstreams/f94ec02c-eb36-4adc-8cf5-c121c5580020/content] (дата звернення: 19.12.2025).
6. Правозастосування в кіберпросторі: виклики та перспективи. BCA Education. URL: [https://www.bca.education/pravozastosuvannya-v-kiberproctori/] (дата звернення: 19.12.2025).

Гладун Владислав В'ячеславович

курсант 1 курсу н.г СР-К9-25-1 ФПФПКП НПУ Дніпровського державного університету внутрішніх справ

Рижков Едуард Володимирович

професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В АНАЛІЗІ ОПЕРАТИВНО-РОЗШУКОВОЇ ІНФОРМАЦІЇ

Роль штучного інтелекту (ШІ) в аналізі оперативно-розшукової інформації стрімко зростає, оскільки сучасні правоохоронні органи

працюють із величезними масивами даних: відеозаписи, інформація з відкритих джерел, цифрові сліди, оперативні повідомлення, бази даних правопорушників та інші відомості, що потребують швидкої та точної обробки. Використання ШІ дозволяє автоматизувати рутинні процеси, виявляти приховані зв'язки, аналізувати складні інформаційні потоки та отримувати висновки, які були б неможливими при звичайному ручному аналізі. Теоретичне підґрунтя сучасних інформаційних технологій, що охоплює структуру, принципи зберігання та обробки даних, наведене у навчальному посібнику «Інформаційні та комунікаційні технології», який формує базу знань для розуміння можливостей застосування інтелектуальних систем у роботі поліцейських підрозділів [1].

Штучний інтелект активно використовується для вирішення завдань, пов'язаних з обробкою великих обсягів оперативно-розшукової інформації. Такі завдання включають: автоматичну ідентифікацію облич на фото та відео, біометричну верифікацію особи, аналіз відеопотоків у режимі реального часу, виявлення аномальної поведінки, виявлення кримінальних патернів, аналіз соціальних зв'язків, оцінку ризику вчинення злочину та визначення «гарячих точок» злочинності. За даними The Policing Project, найчастіше використовувані інструменти ШІ у правоохоронній діяльності — це системи відеоаналітики, інструменти розпізнавання осіб і програмні платформи для прогнозування злочинності [2]. Такі системи здатні обробити за хвилини той обсяг даних, який аналітичні підрозділи традиційно опрацьовують годинами або навіть днями.

Наукові дослідження у сфері безпеки також підтверджують ефективність використання ШІ у підвищенні якості аналізу оперативної інформації. Зокрема, у дослідженні Львівського державного університету внутрішніх справ наголошується, що системи штучного інтелекту можуть виявляти приховані залежності між подіями та суб'єктами, прогнозувати можливі сценарії розвитку ситуацій та формувати нові аналітичні моделі для розшукової діяльності [3]. Це дозволяє підвищити точність оцінки оперативної обстановки, своєчасно виявляти загрози та мінімізувати ризики для працівників поліції.

Окреме значення ШІ має в контексті прогнозної аналітики. Завдяки машинному навчанню система може аналізувати історичні дані та визначати райони, де існує підвищена ймовірність вчинення злочинів. Це дозволяє раціональніше планувати розстановку нарядів, оптимізувати маршрути патрулювання та підвищувати результативність превентивних заходів. Компанія SmartDev у своїх технічних оглядах відзначає, що алгоритми прогнозної аналітики на основі ШІ здатні враховувати десятки параметрів одночасно, включаючи час доби, сезонність, поведінкові патерни та соціально-економічні показники [4].

Штучний інтелект також відіграє важливу роль під час автоматизації процесів розпізнавання та класифікації інформації. Платформи штучного інтелекту, представлені у дослідженнях на ResearchGate, демонструють здатність до глибокого аналізу текстових даних: автоматичного розпізнавання ключових слів, визначення тематичних кластерів, аналізу емоційного забарвлення текстів, виявлення прихованих зв'язків між об'єктами аналізу [5]. У діяльності оперативних підрозділів це дозволяє значно підвищити швидкість обробки інформації, пришвидшити пошук релевантних матеріалів та оптимізувати процес прийняття рішень.

Іншою важливою сферою застосування ШІ є автоматизація аналітичних завдань у комплексних базах даних. У звітах компанії (Shanghai Automotive Industry Corporation) підкреслюється, що сучасні ШІ-системи здатні інтегрувати інформацію з різних джерел — відеоспостереження, баз даних, мобільних пристроїв, інтернет-ресурсів — та формувати єдину аналітичну модель ситуації, що значно підвищує оперативність і точність реагування [6]. Подібні підходи дають змогу своєчасно виявляти підозрілу активність, встановлювати осіб, причетних до злочинів, та формувати аналітичні портрети правопорушників.

Разом із тим, використання ШІ супроводжується вимогами щодо етичності, правової відповідності та захисту персональних даних. Під час роботи з аналітичними системами необхідно враховувати можливі ризики помилкової ідентифікації, викривленості даних, впливу алгоритмічних помилок. Тому технології штучного інтелекту повинні бути лише інструментами, що допомагають спеціалістам, а не замінюють їх. Кінцеве

рішення в оперативно-розшуковій діяльності має залишатися за людиною, яка несе відповідальність за інтерпретацію даних, отриманих із систем штучного інтелекту [7].

Таким чином, роль штучного інтелекту в аналізі оперативно-розшукової інформації є визначальною у сучасних умовах. Використання інтелектуальних систем сприяє підвищенню швидкості та точності обробки інформації, поліпшенню прогнозування, оптимізації ресурсів та підвищенню рівня безпеки. Наукові дослідження та практичний досвід правоохоронних органів світу демонструють, що ШІ стає потужним інструментом у боротьбі зі злочинністю, а подальший розвиток цієї технології визначатиме ефективність роботи аналітичних і оперативних підрозділів.

Література

1. Інформаційні та комунікаційні технології: навч. посібник / О.А. Дісковський, Ю.П. Синиціна, С.О. Прокопов, Е.В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2025. – 263 с. URL: https://osvita.dduvs.edu.ua/md/pluginfile.php/233305/mod_resource/content/3/%D0%9D%D0%9F %D0%86%D0%9A%D0%A2%2C2025 %D0%B4%D0%BE%D1%80%D0%BE%D0%B1.pdf
2. How Policing Agencies Use AI. The Policing Project, 2024. URL: https://www.policingproject.org/ai-explained-articles/2024/9/6/how-policing-agencies-use-ai дата звернення – 01.12.2025.
3. Zachek O., Dmytryk Y., Senyk V. «Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності». Науковий вісник ЛьвДУВС, 2023. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5945/1/19.pdf дата звернення – 01.12.2025.
4. SmartDev. AI Use Cases in Law Enforcement: Predictive Policing and Crime Forecasting, 2025. URL: https://smartdev.com/ai-use-cases-in-law-enforcement/ дата звернення – 01.12.2025.
5. The Role of Artificial Intelligence in Criminal Justice. ResearchGate, 2025.

6. SAIC. Law Enforcement on the AI Frontier: Seizing the Potential, 2025. URL: https://www.saic.com/perspectives/data-and-ai/law-enforcement-on-the-AI-frontier дата звернення – 01.12.2025.
7. PoliceChief Magazine. Rise of High-Tech Policing, 2025. URL: https://www.policechiefmagazine.org/rise-high-tech-policing/ дата звернення – 01.12.2025.

Годовна Карина Сергіївна,

студентка ННІ № 5 Харківського національного університету внутрішніх справ

Гуртова Ксенія Миколаївна,

доктор філософії права, старша викладачка кафедри конституційного і міжнародного права та прав людини Харківського національного університету внутрішніх справ

МІЖНАРОДНІ ВИМОГИ ДО ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ДЛЯ СЕКТОРУ БЕЗПЕКИ

Кібербезпека, як важлива складова протидії глобальним загрозам отримує все більшу підтримку урядів різних країн як в національних стратегіях безпеки, так і в міждержавних угодах та міжнародних документах — конвенціях та модельних документах ООН. Критичні вразливості інформаційної інфраструктури (кіберпростору) різних країн та неспроможність самостійно розв'язати весь комплекс проблем, що виникають при цьому, обумовлюють необхідність об'єднання їх зусиль, у тому числі, шляхом розбудови колективної системи кібер-безпеки [1].

Минулого року Україна визначилась із проєвропейським курсом та курсом на вступ у НАТО. Ці напрями Україна закріпила в основному документі країниКонституції України. Таким чином, з усіх міжнародних зобов'язань щодо забезпечення кібербезпеки, пріоритетними для співпраці було встановлено курс на євроінтеграцію та вступ до НАТО. За результатами більш глибокого аналізу законодавства Європейського

Союзу у сфері кібербезпеки можна дійти висновку, що інституції та політики ЄС не розглядають окремо заходи з кібербезпеки від заходів захисту конфіденційності мереж та/або інформаційних систем, а мають на меті узгоджені дії щодо захисту засобів, інформації та конфіденційності як частини екосистеми кібербезпеки та довіри [1].

Зазначимо, що сьогодні на порядку денному країн Європейського Союзу теж значної актуальності набуває питання щодо наявності «кваліфікованої робочої сили європейського співтовариства». Так у Стратегії Кібербезпеки Європейського Союзу на цифрове десятиліття, оприлюдненої для світової спільноти шляхом спільного повідомлення Європейського Парламенту та ради зазначено, що зусилля країн Європейського Союзу щодо підвищення кваліфікації робочої сили, розвитку, залучення, збереження найкращих талантів у галузі кібербезпеки та інвестування у дослідження й інновації світового класу становлять важливий компонент загального захисту від кіберзагроз. Це галузь із величезним потенціалом. Отже, особлива увага повинна бути приділена розвитку, залученню та збереженню різноманітних талантів у вказаній сфері. Переглянутий План дій щодо цифрової освіти підвищить рівень обізнаності щодо кібербезпеки серед людей, особливо дітей та молоді та організацій. Це також сприятиме участі жінок у таких сферах як наука, технології, техніка та математика (STEM) та підвищенню кваліфікації та перекваліфікації робочих місць в ІКТ у галузі цифрових навичок. Крім того, Комісія спільно з Управлінням інтелектуальної власності Європейського Союзу (ENISA), державами-членами та приватним сектором розроблятиме інструменти підвищення обізнаності та настанви для підвищення стійкості підприємств ЄС проти крадіжок інтелектуальної власності, що здійснюються за допомогою кіберінструментів. Освіта, зокрема професійна освіта та професійно-технічна підготовка, обізнаність та навчання, також повинна підвищувати кібербезпеку та навички кіберзахисту в європейських країнах. Із цією метою відповідні актори ЄС, такі як ENISA, Європейське оборонне агентство (EDA), європейський коледж безпеки та оборони (ESDC) повинні віднайти різноманітні способи досягнення синергії у власній діяльності у напрямі співпраці [2].

Специфіка сектору безпеки (правоохоронних та оборонних структур) вимагає додаткових компетенцій. Наприклад, у системі МВС України підготовка кіберполіцейських передбачає одночасне оволодіння кількома напрямами: «Кібербезпека», «Право» та «Правоохоронна діяльність». Фахівці повинні поєднувати технічні вміння (аналіз мереж, захист систем) із розумінням юридичних аспектів (законодавство з кіберзлочинності). Більше того, як зауважують українські дослідники, інтеграція в європейський простір вимагає переносу європейського досвіду освіти правоохоронців, зокрема у сфері кіберпідготовки [3].

Визнані міжнародні стандарти кібербезпеки визначають ключові компетенції фахівця. Так, Європейська рамка компетентностей із кібербезпеки (ECSF) виділяє основні профілі фахівців (наприклад, розробник рішень з кібербезпеки, аналітик інцидентів, криптограф тощо) і задає перелік їхніх знань, навичок та завдань. Ці профілі узгоджені з рекомендаціями ENISA та міжнародними підходами, що враховують як технічні, так і організаційні аспекти захисту [4].

Література

1. Олексюк Л. Правова база кібербезпеки в Україні: загальний огляд і аналіз. Друге видання. Київ: Міжнародна фундація виборчих систем (IFES), 2021. URL: https://ifesukraine.org/wp-content/uploads/2021/04/IFES-Ukraine-Cybersecurity-Legal-Framework-Overview-2020-v2-2021-04-01-Ukr.pdf
2. Євсюкова О. В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. Державне управління та місцеве самоврядування. 2021. URL: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf
3. Денищук Д.Є. Особливості підготовки поліцейських кіберполіції в умовах сьогодення (на прикладі ХНУВС) // Підготовка поліцейських в умовах реформування системи МВС України : матеріали наук.-практ. Конф., 29 трав. 2020 р., Харків. – Х. : Право, 2020. – С. 233–238.
4. Європейська рамка компетентностей із кібербезпеки (ECSF): Проєкт v0.5. – К. : Агентство ЄС з кібербезпеки, 2022. – 26 с.

Горохова Олександра Андріївна

студентка ННІ № 5 Харківського національного університету внутрішніх справ

Гуртова Ксенія Миколаївна

доктор філософії права, старша викладачка кафедри конституційного і міжнародного права та прав людини Харківського національного університету внутрішніх справ

МІЖНАРОДНІ СТАНДАРТИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНО-ПОЛІТИЧНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Інформаційно-аналітична діяльність Національної поліції України будується на фундаменті міжнародних стандартів, що визначають правила збору, обробки, захисту та використання даних у правоохоронній сфері. У сучасних умовах цифровізації правоохоронні органи працюють із великим масивом інформації — від оперативних даних і відеоспостереження до міжнародних баз розшуку. Це потребує чіткої відповідності міжнародним правовим нормам, що гарантують правомірність застосування інформаційних технологій та захист прав людини.

Одним із головних базових документів є Конвенція Ради Європи, яка зобов'язує держави забезпечувати законність, пропорційність, мінімізацію персональних даних та обов'язковість контролю за їх обробкою [1]. Для Національної поліції ці стандарти є основою при створенні та модернізації інформаційно-аналітичних систем (ІАС), які використовуються для оперативного реагування та кримінального аналізу.

Важливе значення також має Загальний регламент ЄС про захист даних (GDPR), що встановлює найвищі міжнародні вимоги до прозорості, підзвітності, фіксації згоди суб'єктів, аудиту інформаційних систем та впровадження механізмів кіберзахисту [2]. Хоча Україна формально не є членом ЄС, Національна поліція орієнтується на ці стандарти в межах євроінтеграції та виконання Угоди про асоціацію.

У сфері професійної поліцейської діяльності ключове значення має Кодекс поведінки посадових осіб з підтримання правопорядку ООН, що встановлює принципи недопущення зловживань під час збору інформації, а також гарантує, що аналітичні дані не можуть бути використані для порушення прав людини [3]. Це важливо у контексті застосування технологій розпізнавання облич, автоматизованих систем відеоаналітики та обробки даних із телекомунікаційних мереж.

Вагому роль відіграють стандарти міжнародного правоохоронного співробітництва — насамперед Правила обробки даних Інтерполу (RPD) [4]. Україна як член Інтерполу зобов'язана дотримуватися високих вимог до безпеки інформації, уникати втручання третіх держав та гарантувати цілісність даних, що надходять з-понад 190 країн.

Для підвищення ефективності кримінального аналізу Нацполіція також орієнтується на Стандарти Європолу щодо управління інформацією та кримінального аналізу, які включають рекомендації з ризик-менеджменту, обміну розвідувальною інформацією та використання кримінальних профілів [6].

Науковці О. В. Джафарова, В. Ю. Абросімов та інші підкреслюють, що імплементація міжнародних стандартів дозволяє Україні формувати сучасну модель кримінального аналізу, підвищувати якість прийняття управлінських рішень та інтегруватися у європейський безпековий простір [5]. Це особливо важливо в умовах воєнної агресії, коли інформаційна складова набуває стратегічного значення.

Водночас існують і виклики. По-перше, технічна інфраструктура потребує модернізації — багато систем створювалися до активної цифровізації та не відповідають усім вимогам Конвенції 108+ чи GDPR. По-друге, необхідна глибока підготовка персоналу у сфері кібербезпеки, роботи з великими даними та міжнародних правил захисту інформації. По-третє, законодавство України досі потребує вдосконалення, зокрема щодо незалежного контролю за діяльністю поліції та механізмів аудиту інформаційних систем.

Однак поступове впровадження міжнародних стандартів відкриває нові можливості: інтеграцію до європейських та світових інформаційних платформ, підвищення довіри громадян, зміцнення правових гарантій, а також підвищення ефективності протидії злочинності шляхом використання сучасних цифрових технологій.

Література

1. Council of Europe. Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data. URL: https://www.coe.int/en/web/data-protection/convention108-plus
2. European Union. General Data Protection Regulation (GDPR), 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
3. United Nations. Code of Conduct for Law Enforcement Officials, 1979. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials
4. Interpol. Rules on the Processing of Data (RPD). URL: https://www.interpol.int/en/Who-we-are/Legal-framework/Rules-on-the-Processing-of-Data
5. Джафарова О. В., Абросімов В. Ю. Інформаційно-аналітична діяльність поліції: міжнародні стандарти та практики. Науковий вісник Національної академії внутрішніх справ, 2021. URL: https://visnyk.naiau.kiev.ua
6. Europol. Information Management and Analysis Standards. URL: https://www.europol.europa.eu
7. UNODC. Handbook on Police Accountability, Oversight and Integrity. URL: https://www.unodc.org

Гранківська Софія Романівна

курсант факультету №2 Львівського державного університету внутрішніх справ

Мусійовська Мар'яна Михайлівна

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ З МЕТОЮ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Стрімка цифровізація та зростання залежності суспільства від електронних комунікацій зумовили появу нових кіберзагроз. В умовах воєнного стану кібератаки стали складовою гібридної війни та спрямовані на ураження державних інформаційних систем, об'єктів критичної інфраструктури й дестабілізацію суспільних процесів [1].

За таких умов оперативно-розшукова діяльність кримінальної поліції набуває особливого значення, оскільки забезпечує своєчасне виявлення та припинення кіберзлочинів, встановлення причетних осіб і документування протиправної діяльності. Ефективність цих заходів безпосередньо впливає на рівень кібербезпеки держави [4].

Оперативно-розшукова діяльність є важливим інструментом держави у боротьбі зі злочинністю, зокрема у сфері кібербезпеки. Стрімкий розвиток цифрових технологій і зростання кіберзагроз зумовлюють необхідність адаптації традиційних методів оперативної роботи до умов кіберпростору. До ключових понять теми належать: кібербезпека, кіберзлочин, оперативно-розшукові заходи, цифрові сліди, інформаційна та критична інформаційна інфраструктура, телекомунікаційні мережі. Кібербезпека розуміється як стан захищеності життєво важливих

інтересів особи, суспільства і держави від кіберзагроз. В умовах воєнного стану вона охоплює не лише технічний захист інформаційних ресурсів, а й протидію інформаційно-психологічним операціям, кібердиверсіям та атакам на стратегічні об'єкти.

Правове регулювання оперативно-розшукової діяльності у сфері кібербезпеки здійснюється на основі законів України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про основні засади забезпечення кібербезпеки України», Кримінального процесуального кодексу України, а також міжнародних стандартів, зокрема Будапештської конвенції про кіберзлочинність. Нормативна база визначає види оперативно-розшукових заходів, порядок їх застосування та гарантії дотримання прав людини.

Забезпечення кібербезпеки має комплексний характер і поєднує технічні, організаційні та правові заходи. Особливу роль у цьому механізмі відіграє оперативно-розшукова діяльність, яка спрямована на раннє виявлення кіберзлочинів, документування протиправних дій у цифровому середовищі, встановлення осіб злочинців, протидію діяльності хакерських угруповань і міжнародних кіберзлочинних схем. У період воєнного стану кіберзагрози набувають більш складного та системного характеру. Зростає кількість атак на об'єкти критичної інформаційної інфраструктури, застосовується шкідливе програмне забезпечення військового рівня, активно використовується анонімізація через VPN, Tor та криптографічні інструменти, що суттєво ускладнює проведення оперативно-розшукових заходів. [2] Оперативні підрозділи кримінальної поліції здійснюють негласні слідчі дії, моніторинг телекомунікаційних мереж, аналіз цифрових слідів, технічні експертизи, виявлення шкідливого програмного забезпечення, документування кіберзлочинів та взаємодіють з міжнародними організаціями, зокрема Europol і Interpol [4].

Водночас проблемними залишаються питання матеріально-технічного забезпечення, доступу до сучасних програмних рішень і технологій штучного інтелекту, а також ефективної міжвідомчої взаємодії між Національною поліцією, СБУ, Держспецзв'язку та іншими суб'єктами забезпечення кібербезпеки.

З метою підвищення ефективності оперативно-розшукової діяльності кримінальної поліції в умовах зростання кіберзагроз необхідне комплексне вдосконалення нормативного, організаційного та технічного забезпечення. Доцільним є уточнення правових процедур застосування оперативно-розшукових заходів у цифровому середовищі та розширення доступу до даних суб'єктів цифрової інфраструктури із забезпеченням належного контролю за дотриманням прав людини.

Важливим напрямом є посилення технічного оснащення підрозділів кримінальної поліції сучасними засобами цифрової форензики, кібермоніторингу, захищеними каналами зв'язку та аналітичними платформами. Не менш значущим є підвищення рівня професійної підготовки кадрів, зокрема у сфері комп'ютерних мереж, криптографії та аналізу цифрових даних [6].

Ефективна протидія кіберзагрозам також потребує посилення міжвідомчої та міжнародної взаємодії, а також створення єдиної аналітичної платформи для аналізу кіберінцидентів і прогнозування нових загроз. Загалом удосконалення оперативно-розшукової діяльності має ґрунтуватися на поєднанні сучасних технологій, міжнародного досвіду та професійної підготовки кадрів з метою забезпечення кібербезпеки та національної стійкості в умовах воєнного стану [3] .

У ході дослідження встановлено, що забезпечення кібербезпеки на об'єктах інформаційної діяльності в умовах воєнного стану є одним із пріоритетних напрямів діяльності держави. Кіберпростір перетворився на повноцінне поле протистояння, у якому противник здійснює вплив на державні процеси та об'єкти критичної інфраструктури, що зумовлює зростання ролі оперативно-розшукової діяльності кримінальної поліції. Нормативно-правове регулювання оперативно-розшукової діяльності загалом сформоване, проте потребує подальшого оновлення та адаптації до сучасних умов інформаційної війни, зокрема в частині доступу до цифрових даних, роботи з електронними доказами та міжнародної взаємодії.

Аналіз практики засвідчив наявність позитивних результатів у діяльності підрозділів кримінальної поліції у сфері протидії кіберзлочинності, водночас зберігаються проблеми технічного забезпечення, кадрового потенціалу та складності міждержавного обміну інформацією.

Отже, підвищення ефективності оперативно-розшукової діяльності можливе лише за умови комплексного підходу, який передбачає удосконалення законодавства, модернізацію технічної бази, підготовку фахівців, посилення міжвідомчої та міжнародної співпраці. Оперативно-розшукова діяльність кримінальної поліції є ключовим інструментом забезпечення кібербезпеки України та має залишатися одним із пріоритетів державної політики в умовах воєнного стану.

Література

1. Титарчук Є. О., Мусійовька М. М., Фадеічев С. В. Моделювання ризиків у кібербезпеці критичних інфраструктур на основі машинного навчання. Вісник Херсонського національного технічного університету. 2025. № 4 (95)
2. Національна поліція України. Звіти про діяльність підрозділів кіберполіції (2022–2024). Онлайн-ресурс. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/
3. Лемешко О. В. Особливості боротьби з кіберзлочинністю в умовах воєнного стану. Юридична наука. 2023. №4. С. 112–121.
4. Титаренко О. М. Оперативно-розшукові заходи у протидії кіберзлочинам. Вісник Національної академії внутрішніх справ. 2022. №2.
5. Ярмиш Н. М., Грищук В. К. Оперативно-розшукова діяльність. навчальний посібник. Київ. Атіка. 2020.
6. Шевчук О. В. Забезпечення кібербезпеки: правові та організаційні аспекти. — Київ: НаУКМА, 2021.

Гриневич Катерина Іванівна

курсант факультету №1 Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

СУЧАСНІ ВИКЛИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ТА РОЛЬ АНАЛІТИЧНИХ ЦЕНТРІВ У ЇХ ПОДОЛАННІ

Інформаційна безпека є одним із ключових елементів національної безпеки України, особливо в умовах триваючої гібридної агресії. Сучасні виклики у цій сфері відзначаються високою динамічністю, складністю та багатогранністю, що вимагає комплексної та оперативної реакції держави.

Одним із найсерйозніших викликів є гібридні інформаційні операції, які включають поширення дезінформації, фейків та маніпулятивного контенту з метою впливу на суспільну думку, підриву довіри до органів влади та дестабілізації внутрішньополітичної ситуації. Значну небезпеку становлять і кібератаки, що спрямовані на державні системи, критичну інфраструктуру, військові об’єкти та комунікаційні мережі. Такі атаки можуть призвести до витоку даних, блокування роботи органів державної влади та паралічу важливих сервісів [1, С. 210].

Окремою проблемою є вразливість критичної інформаційної інфраструктури, яка часто потребує модернізації, посилення захисту та вдосконалення систем реагування на інциденти. Поширеною залишається і проблема низької цифрової грамотності частини населення, що сприяє легкому поширенню маніпуляцій та впливу ворожої пропаганди.

Аналітичні центри в Україні виконують низку практичних функцій, які безпосередньо впливають на стан інформаційної безпеки. Передусім

вони здійснюють моніторинг інформаційного простору, фіксують діяльність російських пропагандистських ресурсів, Telegram-каналів, ботмереж і платформ, через які поширюється дезінформація. Наприклад, такі центри регулярно відстежують наративи про «втому Заходу», «нелегітимність влади» чи «неефективність оборони», які поширюють іноземні інформаційні мережі.

Другою важливою функцією є аналіз ворожих інформаційних операцій. Аналітичні групи відпрацьовують зв'язки між джерелами, визначають ключові канали поширення, часові піки активності та мету кожної кампанії. На основі цих даних вони готують докладні звіти та передають їх державним установам, що дозволяє оперативно реагувати на загрози.

По-третє, аналітичні центри формують рекомендації для органів державної влади. Напрацьовані висновки використовують міністерства, відомства та підрозділи сектору оборони для коригування комунікаційної політики, проведення інформаційних роз'яснень або блокування шкідливих ресурсів [2, С. 156].

Крім того, такі центри співпрацюють із міжнародними партнерами, зокрема з ЄС та США, передаючи дані про спроби втручання іноземних спецслужб у інформаційний простір. Деякі з них беруть участь у спільних програмах з кіберзахисту та протидії дезінформації, що дозволяє отримувати доступ до технічних засобів, методик OSINT-розвідки й аналітичних платформ.

Окремо аналітичні центри займаються навчанням фахівців, проводять тренінги з кібергігієни, аналізу інформаційних операцій та виявлення фейкових матеріалів для військових, держслужбовців і журналістів.

Проте, аналітичні центри в Україні стикаються з низкою практичних труднощів, які ускладнюють їхню повноцінну роботу у сфері інформаційної безпеки. Насамперед проблему становить обмежене фінансування. Багато центрів працюють переважно за рахунок грантових програм, які мають тимчасовий характер, що не дозволяє стабільно утримувати кваліфікованих аналітиків або інвестувати у технічні засоби моніторингу інформаційного простору [3].

Другою проблемою є недостатній обмін даними між державними та недержавними структурами. Частина інформації залишається закритою через формальні заборони чи бюрократичні обмеження. Це знижує точність аналітичних висновків, оскільки центри не отримують доступ до офіційних даних або оперативної інформації щодо кібератак і інформаційних операцій.

Проблеми виникають і в кадровому забезпеченні. В Україні обмежена кількість фахівців, здатних працювати з великими масивами даних, сучасними аналітичними платформами, інструментами OSINT чи системами виявлення бот-мереж. Через низьку оплату праці частина таких спеціалістів переходить у приватний сектор або працює на іноземні дослідницькі структури.

Складнощі спостерігаються також у сфері технічного забезпечення. Не всі аналітичні центри мають доступ до сучасних програм для аналізу соціальних мереж, систем відстеження кібератак або інструментів автоматизованого збору даних. Це зменшує оперативність і точність їхніх досліджень [4, С. 45–53].

Ще однією проблемою є низький рівень взаємодії з регіональними структурами. Більшість аналітичних центрів зосереджені у великих містах, зокрема у Києві, тоді як у регіонах бракує платформ, які могли б збирати інформацію про локальні прояви інформаційних операцій.

Крім того, аналітичні центри часто працюють в умовах правової невизначеності, оскільки законодавство не встановлює чітких процедур їхньої взаємодії з державними органами у сфері інформаційної безпеки, а частина рекомендацій залишається без практичного застосування.

У найближчі роки аналітична діяльність у сфері інформаційної безпеки може розвиватися за кількома чітко визначеними напрямами. Перший із них – впровадження інструментів штучного інтелекту та автоматизованих систем аналізу даних. Українські установи вже тестують програмні рішення для виявлення бот-мереж, автоматичного розпізнавання фейкових повідомлень і моніторингу інформаційних операцій у режимі реального часу. Використання таких систем дозволить

скоротити час на аналіз великих обсягів даних і покращити точність виявлення загроз.

Другий напрям – створення єдиної національної аналітичної платформи для обміну даними між державними структурами, аналітичними центрами та кіберпідрозділами. Її функціонування забезпечить доступ до оперативної інформації про кібератаки, пропагандистські кампанії та нові методи інформаційного впливу.

Третя перспектива стосується посилення міжнародної співпраці. Аналітичні центри України вже беруть участь у програмах ЄС та НАТО, що дозволяє отримувати доступ до аналітичних інструментів, методик оцінки інформаційних операцій і тренінгів для аналітиків. Розширення такої співпраці може забезпечити більш ефективні механізми реагування на транснаціональні загрози.

Четвертий напрям – професійна підготовка кадрів. В університетах та спеціалізованих навчальних центрах планується розширення програм з OSINT-розвідки, аналізу дезінформації, кібергігієни та інформаційних технологій захисту. Це має збільшити кількість фахівців, здатних працювати з сучасними аналітичними інструментами [5].

Також перспективним є формування регіональних аналітичних осередків, які збиратимуть дані про локальні інформаційні операції та взаємодіятимуть із місцевими органами влади. Це дозволить отримувати більш повну картину інформаційної обстановки в країні.

Окремим напрямом є модернізація технічної бази, зокрема закупівля програмних комплексів для аналізу соціальних мереж, моніторингу кіберінцидентів і виявлення координованої інформаційної активності [6, с .184].

У висновку перспективи розвитку аналітичної діяльності у сфері інформаційної безпеки України пов'язані з кількома ключовими напрямами. По-перше, планується створення єдиних національних цифрових платформ для збору, аналізу та моніторингу інформації, що забезпечить більш оперативне виявлення загроз. По-друге, підвищується рівень професійної підготовки аналітиків через спеціалізовані освітні програми і

тренінги з OSINT, кібербезпеки та data-аналізу. Використання технологій штучного інтелекту та обробки великих даних дозволить автоматизовано виявляти інформаційні операції та фейки. Значну роль відіграє посилення співпраці між державними установами та недержавними аналітичними центрами для обміну інформацією, спільних досліджень та вироблення практичних рекомендацій. Одночасно розвиваються механізми проактивного протидії інформаційним атакам та системи раннього попередження про загрози. Окрім цього, важливо розширювати міжнародне партнерство, зокрема участь у програмах НАТО та ЄС, обмін досвідом та аналітичними даними з міжнародними структурами, що підвищує ефективність захисту інформаційного простору України.

Література

1. Левченко, М.М. Виклики інформаційної безпеки та сучасні методи аналітичної діяльності. – Харків: ХНУ, 2021. – 210 с.
2. Яценко, І.В. Аналітичні центри як елемент національної системи кібербезпеки. – Київ: Науково-дослідний інститут безпеки, 2021. – 156 с.
3. Державний центр кіберзахисту (при Державна служба спеціального зв'язку та захисту інформації України). – URL: https://scpc.gov.ua/uk (дата звернення: 09.12.2025).
4. Кравчук, П.О. Протидія інформаційним загрозам у секторі оборони України. // Вісник Національної академії оборони України. – 2022. – № 3. – С. 45–53.
5. Закон України «Про основи національної безпеки України» від 21.06.2018 № 2469-VIII. – URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 09.12.2025).
6. Бондаренко, С.І. Інформаційна безпека України: сучасний стан та перспективи розвитку. – Київ: Наукова думка, 2021. – 184 с.

Д'яков Андрій Володимирович
доцент кафедри інформаційних технологій ЛьвДУВС кандидат технічних наук

СИСТЕМНІ ПІДХОДИ ДО ПРОТИДІЇ КІБЕРЗАГРОЗАМ ТА ДЕЗІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ У СЕКТОРІ БЕЗПЕКИ УКРАЇНИ

У контексті збройної агресії проти України та трансформації характеру воєнних дій інформаційна та кібербезпека постають ключовими векторами національної безпеки. Особливістю сучасного протистояння стало поєднання фізичних і віртуальних методів впливу, коли кіберпростір використовується як інструмент політичного, економічного та психологічного тиску. У відповідь на це Україна змушена модернізувати підходи до захисту власного інформаційного середовища, інфраструктури, військових систем управління, а також інформаційної свідомості громадян. Усе це вимагає системного аналізу, наукового обґрунтування та інтеграції міжнародного досвіду.

Поняття «кіберзагроза» в умовах гібридної війни набуває розширеного значення: це не лише хакерські атаки, але й деструктивний інформаційний вплив, злом систем управління, підміна даних, цілеспрямоване поширення фейків, використання «deep fake» технологій, створення та модифікація бот-мереж. Головною ознакою сучасних загроз є їхня скоординованість і багаторівневість. Вони здатні не лише порушити роботу окремих органів влади, але й викликати дестабілізацію в масштабах держави.

У відповідь на ці виклики виникає необхідність системного підходу до протидії кіберзагрозам. Це включає:

Технологічне зміцнення інформаційної інфраструктури. Застосування концепцій *Zero Trust*, принципів *кіберрезильєнтності,* шифрування з постквантовим захистом, використання SIEM-систем (наприклад, IBM QRadar, ArcSight), впровадження розподілених реєстрів (blockchain)

для збереження критично важливої інформації. Особливу роль відіграють алгоритми машинного навчання, здатні виявляти аномалії та атаки типу APT (Advanced Persistent Threat).

Міжвідомча координація. Сектор безпеки та оборони України об'єднує зусилля Міністерства оборони, СБУ, Держспецзв'язку, Державної служби спеціального зв'язку та захисту інформації. Необхідним є створення єдиної архітектури обміну даними з дотриманням стандартів ISO/IEC 27001 та NIST CSF, а також розробка протоколів швидкого реагування на кіберінциденти.

Протидія інформаційно-психологічним операціям (ІПсО). Використання OSINT-аналітики дозволяє виявляти інформаційні кампанії у відкритих джерелах, таких як соціальні мережі, Telegram, відеоплатформи, форуми. Поєднання аналітики великих даних з NLP (*Natural Language Processin*g) дає змогу ідентифікувати ботів, «мережі впливу», скоординовані фейкові наративи. Прикладом є українські стартапи *LetsData, InfoLight*, які співпрацюють з Центром стратегічних комунікацій при РНБО.

Розвиток національного програмного забезпечення. Зменшення залежності від іноземного програмного забезпечення, особливо з країнами ризику, та стимулювання розробки вітчизняних рішень у сфері кіберзахисту має стати одним із пріоритетів. Особливо у сфері SCADA-систем, захисту баз даних та систем автентифікації.

Підготовка фахівців. Важливою є системна підготовка офіцерів кібербезпеки, фахівців з цифрової розвідки та інформаційного аналізу. Зростає роль міждисциплінарної освіти: на перетині права, інформаційних технологій та психології. Необхідно розширювати CTF-платформи, вводити дуальну освіту, співпрацю з НАТО та ENISA.

Міжнародна інтеграція та обмін інформацією. Україна бере участь у міжнародних кіберкоаліціях, у тому числі в навчаннях Locked Shields, Cyber Europe, має меморандуми про співпрацю з CERT-структурами Естонії, Литви, Польщі. Надважливою є інтеграція до програм НАТО CCDCOE (Центр передового досвіду з кібероборони).

Правове регулювання та національні стратегії. Нормативна база вимагає перегляду та доповнення. Стратегія кібербезпеки України до 2025 року, прийнята у 2021 р., визначає пріоритети, але її імплементація стримується браком підзаконних актів, дублюванням функцій різних органів, недостатньою міжвідомчою взаємодією. Доцільно запровадити закон про інформаційний суверенітет, а також обов'язкову сертифікацію кіберзахисту для суб'єктів критичної інфраструктури.

Ці напрямки лише в сукупності можуть сформувати ефективну систему кібероборони, яка відповідатиме масштабам сучасних викликів. Ізоляційні або суто технократичні підходи є заздалегідь приреченими на неефективність. Потрібне поєднання високих технологій, суспільної свідомості, нормативного регулювання та кадрового забезпечення.

Сучасні атаки мають ознаки системної координації — це означає, що захист має бути системним. Саме тому ключовим поняттям стає *«кіберрезильєнтність»* — здатність інформаційної системи не лише захищатися, а й продовжувати функціонувати під час атак, швидко відновлюватися після збоїв, і головне — вчитися на виявлених загрозах.

Надзвичайно важливим є створення інституційної культури кібербезпеки в органах влади. Державні службовці повинні розуміти основи інформаційної безпеки, правила роботи з критичними даними, способи розпізнавання фішингових атак, основи кібергігієни. Це потребує запровадження обов'язкових навчань, сертифікації та ротації ІТ-спеціалістів.

Не менш важливим є створення державного механізму протидії дезінформації. Тут варто враховувати баланс між захистом національних інтересів та збереженням свободи слова. Доцільним є створення незалежного органу або омбудсмена з моніторингу інформаційних операцій, який діятиме в межах правової системи, а не адміністративного примусу.

Враховуючи досвід країн Балтії, можна запропонувати створення національної мережі «інформаційних референтів» — локальних експертів, які координуються державними структурами, але працюють із громадами, пояснюючи інформаційні ризики, проводячи інформаційні кампанії на рівні ОТГ.

У підсумку слід відзначити, що кіберзахист — це не лише технічне питання, а питання безпеки демократії, національної ідентичності та майбутнього держави. У добу цифрових конфліктів перемогу здобуває не той, хто більше атакує, а той, хто краще організований, здатен швидко реагувати та передбачати дії противника.

Джулай Максим Станіславович

курсант ФПФПКП НПУ Дніпровського державного університету внутрішніх справ

Рижков Едуард Володимирович

професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

РОЛЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Стрімкий розвиток інформаційно-комунікаційних технологій визначає нові підходи до організації діяльності Національної поліції України. Сучасна правоохоронна система потребує швидкої обробки інформації, ефективних каналів комунікації, доступу до державних реєстрів, аналітичних інструментів та високого рівня інформаційної безпеки. Інформаційно-комунікаційні технології (далі - ІКТ) є невід'ємною складовою професійної підготовки майбутніх поліцейських як практичних працівників [1, с. 39].

Одним із ключових напрямів використання ІКТ є застосування державних та єдиних реєстрів, що забезпечують доступ до офіційних відомостей про фізичних осіб, юридичних осіб, майно та документи. Ці автоматизовані системи створені для накопичення, перевірки, обробки та офіційного підтвердження даних, що є важливим для розкриття злочинів, ідентифікації осіб, перевірки документів, встановлення правового статусу суб'єктів та пошуку майна чи транспортних засобів. Значну роль у

підтримці таких реєстрів відіграє Державне підприємство «НАІС», яке забезпечує їх технічний супровід, захист персональних даних та доступ користувачів до інформаційних ресурсів. Воно відповідальне за адміністрування та розвиток важливих державних реєстрів України, зокрема: Державного реєстру речових прав на нерухоме майно (ДРРП), Автоматизованої системи виконавчого провадження (АСВП) та Державного реєстру обтяжень рухомого майна (ДРОРМ). Також воно забезпечує роботу цих систем, оновлює їх функціонал, а також надає послуги та товари (як-от захищені носії для електронного підпису) для органів влади та громадян.

Важливу роль у підвищенні ефективності роботи поліції відіграють інформаційно-довідкові системи Міністерства юстиції, зокрема портал НАІС, що містить структуровані нормативні документи, форми договорів та доступ до численних реєстрів за різними категоріями. Цей інструмент дозволяє працівникам поліції оперативно здійснювати юридичні перевірки, аналіз інформації та оформлення службових документів

Важливою сферою діяльності Національної поліції є забезпечення інформаційної безпеки. Система інформаційної безпеки передбачає захист даних від несанкціонованого доступу, випадкових або навмисних змін та забезпечення конфіденційності. Акцентуємо увагу на трьох ключових рівнях безпеки: законодавчо-правовому, адміністративному та програмно-технічному, що забезпечують комплексний захист інформаційних систем поліції. Практичний захист включає використання сертифікованих засобів криптографічного та технічного захисту інформації, рекомендованих державою [2, с. 57].

Використання ІКТ також забезпечує ефективне виконання основних службових завдань. Зокрема, автоматизація процесів за допомогою технологій штучного інтелекту, таких як Google Gemini, дозволяє оптимізувати роботу з документами, аналітичними матеріалами, презентаціями та інформаційними системами. ШІ-технології допомагають працівникам поліції оперативно генерувати документи, обробляти великі масиви інформації та підвищувати точність виконання службових завдань

Крім того, використання ІКТ у Національній поліції регламентується низкою нормативно-правових актів, що забезпечують правову основу для застосування інформаційних систем і засобів захисту інформації. Зокрема, накази НПУ щодо використання інформаційних систем, інформаційного обліку техніки, а також доступу до інформаційно-комунікаційної системи «Інформаційний портал Національної поліції» визначають порядок ведення реєстрів, обліку та захисту даних у процесі службової діяльності [3, с. 386].

Таким чином, ІКТ є критично важливим елементом діяльності Національної поліції України. Вони забезпечують оперативність, точність та ефективність службових дій, підвищують рівень інформаційної безпеки, сприяють цифровій трансформації правоохоронної системи та формуванню компетентного працівника поліції, здатного діяти в умовах сучасного інформаційного середовища.

Література

1. Інформаційні та комунікаційні технології: навчальний посібник / О.А. Дисковський, Е.В. Рижков, Ю.П. Синиціна, С.О. Прокопов. – ДДУВС, 2025. – 263 с. URL: https://osvita.dduvs.edu.ua/md/pluginfile.php/233305/mod_resource/content/3/%D0%9D%D0%9F%D0%86%D0%9A%D0%A2%2C2025%D0%B4%D0%BE%D1%80%D0%BE%D0%B1.pdf.
2. Основи інформаційної безпеки : навч. посіб. / О.С. Гавриш, В.Б. Вишня, Е.В. Рижков – Дніпро : ДДУВС, 2020. – 126 с.
3. Інформаційні технології : підручник. / І.В. Краснобрижий, С.О. Прокопов, В.Б. Вишня, Е.В. Рижков, К.Ю. Ісмайлов. – Дніпро : ДДУВС, 2021. – 492 с. URL: http://dspace.oduvs.edu.ua/handle/123456789/4325

Єсімов Сергій Сергійович
професор кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

МІЖНАРОДНО-ПРАВОВА ОХОРОНА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

Необхідність застосування саме комбінованих механізмів правової охорони програмного забезпечення обумовлена необхідністю мінімізації ризиків, пов'язаних з існуючими недоліками кожного окремого механізму, а саме:

1. Авторське право – охорона форми програмного забезпечення, тобто. вихідного коду програмного забезпечення, без можливості повноцінної охорони його змісту; складність доведення факту запозичення вихідного коду у спорах щодо порушення прав на програмне забезпечення [1];
2. Патентне право – складність контролю розповсюдження пристроїв, що містять таке програмне забезпечення з метою запобігання порушенню прав патентовласника; відсутність єдиного міжнародного патенту та однаковості патентної практики щодо програмного забезпечення; ризик монополізації ринку та посилення ситуацій зловживання патентними правами у зв'язку з поширенням патентної охорони щодо програмного забезпечення;
3. Ноу-хау – складність встановлення та підтримання режиму комерційної таємниці щодо програмного забезпечення; неможливість застосування даного режиму до програмного забезпечення, призначеного для публічного поширення, а отже, до програмного забезпечення, обсяг якого над ринком превалює; необхідність доведення не лише факту отримання інформації (початковий код програмного забезпечення), а й факту її використання.

Глобальним документом, що закріплює механізм правової охорони прав на програмне забезпечення через поширення на нього режиму

авторсько-правової охорони, став Договір Всесвітньої організації інтелектуальної власності з авторського права (далі – ДАП) від 1996 р. ст. 4 ДАП закріплює режим правової охорони програмного забезпечення як літературного твору, тобто. фактичне закріплення правової охорони програмного забезпечення режимом авторського права [2].

Крім прав автора, передбачених Бернської конвенцією про охорону літературних і мистецьких творів від 9 вересня 1886 р. [3], ДАП запроваджує нове «право повідомлення для загального відомості» (стаття 8 ДАП), під яким розуміється виняткове право дозволяти будь-яке повідомлення твори для загального зв'язку у проводах чи засобами бездротової.

Закріплення даного права насамперед пов'язане з розвитком мережі Інтернет як основного способу передачі та поширення різних видів інформації та екземплярів об'єктів авторського права, у тому числі екземплярів програмного забезпечення. Важливим доповненням, запровадженим ДАП, є поширення режиму охорони на технічні засоби захисту авторських прав (стаття 11 ДАП).

Технічні засоби захисту авторських прав мають особливе значення у існуючих механізмах правової охорони програмного забезпечення, оскільки, по-перше, технічні засоби захисту авторських прав природи можуть бути програмним забезпеченням; по-друге, закріплення регулювання технічних засобів як об'єкта, що охороняється, сприяє розвитку самозахисту своїх прав правовласниками; по-третє, удосконалення технічних засобів захисту програмного забезпечення призводить до створення нових договірних механізмів охорони програмного забезпечення та способів розповсюдження програмного забезпечення; по-четверте, технічні засоби захисту програмного забезпечення можуть створювати певні складнощі для користувачів, які мають чинність закону, рішення суду або договору за право використання програмного забезпечення, в частині реалізації такого права.

ДАП передбачає такий захід захисту прав, як розміщення «інформації про управління правами» йдеться про інформацію, яка ідентифікує твір, автора твору, володаря будь-якого права на твір чи інформацію про умови використання твору та будь-які цифри та коди. З метою

забезпечення можливості реалізації такого заходу захисту п.1 ч.1 ст.12 ДАП зобов'язує держави-учасниці забезпечити наявність доступних правовласнику юридичних механізмів протидії видаленню або заміні такої інформації.

Діє Директива N 2009/24/ЄС Європейського парламенту та Ради Європейського Союзу «Про правову охорону комп'ютерних програм (кодифікована версія)» (далі – Директива), яка є оновленою версією попередньої Директиви ЄС № 91/250/ЕЕС. Оскільки держави-учасниці ЄС зобов'язані імплементувати положення Директиви в їхнє національне законодавство в будь-якому порядку, що підходить для кожної держави-учасниці ЄС, саме в Директиві закріплюються основоположні принципи охорони прав на програмне забезпечення, які знаходять відображення в національних джерелах права та правозастосовній практиці [3]. Директива встановлює єдиний критерій надання охорони програмного забезпечення його оригінальність.

Визначення критерію оригінальності не встановлено на рівні Директиви, ні в судовій практиці, ні навіть у доктрині. Відсутність законодавчого визначення критерію оригінальності може бути обґрунтовано тим, що у разі його наявності могла бути створена монополія на певні види програмного забезпечення. Відсутність законодавчого визначення критерію оригінальності дозволяє створювати різним правовласникам схоже за своїм призначенням програмне забезпечення, що позитивно позначається на ринку програмного забезпечення, наприклад, наявність різних видів операційних систем, системних утиліт, антивірусного програмного забезпечення.

Критерій оригінальності програмного забезпечення повинен насамперед застосовуватися безпосередньо до вихідного коду програмного забезпечення, який і є зовнішньою формою висловлювання, тобто. об'єкт авторського права, і, як зазначає ряд дослідників, становить основний предмет незаконного запозичення у справах порушення прав на програмне забезпечення. Відсутність критерію оригінальності на законодавчому рівні є загальносвітовою тенденцією.

Директива ЄС сприйняла сучасну загальносвітову практику визначення критеріїв надання правової охорони програмного забезпечення режимом авторського права єдиним критерієм оригінальності за умови залишення визначення цього критерію на розсуд правозастосовних органів, які, у свою чергу, виробили та продовжили вдосконалювати диференційовані підходи до оцінки оригінальності програмного забезпечення. як окремих алгоритмів та команд, закріплених у вихідному та об'єктному коді, так і елементів аудіовізуального відображення, що породжуються програмним забезпеченням при його відтворенні у пам'яті комп'ютерного пристрою.

Аналіз міжнародних джерел права дозволяє зробити висновок про те, що хоча режим авторського права є загальновживаним і загальновизнаним механізмом правової охорони програмного забезпечення, ці джерела встановлюють гнучкий підхід, що дозволяє у відповідних випадках використовувати інші механізми правової охорони програмного забезпечення.

Динаміка розвитку ринку програмного забезпечення, кваліфікації співробітників державних органів, юристів і програмістів правовласників дозволяють з надією дивитися в майбутнє і вивести припущення про те, що багато держав приймуть побажання учасників ринку про можливість надання їм більш гнучких механізмів правової охорони прав на програмне забезпечення та договірних способів його поширення, що дозволить регулювати кінцевих користувачів. Подібний підхід дозволить забезпечити додатковий поштовх до розвитку нових технологій та дотримання багатостороннього балансу інтересів правовласників, користувачів-фізичних осіб, користувачів-суб'єктів підприємництва та держави в галузі регулювання діяльності зі створення, розповсюдження та використання програмного забезпечення.

Література

1. Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX. URL. https://zakon.rada.gov.ua/laws/show/2811-20#Text

2. Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20 грудня 1996 року та положення Бернської конвенції (1971 р.), на які містяться посилання у Договорі (Договір ВОІВ про авторське право) (1996). URL. https://zakon.rada.gov.ua/laws/show/995_770#Text
3. Про приєднання України до Бернської конвенції про охорону літературних і художніх творів (Паризького акта від 24 липня 1971 року, зміненого 2 жовтня 1979 року). URL. https://zakon.rada.gov.ua/laws/show/189/95-%D0%B2%D1%80#Text
4. Директива Європейського парламенту та Ради ЄС № 2009/24/ЄС від 23.04.2009 р. про правову охорону комп'ютерних програм (зведена редакція), Європейський союз (ЄС). URL. https://www.wipo.int/wipolex/ru/legislation/ details/8612

Жогло Ольга Володимирівна
викладач кафедри психології діяльності в особливих умовах Національний університет цивільного захисту України

ПСИХОЛОГІЧНА АНАЛІТИКА В СИСТЕМІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У сучасних умовах діяльність органів сектору безпеки і оборони України відзначається високим рівнем невизначеності та постійною загрозою для життя і здоров'я персоналу. Виконання завдань у таких умовах потребує швидкого прийняття рішень та роботи під значним психоемоційним навантаженням. Ці особливості формують складну операційну реальність, де управлінські рішення мають стратегічний характер і можуть нести високі ризики. У цьому контексті інформаційно-аналітичне забезпечення стає не просто допоміжним інструментом, а

ключовим механізмом, що забезпечує планування, оцінку ризиків і оперативне реагування на загрози [1] .

Ефективність будь-яких аналітичних систем значною мірою залежить від людського фактору – психоемоційного стану персоналу, його здатності до адаптації, стресостійкості та когнітивної гнучкості. Саме тому сучасні системи управління потребують інтеграції психологічної аналітики як окремого компонента інформаційно-аналітичного забезпечення. Ігнорування психофізіологічних особливостей людини може призвести до неефективного використання навіть найсучасніших технічних та інформаційних платформ і зробити управлінські рішення неточними або небезпечними [2] .

Психологічна аналітика у цьому контексті визначається як сукупність методів, інструментів та технологій, що дозволяють оцінювати психологічну готовність персоналу, прогнозувати рівень стресових реакцій, виявляти фактори ризику професійного вигорання та оптимізувати управління людськими ресурсами у кризових ситуаціях. Вона виступає інтегративним механізмом, який поєднує психологічні знання з аналітичними технологіями та даними різних систем, включаючи інформаційні, технічні, медичні та оперативні платформи.

Серед основних напрямів застосування психологічної аналітики у секторі безпеки і оборони можна виділити:

1. Оцінка когнітивних та емоційних характеристик персоналу, включаючи здатність до швидкого прийняття рішень, концентрацію уваги, стійкість до дезорієнтації та ефективну роботу в стресових умовах.
2. Моніторинг стресостійкості у реальному часі, що дозволяє виявляти симптоми втоми, перевантаження та емоційного виснаження до того, як вони негативно вплинуть на виконання завдань.
3. Прогнозування психоемоційних ризиків у екстремальних умовах, яке включає моделювання сценаріїв кризових ситуацій та оцінку потенційного впливу стресових факторів на колектив і окремих співробітників.
4. Підтримка прийняття рішень керівниками підрозділів, оскільки розуміння психоемоційного стану персоналу дозволяє ефективніше

планувати операції, розподіляти завдання та уникати критичних помилок у кризових ситуаціях.

5. Планування заходів щодо підвищення ефективності навчання та тренінгів, включаючи адаптацію програм під конкретні психофізіологічні та когнітивні характеристики персоналу, що підвищує результативність підготовки [1] .

Інформаційно-аналітична система, доповнена психологічними даними, дозволяє інтегрувати оцінку готовності персоналу до виконання завдань та враховувати потенційні ризики психоемоційного виснаження.

Практичне значення психологічної аналітики проявляється у кількох ключових аспектах:

– По-перше, вона дозволяє оцінювати психологічну готовність персоналу до роботи в умовах високого ризику та прогнозувати можливі стресові реакції.

– По-друге, інтеграція психологічних даних у загальні аналітичні системи підвищує точність прогнозів і ефективність управлінських рішень, зменшуючи ймовірність помилок та підвищуючи ефективність взаємодії в команді.

– По-третє, психологічна аналітика створює основу для формування превентивних заходів щодо підтримки психоемоційного стану персоналу, включаючи індивідуальні консультації, групові тренінги, методики саморегуляції та програми психологічної реабілітації після виконання складних завдань [2] .

Важливо підкреслити, що впровадження психологічної аналітики в інформаційно-аналітичне забезпечення передбачає міждисциплінарний підхід, де психологічні дані поєднуються з технічними, оперативними та стратегічними джерелами інформації. Такий підхід створює умови для комплексного аналізу ситуацій, підвищує точність управлінських рішень і дозволяє оптимально розподіляти ресурси персоналу, враховуючи його психоемоційні та когнітивні характеристики.

На сучасному етапі психологічна аналітика стає не лише невід'ємною складовою підготовки та підвищення ефективності роботи фахівців

екстремального профілю, а й ключовим фактором формування стійкості організаційних систем у кризових умовах. Вона дозволяє адаптувати освітні та тренінгові програми під індивідуальні та колективні потреби персоналу, підвищувати професійну компетентність, зменшувати ризики хронічного стресу, вторинної травматизації та професійного вигорання, а також забезпечує системну підтримку психологічної безпеки організації.

Таким чином, психологічна аналітика є стратегічно важливим компонентом інформаційно-аналітичного забезпечення органів сектору безпеки і оборони. Її інтеграція сприяє підвищенню готовності персоналу до діяльності в складних і критичних умовах, оптимізації управлінських рішень та ефективному використанню ресурсів. Розвиток психологічної аналітики відкриває нові можливості для прогнозування поведінки персоналу в кризових ситуаціях, удосконалення систем підготовки та підвищення оперативної ефективності органів безпеки. У довгостроковій перспективі використання психологічних даних у комплексних аналітичних системах дозволяє формувати адаптивні та стійкі організаційні структури, здатні оперативно реагувати на сучасні загрози.

Отже, психологічна аналітика виступає не лише інструментом підвищення ефективності управління, а й необхідною умовою розвитку сучасного сектору безпеки і оборони в умовах нестабільності та високої невизначеності.

Література

1. Алещенко В. В., Хміляр О. Ф. Інформаційно-психологічна безпека особистості в умовах воєнних дій. Вісник Національного університету оборони України. № 1 (83). 2025. С. 16-25. DOI: 10.33099/2617-6858-2025-83-1-16-25.
2. Осьодло В. І., Грилюк С. М., Тютюнник Л. Л. Сучасний стан і перспективи психологічного забезпечення в Збройних Силах України. Дніпровський науковий часопис публічного управління, психології, права, № 2. 2021. С. 86–92. DOI: https://doi.org/10.51547/ppp.dp.ua/2021.1.14

Зачек Олег Ігорович
кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій Львівського державного університету внутрішніх справ

НЕБЕЗПЕКА ВИКОРИСТАННЯ ШИРОКОДОСТУПНИХ МЕСЕНДЖЕРІВ В ОРГАНАХ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

Умови повномасштабної війни суттєво підвищили роль цифрових комунікацій у діяльності органів сектору безпеки та оборони України. Широкодоступні месенджери (Telegram, WhatsApp, Viber, Signal тощо) є дуже зручними для оперативного обміну інформацією, однак їх застосування в службовій діяльності створює значні ризики для інформаційної та кібербезпеки. Тому 19 вересня 2024 року Національний координаційний центр кібербезпеки (НКЦК) прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури, зазначивши, що «Telegram активно використовується ворогом для кібератак, розповсюдження фішингу та шкідливого програмного забезпечення, встановлення геолокації користувачів, корегування ракетних ударів тощо» [1]. Внаслідок цього в державних установах було заборонено використовувати месенджер Telegram на службових пристроях.

Основна загроза полягає у відсутності повного контролю держави над інфраструктурою таких сервісів, зберіганням даних, механізмами шифрування та юрисдикцією обробки інформації. Навіть за наявності наскрізного шифрування залишаються ризики компрометації метаданих, перехоплення трафіку, використання вразливостей клієнтських застосунків або зараження кінцевих пристроїв шкідливим програмним забезпеченням.

За інформацією сайту «Чатові онлайн» проекту «BRAMA», який діє за підтримки Департаменту кіберполіції Національної поліції України, основною проблемою публічно доступних месенджерів є безпека, і жоден

з них не може гарантувати повну безпеку, зокрема Electronic Frontier Foundation не може рекомендувати жоден додаток, як такий, що гарантує повну безпеку [2].

Додаткову небезпеку становить активне використання месенджерів противником для проведення розвідувальних операцій, соціального інжинірингу, фішингових атак, поширення дезінформації та ідентифікації військовослужбовців, правоохоронців і посадових осіб. Створення фейкових акаунтів, каналів і чатів дозволяє зловмисникам збирати чутливу інформацію, впливати на морально-психологічний стан особового складу та координувати інформаційні операції.

Суттєвим ризиком є також людський фактор: використання особистих облікових записів у службових цілях, слабкі паролі, відсутність двофакторної автентифікації, збереження службової інформації на приватних пристроях. Це значно підвищує ймовірність витоку даних у разі втрати, викрадення або зламу смартфонів.

Спочатку вважалося, що WhatsApp є більш безпечним ніж Telegram. Однак, з'явилася інформація, що розробники WhatsApp попереджають про загрози безпеці та конфіденційності через необхідність виконання вимоги Закону про цифрові ринки Європейського Союзу щодо забезпечення можливості міжплатформового обміну повідомленнями з іншими месенджерами, з-за чого неможливо гарантувати безпеку повідомлень шляхом наскрізного шифрування [3].

Месенджер Signal вважається найбільш захищеним, через що його широко використовують в Збройних силах України. Але на думку офіцера, який служить в Міністерстві оборони України, Андрія Єрмолаєва, хоча Signal є досить добре захищеним, у випадку ураження 0-day експлойтом листування будуть розкриті [4].

У зв'язку з цим актуальним є обмеження або заборона використання широкодоступних месенджерів для передавання службової інформації в органах сектору безпеки та оборони, впровадження захищених відомчих систем зв'язку, розроблення чітких нормативних вимог і підвищення рівня кібергігієни персоналу. Лише комплексний

організаційно-правовий і технічний підхід здатний мінімізувати ризики, пов'язані з використанням масових комунікаційних платформ в умовах воєнного стану.

Тому в даний час перелік заборонених для передачі службової інформації месенджерів розширюється. На виконання доручення Міністра внутрішніх справ України від 09.12.2025 №96/01/16 було видано наказ по Львівському державному університету внутрішніх справ від 11.12.2025 № 546 «Про обмеження використання публічно доступних месенджерів», яким було заборонено працівникам університету встановлення програмного забезпечення WhatsApp та Telegram, а також інших публічно доступних месенджерів на службових комп'ютерах (пристроях).

Література

1. НКЦК прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури // Рада національної безпеки і оборони України. Новини від 20.09.2024. URL: https://www.rnbo.gov.ua/ua/Diialnist/6994.html. (дата звернення: 15.12.2025).
2. Ризики в соціальних мережах // Чатові онлайн від 01.05.2024. URL: https://chatovi.online/articles/Riziki%20v%20sotsial%27nikh%20merezhakh. (дата звернення: 15.12.2025).
3. 2 мільярди користувачів WhatsApp опинилися під загрозою втрати конфіденційності // No worries.news 09.03.2024. URL: https://noworries.news/2-milyardy-korystuvachiv-whatsapp-opynylysya-pid-zagrozoyu-vtraty-konfidenczijnosti/. (дата звернення: 15.12.2025).
4. Андрій Єрмолаєв. Коротке дослідження безпеки використання месенджера Signal на iOS (iPhone) // DOU.UA від 05.03.2025. URL: https://dou.ua/forums/topic/53631/. (дата звернення: 15.12.2025).
5. Наказ ЛьвДУВС від 11.12.2025 № 546 «Про обмеження використання публічно доступних месенджерів».

Ivanova Roksolana Yuriivna
Professor of International and European Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Ph.D. in Law, Associated Professor

INTERNATIONAL ORGANIZATIONS IN INFORMATION AND ANALYTICAL SUPPORT OF THE SECURITY AND DEFENSE SECTOR UNDER HYBRID THREATS

The blending of military force, information manipulation, cyber operations, economic coercion, and destabilization constitutes a new class of threat which alter patterns of security governance. These new threat dynamics require security and defense to leverage new information and analytical frameworks. In such context, the analytical dimension of the defense and security system no longer constitutes the periphery, but the very foundation of security policy and the principal options of defense and security.

A high degree of sophistication and a transnational dimension characterize what we have called hybrid threats. In destabilizing a target state and neutralizing its public institutions, such threats simultaneously employ disinformation, cyberattacks, clandestine transfers of financial resources, corruptive strategies, and economic coercion. These threats create a new dimension of the security of a state where the internal and the external threats collide and compromise the spatial order of the legal, institutional, and administrational frameworks. Counteraction and the integration of various systems require the identification, assessment of the risks and the impact of those risks, and the system of information and analytical support.

Globalization has created a situation where states turn to inter-governmental organizations for not just political coordination but also analytical expertise. International organizations serve as analytical actors in the security and defense field. They collect and analyze vast amounts of data on security and instability, economic and financial risk, economic resilience, and the institutional weaknesses of states, and in turn, focus a state's attention on national security.

Also, international financial institutions and other specialized agencies provide important analytical assistance. The International Monetary Fund carries out macroeconomic monitoring and analyzes the sustainability of a country's finances, health, balance of payments, and stability of the financial sector, all of which are national security concerns under hybrid threats. The World Bank, in turn, adds to that analysis by assessing the quality of governance and institutions, the resilience of societies, and the socio-economic impacts of crises (providing the analytical underpinnings for security analysis to be valued). Such analysis is utilized by states to formulate security and related legislative strategies.

Multinational organizations have also assumed important analytical roles pertaining to financial security. The FadF has developed risk-based analytical frameworks to identify potential financial abuse threats related to laundering and financing terrorism. These analytical mechanisms help safeguard the financial apparatus from threats' abuse and the financing of financing hybrid operations. Thus, financial analytical mechanisms are part of the security and defense policy.

The U.N., the European Union, NATO and the OECD are also International organizations that serve as strategic analysis and information exchange hubs. They support national strategic planning and policy integration with their reports on geo-strategic phenomena, security risks, and institutional weaknesses. International organizations facilitate analytical information exchange among states through peer review, monitoring, and reporting processes. This is critical to addressing hybrid threats that are beyond the nation's borders.

This issue looks first of all at international organizations. The analysis of international organizations from a legal perspective considers constituent instruments, provisions of international organizations, and legal acts of lesser rank. The scope of these legal documents defines the power to collect information, the scope of the monitoring of the confidentiality regimes, the legal nature of the analytical documents, and the analytical output. The analytical tools of soft law and others are forms of law. Proposed law may not be law in the formal sense, but in practice, it does affect national legal systems

and systems of governance. The impact of the proposed frameworks and instruments 'soft law' status analysis goes far beyond the 'soft law' status of the instruments. The impact of the instruments proposed on the national legal systems and systems of governance is huge and must be taken in account. Governance systems the public control of finances, cyber security, the procurement of public services, and the transparency of public institutions are restricted in instruments. proposed law public governance systems affect the systems of public governance proposed instruments. The scope of these legal documents restrict in governance the control of public finances and the transparency of institutions.

Sovereignty issues concern many practitioners. Where public governance systems proposed instruments affect the cyber security instruments proposed, the proposed instruments of legal public control governance systems and transparency of public institutions public control of the finances proposed governance systems the instruments proposed concern many practitioners. The systems of public control of the finances proposed impact the cyber security instruments proposed. While International Organizations augment National Analytical Capacities, a Versatile Dependence on Analytical outputs may limit National Discretion. A Versatile Dependence on Analytical outputs may limit National Discretion. International Analytical Support should complement national analytical systems. The control of public finances proposed instruments should be incorporated into the systems to augment the national analytical systems of public control of finances. The Integration of Analytical Instruments Proposed International Supporting the control of public finances proposed systems must be complemented. Analytical systems of public control. Finance proposed systems must be complemented.To work constructively with global institutions, countries must have the systems in place to legally share and analyze data in a coordinated fashion with their national security infrastructures. Countries may otherwise miss out on the benefits of international analytical assistance and may have considerable legal risks associated with the use of foreign data. When dealing with hybrid, multi-type threats, countries must find the right balance legally and to exercise proportionality and accountability in a way that national and international faith in democracy is preserved and fundamental rights are observed [6].

Accordingly, global institutions must be seen as crucial players in the security and defense domain's information and analytical assistance in times of hybrid threats. Their analysis contributes to the understanding of the threat and its risks and helps in making choices to steer strategy. At the same time, the governance of security on the national level, as well as its legal frameworks still needs to be bolstered to maintain effective control over security in a more complex environment.

References

1. International economic relations and prospects for national developments: contemporary challenges and solutions: monograph / ed. M. Fleychuk, U. Ganski, V. Kazlouski. Daugavpils: Daugava Print, 2018. 368 p.
2. International Monetary Fund. Global Financial Stability Report. Washington, DC: International Monetary Fund, 2023.
3. World Bank. World Development Report 2022: Finance for an Equitable Recovery. Washington, DC: World Bank, 2022.
4. Rodrik D. The Globalization Paradox: Democracy and the Future of the World Economy. New York: W.W. Norton & Company, 2011.
5. UN Conference on Trade and Development. Trade and Development Report 2023. Geneva: United Nations, 2023.
6. European Commission. EU Economic Governance Review: Key Documents and Policy Directions. Brussels: European Commission, 2023.
7. Organisation for Economic Co-operation and Development. Global Economic Outlook and Policy Responses to Fragmentation. Paris: OECD, 2023.

Іващенко Сергій Миколайович

доцент кафедри права Національної безпеки та правової роботи Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого, полковник

Скорик Вероніка Вячеславівна

курсант Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Правові засади захисту інформації у Збройних Силах України в умовах воєнного стану набувають виняткової важливості, оскільки є невід'ємною складовою національної безпеки та оборони, закріпленою в статті 17 Конституції України [1]. Актуальність наведеного питання зумовлена необхідністю збереження військової таємниці, забезпечення стійкості систем управління військами та ефективної протидії розвідувально-підривній діяльності противника, зокрема у кіберпросторі. Юридичним фундаментом наведеного напряму є низка законодавчих актів. Серед них — Закон України «Про захист інформації в інформаційно-комунікаційних системах» [2], що встановлює загальні принципи та об'єкти захисту, а також Закон України «Про державну таємницю» [3], який регулює роботу з інформацією з обмеженим доступом. Специфіка воєнного стану вимагає застосування норм Законів України «Про основи національного спротиву» [4] та «Про правовий режим воєнного стану» [5], які конкретизують повноваження та особливості організації захисту інформації в умовах агресії, а також деталізуються нормативно-правовими актами Міністерства оборони України та Генерального штабу Збройних Сил України.

Специфіка правового режиму захисту інформації в умовах воєнного стану полягає у розширенні правових повноважень військового командування та органів військового управління щодо обмеження доступу, контролю та поширення інформації, особливо в зоні бойових дій,

відповідно до статті 19 Закону України «Про правовий режим воєнного стану» [5]. Правові норми передбачають пріоритет заходів військової безпеки над правом на доступ до публічної інформації, що є виправданим для запобігання розголошенню відомостей про переміщення військ, озброєння чи плани операцій. Одночасно відбувається посилення юридичної відповідальності (кримінальної та адміністративної) за несанкціоноване поширення, витік або втрату інформації з обмеженим доступом, зокрема державної таємниці, згідно з нормами Кримінального кодексу України (статті 328, 422) [6].

Правове регулювання захисту інформації у Збройних Силах України охоплює декілька основних напрямів. Перш за все, це захист інформації, що становить державну таємницю, який регламентує режим секретності, порядок засекречування/розсекречування, допуску та доступу до таємної інформації відповідно до вимог Закону України «Про державну таємницю» [3]. Другим критичним напрямом є кіберзахист та інформаційна безпека, що встановлює правові вимоги до побудови комплексних систем захисту інформації в інформаційно-телекомунікаційних системах Збройних Сил України, їх сертифікації та регулює протидію кібератакам, зокрема відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [7]. Крім того, важливою складовою є правові основи оперативного маскування та дезінформації, що включає обмеження поширення відомостей, які можуть бути використані противником. Не менш важливим є захист персональних даних військовослужбовців та працівників Збройних Сил України в умовах підвищеної загрози їх компрометації, згідно з Законом України «Про захист персональних даних» [8].

Попри наявну правову базу, існують і проблемні аспекти, які потребують удосконалення. Зокрема, необхідною є гармонізація національного законодавства у сфері кіберзахисту з вимогами та стандартами НАТО для забезпечення взаємосумісності. Важливим є також правове регулювання питань кадрового та ресурсного забезпечення, зокрема підготовки фахівців з кібербезпеки. Нарешті, гостро стоїть питання пошуку оптимального балансу між безпекою та відкритістю, тобто між

забезпеченням військової безпеки та дотриманням принципів прозорості та свободи слова, наприклад, у взаємодії із засобами медіа. На підставі викладеного можна зробити висновок, що правові засади захисту інформації у Збройних Силах України в умовах воєнного стану є комплексною та динамічною системою, яка постійно адаптується до нових викликів. Подальше удосконалення законодавства та посилення виконавчої дисципліни є критично важливими для забезпечення обороноздатності держави.

Література

1. Верховна Рада України; Конституція України,Закон від 28.06.1996 № 254к/96-ВР.
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР.
3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII.
4. Закон України «Про основи національного спротиву» від 16.07.2021 № 1702-IX.
5. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII.
6. Кримінальний кодекс України від 05.04.2001 № 2341-III (статті 328, 422).
7. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
8. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.

Івкова Валерія Сергіївна
аспірант кафедри захисту інформації Національного університету «Львівська політехніка»

ОЦІНКА РИЗИКІВ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ВІДКРИТІ ДЖЕРЕЛА ЯК СКЛАДНИК АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ

Еволюція інформаційних технологій радикально змінила ландшафт національної безпеки, перетворивши відкриті джерела інформації та OSINT на один із ключових інструментів сучасної аналітики. Традиційне розуміння розвідувальної діяльності, що десятиліттями базувалося на пріоритеті таємних методів збору даних, сьогодні поступається місцем інтегрованим підходам, де понад 80% критично важливих даних отримуються з публічно доступних або комерційних сегментів інформаційного простору.

Розвідка на основі відкритих джерел визначається як систематичний процес збору, обробки та аналізу публічно доступної інформації для задоволення специфічних розвідувальних вимог та підтримки процесу прийняття рішень.

Проте парадокс OSINT полягає в його двосічному характері. Ті самі інструменти, що використовуються силами безпеки для захисту держави, стають потужною зброєю в руках супротивника для виявлення та експлуатації конфіденційної інформації. Оцінка ризиків витоку такої інформації через відкриті джерела є критично важливою для забезпечення оперативної безпеки та підтримки стійкості державних інституцій. Конфіденційна інформація в цьому контексті охоплює широкий спектр даних: від персональних відомостей про особовий склад до технічних параметрів критичної інфраструктури та стратегічних планів оборони [1, с.171].

Згідно Закону України «Про захист інформації в інформаційно-комунікаційних системах» під витоком даних слід розуміти діяння,

внаслідок якого відомості, що оброблюються в інформаційній системі, стали відомі суб'єктам, які не мають права доступу до такої інформації. З точки зору кримінального законодавства витоком даних є наслідок несанкціонованого втручання. Проте, вказані поняття не охоплюють інформацію, яка стала відомо опосередковано, наприклад шляхом публікації особистих фото, на яких зображено частину документів або технічне забезпечення приміщення.

Ризики витоку інформації через відкриті джерела не є монолітними; вони формуються внаслідок взаємодії технічних вразливостей, організаційних прорахунків та людського фактора. У сучасному цифровому світі будь-яка активність організації або її співробітників залишає слід, який може бути інтерпретований супротивником. Концепція «мозаїчного аналізу» припускає, що навіть дрібні, на перший погляд неважливі фрагменти публічної інформації, зібрані разом, можуть розкрити таємниці стратегічного рівня [2].

Для ефективної протидії витокам сили безпеки повинні перейти від реактивної моделі (реагування на інциденти) до проактивної стратегії Counter-OSINT. Це передбачає не лише технічний захист, а й зміну організаційної культури поводження з інформацією [1, с. 174].

Класичний підхід OPSEC повинен бути доповнений «цифровою гігієною», це включає:

Мапування цифрового сліду - організації повинні проводити регулярні «аудити видимості», використовуючи ті самі інструменти, що й зловмисники (TheHarvester, SpiderFoot, тощо), щоб побачити, яка інформація про них доступна в мережі.

Класифікація інформації на етапі створення. Зокрема, пропонується впровадження систем, які автоматично видаляють метадані з файлів перед їх завантаженням на публічні ресурси.

Контроль витоків через треті сторони, який передбачає оцінку ризиків підрядників та партнерів, через чиї публічні звіти або вакансії може витікати інформація про замовника.

Оцінка ризиків витоку конфіденційної інформації через відкриті джерела стала невід'ємною частиною архітектури національної безпеки. У світі, де інформація генерується зі швидкістю світла, сили безпеки повинні не лише досконало володіти методами OSINT для розвідки, а й вибудовувати ешелоновану оборону власного інформаційного простору.

Майбутнє аналітичного забезпечення полягає в глибокій інтеграції ШІ, який дозволить автоматизувати як збір розвідувальних даних, так і безперервний моніторинг власних ризиків. Проте технології залишаються лише інструментами в руках людини. Ключовим фактором успіху є розвиток аналітичного мислення, суворе дотримання етичних норм та безперервне навчання особового складу принципам оперативної безпеки в цифрову епоху.

Україна, маючи унікальний досвід протидії агресії в умовах тотальної інформаційної відкритості, має всі шанси стати світовим лідером у розробці стандартів Counter-OSINT та інноваційних методів аналізу відкритих джерел. Це потребує тісної співпраці між державним сектором, науковими установами та приватним технологічним бізнесом для створення стійкої та проактивної системи національної безпеки.

Своєчасна ідентифікація ризиків, впровадження стандартів ISO 27005 та NIST 800-30, а також критичне розуміння можливостей штучного інтелекту дозволять силам безпеки України перетворити вразливість відкритих джерел на стратегічну перевагу, забезпечуючи надійний захист держави та її громадян від сучасних та майбутніх загроз.

Література

1. Івкова, В., & Опірський, І. (2025). OSINT-ТЕХНОЛОГІЇ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ДЕРЖАВИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), с. 165–179. https://doi.org/10.28925/2663-4023.2025.27.749
2. Kimery A. DOD service members, others face security risks from publicly accessible digital data | Biometric Update. Biometric Update | Biometrics News, Companies and Explainers. URL: https://www.biometricupdate.com/202511/dod-service-members-others-face-security-risks-from-publicly-accessible-digital-data

Іоєнко Сергій Сергійович
здобувач заочної форми навчання другого «магістерського» рівня вищої освіти Одеського державного університету внутрішніх справ

ІНФОРМАЦІЙНА АНАЛІТИКА ЯК ЗАСІБ ОДЕРЖАННЯ ЗНАНЬ

У сучасному інформаційному суспільстві здатність ефективно обробляти, аналізувати та інтерпретувати дані стає критично важливою компетенцією, а особливо для правоохоронних органів [8]. Національна поліція України (далі – НПУ), функціонуючи в умовах динамічних змін криміногенної обстановки та зростаючих обсягів інформації, потребує застосування передових методів інформаційної аналітики для прийняття обґрунтованих управлінських рішень [6]. Інформаційна аналітика при активному застосуванні в практичній діяльності дозволяє трансформувати великі масиви даних у цінні знання, що забезпечують стратегічну перевагу в протидії злочинності.

Поєднуючи методи статистики, машинного навчання, візуалізації даних та когнітивних наук з метою вилучення значущої інформації з різноманітних джерел даних, інформаційна аналітика являє собою міждисциплінарну галузь знань [3]. За визначенням сучасних дослідників, інформаційна аналітика охоплює процеси збору, обробки, аналізу та інтерпретації даних для підтримки прийняття рішень в умовах невизначеності.

Ключовою особливістю інформаційної аналітики є її здатність перетворювати необроблені дані на структуровану інформацію, а згодом – на практично застосовні знання. Ця трансформація відбувається через послідовні етапи когнітивної обробки, де кожен рівень додає додаткову цінність: дані стають інформацією через контекстуалізацію, інформація перетворюється на знання через аналіз та інтерпретацію, а знання в подальшому набувають форми мудрості через практичне застосування та накопичення досвіду.

Сучасна інформаційна аналітика ґрунтується на кількох базових методологічних підходах, кожен із яких виконує власну функцію в процесі дослідження даних, але найбільшої ефективності вони набувають саме у взаємодії між собою.

Першою фундаментальною складовою є дескриптивна аналітика, що забезпечує узагальнення та систематизацію історичних даних. На цьому етапі аналітик визначає характерні тенденції й закономірності, оцінює рівень і структуру явищ, що досліджуються, а також отримує первинні уявлення про динаміку процесів [2]. Для правоохоронної діяльності це означає виявлення тенденції злочинності, визначення гарячих точок у просторі, аналіз сезонних коливань чи структурних особливостей правопорушень.

Другою методологічною складовою є діагностична аналітика, яка спрямована на встановлення причин і механізмів формування подій та явищ. На цьому рівні увага приділяється з'ясуванню того, чому саме відбулося те чи інше явище, який набір факторів вплинув на його розвиток і як вони взаємодіють між собою. Діагностичний підхід передбачає аналіз кореляційних і причинно-наслідкових зв'язків між змінними, дослідження залежностей і виявлення ключових установок поведінки системи. Для аналітичних підрозділів НПУ цей тип аналізу є надзвичайно важливим, оскільки допомагає встановити, які соціальні, економічні, географічні чи поведінкові чинники сприяють зростанню рівня злочинності, як зміни у середовищі впливають на криміногенну ситуацію, та які системні процеси лежать в основі правопорушень.

Предиктивна аналітика є наступним етапом, що формує прогностичний погляд на ситуацію. Вона застосовує статистичні моделі, математичні методи та алгоритми машинного навчання для визначення ймовірності майбутніх подій на основі виявлених закономірностей [4]. Застосування предиктивного аналізу дозволяє оцінювати потенційні ризики, прогнозувати розвиток криміногенної ситуації у різних районах, визначати періоди можливого зростання злочинної активності, а також створювати моделі поведінки правопорушників. У роботі НПУ такі прогнози можуть слугувати підґрунтям для планування оперативно-

службової діяльності, визначення пріоритетів ресурсного забезпечення, підготовки превентивних заходів та оптимізації розміщення патрульних нарядів. Застосування машинного навчання, зокрема алгоритмів кластеризації, регресійного аналізу та дерев рішень, робить прогнози більш точними та адаптивними. [3]

Завершальною складовою виступає прескриптивна аналітика — найвищий рівень аналітичної діяльності, що інтегрує результати попередніх етапів і спрямований не лише на прогнозування, а й на формування оптимальної стратегії дій у конкретних умовах. Прескриптивна аналітика пропонує найбільш ефективні сценарії прийняття рішень, визначає можливі варіанти реагування та оцінює наслідки кожного з них, ґрунтуючись на моделюванні, оптимізаційних методах і теорії ухвалення рішень. Для НПУ ці можливості означають формування обґрунтованих превентивних заходів, оптимізацію оперативних операцій, підготовку рекомендацій для командирів підрозділів та розробку стратегічних рішень, спрямованих на зниження рівня злочинності та підвищення ефективності реагування.

У контексті діяльності аналітичних підрозділів Національної поліції України особливого значення набуває не окреме застосування кожного підходу, а їх інтеграція в єдину аналітичну систему.

Дескриптивна аналітика забезпечує розуміння поточного стану криміногенної обстановки, діагностична — виявляє сутнісні причини та чинники, що формують злочинну активність, предиктивна — дозволяє прогнозувати можливі прояви правопорушень, а прескриптивна — розробляє можливі варіанти реагування та оптимальні управлінські рішення. У комплексі такі підходи формують цілісну методологічну основу аналітичної підтримки правоохоронної діяльності, підвищуючи ефективність планування, управління та оперативної роботи в умовах сучасної криміногенної динаміки. [5].

Технологічна підґрунтя сучасної інформаційної аналітики складає широкий спектр інструментів та платформ. Системи управління базами даних забезпечують зберігання та структурування великих обсягів інформації. Інструменти бізнес-аналітики та візуалізації даних дозволяють створювати інтерактивні дашборди та звіти для оперативного

моніторингу ключових показників. Платформи для роботи з великими даними надають можливість обробляти структуровані та неструктуровані дані з різноманітних джерел [9].

Особливу роль відіграють технології штучного інтелекту та машинного навчання, які автоматизують процеси виявлення аномалій, класифікації об'єктів, кластеризації даних та прогнозування [1]. Алгоритми обробки природної мови дозволяють аналізувати текстові документи, виявляти сентимент та витягувати ключову інформацію з неструктурованих джерел. Технології геопросторового аналізу забезпечують можливість картографування злочинності та виявлення географічних патернів злочинних проявів.

Центральним аспектом інформаційної аналітики є процес перетворення сирих даних на практично застосовні знання. Цей процес включає кілька послідовних етапів, кожен з яких додає якісно нову характеристику інформаційному продукту.

На етапі збору даних формується емпірична база аналізу через агрегацію інформації з різноманітних джерел: офіційної статистики, оперативних матеріалів, відкритих джерел, соціальних мереж, технічних систем спостереження [7]. Якість вихідних даних критично впливає на достовірність подальших аналітичних висновків, тому особлива увага приділяється верифікації джерел та валідації даних.

Етап обробки та очищення даних передбачає усунення помилок, дублікатів, неповних записів, стандартизацію форматів та структурування інформації. Використання методів нормалізації, агрегації та трансформації дозволяє підготувати дані до подальшого аналізу. На цьому етапі необроблені дані набувають форми структурованої інформації, придатної для аналітичної роботи.

Аналітична обробка включає застосування статистичних методів, алгоритмів машинного навчання, методів інтелектуального аналізу даних для виявлення закономірностей, трендів, кореляцій та аномалій. Саме на цьому етапі відбувається перетворення інформації на знання через виявлення прихованих патернів та встановлення значущих зв'язків між даними.

Етап інтерпретації та контекстуалізації передбачає осмислення отриманих аналітичних результатів у контексті конкретних завдань та ситуацій. Аналітик інтегрує формальні результати аналізу з експертними знаннями, врахуванням специфіки оперативної обстановки та стратегічних пріоритетів організації. На цьому етапі знання набувають форми практичних рекомендацій та обґрунтованих висновків.

Інформаційна аналітика дозволяє отримувати різні типи знань, кожен з яких має специфічну цінність для діяльності правоохоронних органів. Дескриптивні знання описують поточний стан об'єктів аналізу, характеризують тенденції та закономірності в історичній ретроспективі [2]. Вони відповідають на питання «що відбувається?» та формують емпіричну основу для прийняття рішень.

Пояснювальні знання розкривають причинно-наслідкові зв'язки між явищами, пояснюють механізми формування певних процесів та подій. Такі знання відповідають на питання «чому це відбувається?» та дозволяють розуміти глибинні фактори, що впливають на криміногенну ситуацію.

Прогностичні знання стосуються майбутніх станів та подій, формуються на основі екстраполяції виявлених закономірностей та моделювання можливих сценаріїв розвитку [4]. Вони відповідають на питання «що може статися?» та забезпечують можливість превентивного реагування на потенційні загрози.

Прескриптивні знання пропонують конкретні дії та рішення, оптимальні для досягнення визначених цілей в умовах конкретної ситуації. Такі знання відповідають на питання «що потрібно робити?» та безпосередньо підтримують процес управлінського рішення.

Висновки

Інформаційна аналітика являє собою потужний засіб трансформації даних у цінні знання, що забезпечують обґрунтоване прийняття рішень в діяльності правоохоронних органів. Через послідовні етапи збору, обробки, аналізу та інтерпретації даних формуються різні типи знань, кожен з яких відіграє важливу роль у забезпеченні ефективності поліцейської роботи [3].

Застосування методів інформаційної аналітики в діяльності НПУ дозволяє підвищити якість аналізу криміногенної обстановки, забезпечити своєчасне виявлення та прогнозування загроз, оптимізувати використання ресурсів, підвищити рівень превентивної роботи. Інтеграція сучасних технологій штучного інтелекту, великих даних, геопросторового аналізу створює нові можливості для розвитку аналітичних спроможностей правоохоронних органів [1].

Водночас ефективне використання інформаційної аналітики вимагає вирішення комплексу технологічних, методологічних, організаційних та етичних викликів. Необхідне забезпечення якості даних, розвиток технологічної інфраструктури, підготовка кваліфікованих кадрів, формування відповідної організаційної культури, дотримання балансу між ефективністю та захистом прав громадян [10]. А перспективи розвитку пов'язані з подальшим удосконаленням технологій штучного інтелекту, розширенням джерел даних, інтеграцією аналітичних систем, розвитком міжнародного співробітництва. Інформаційна аналітика залишатиметься ключовим інструментом модернізації правоохоронної системи та підвищення її здатності ефективно протидіяти сучасним викликам у сфері громадської безпеки.

Література

1. Chen H., Chung W., Xu J.J., Wang G., Qin Y., Chau M. Crime data mining: a general framework and some examples. Computer. 2004. Vol. 37. No. 4. P. 50-56. https://doi.org/10.1109/MC.2004.1297301
2. Davenport T.H., Harris J.G. Competing on Analytics: The New Science of Winning. Boston: Harvard Business School Press, 2007. 240 p.
3. Provost F., Fawcett T. Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking. O'Reilly Media, 2013. 414 p.
4. Perry W.L., McInnis B., Price C.C., Smith S., Hollywood J.S. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation, 2013. https://www.rand.org/pubs/research_reports/ RR233.html

5. Ratcliffe J.H. Intelligence-Led Policing. 2nd ed. Routledge, 2016. 300 p. https://doi.org/10.4324/9781315717579
6. Europol. European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. Publications Office of the European Union, 2021. https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment
7. UNODC. Research Brief: Using Data Analytics to Support Anti-Corruption Efforts. United Nations Office on Drugs and Crime, 2019. https://www.unodc.org/documents/data-and-analysis/statistics/corruption/Research_brief_data_analytics_anti-corruption.pdf
8. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: http://zakon.rada.gov. ua/laws/show/580-19.
9. European Commission. Communication on Artificial Intelligence for Europe. COM(2018) 237 final. Brussels, 2018. https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)237
10. Interpol. Global Guidelines for Digital Forensics Laboratories. Lyon: INTERPOL, 2019. https://www.interpol.int/en/How-we-work/Forensics/Digital-Forensics/

Іщенко Артем Муратович

студент Львівського державного університету безпеки життєдіяльності

Ткачук Ростислав Львович

професор кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, д.т.н., професор

Івануса Андрій Іванович

начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, к.т.н., доцент,

ІНФОРМАЦІЙНО-АНАЛІТИЧНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ ОСВІТНІМ ПРОЦЕСОМ ВНЗ МВС ТА ДСНС УКРАЇНИ

Сучасний освітній процес характеризується високим рівнем інформаційної насиченості, цифровізацією управлінських і навчальних процедур та динамічними змінами в організації навчальної діяльності. У цих умовах зростає роль інформаційно-аналітичних технологій (ІАТ), які забезпечують перехід від інтуїтивного управління до прийняття рішень на основі даних [1]. Для вищих навчальних закладів системи МВС та ДСНС України це питання набуває особливої актуальності з огляду на специфіку підготовки фахівців у сфері безпеки, необхідність жорсткого контролю дисципліни, успішності та ресурсного забезпечення.

Інформаційно-аналітичні технології в освіті спрямовані на систематизацію, зберігання, обробку та аналіз великих обсягів даних з метою формування аналітичної інформації для управління освітнім процесом. Вони забезпечують можливість моніторингу успішності здобувачів освіти, прогнозування результатів навчання, оцінювання ефективності освітніх програм і діяльності викладачів [2, 3].

Для практичної реалізації ІАТ використовуються операційні системи, сервісні програмні продукти, мови програмування та прикладні інформаційні системи, зокрема бази даних, статистичні пакети та інструменти візуалізації. У навчальному процесі застосовуються технології оброблення даних, системи підтримки прийняття рішень та експертні системи, що

дозволяють автоматизувати рутинні операції, формування звітності та аналітичних оглядів.

Інформаційно-аналітична діяльність у вищих навчальних закладах МВС та ДСНС спрямована на трансформацію первинних даних про навчальну активність, успішність, відвідуваність, виконання практичних завдань і адміністративні процеси у структуровані знання. Отримані результати слугують основою для обґрунтованих управлінських та педагогічних рішень.

Основу організації аналітичного процесу складають такі принципи [4]:

– достовірність, що передбачає системний відбір та аналіз інформації з урахуванням причинно-наслідкових зв'язків;

– своєчасність, яка забезпечує подання аналітичних матеріалів у моменти, критично важливі для прийняття рішень;

– ясність і логічність викладення, що гарантує зрозумілість аналітичних висновків для різних категорій користувачів.

Практичне застосування зазначених принципів реалізується через системну підготовку аналітичних звітів про результати навчальної діяльності, відвідуваність, дисциплінарну поведінку та динаміку успішності здобувачів освіти, що дозволяє своєчасно виявляти проблемні аспекти освітнього процесу. Використання інструментів прогнозної аналітики забезпечує оцінювання ймовірних результатів навчання, раннє виявлення ризиків академічної неуспішності та обґрунтування коригувальних педагогічних заходів. Аналіз зібраних даних також дає змогу оцінювати ефективність застосовуваних освітніх методик, форм і засобів навчання, визначати їх відповідність поставленим цілям підготовки фахівців. Отримані аналітичні результати слугують інформаційною основою для підтримки адміністрації закладу у плануванні навчального процесу, оптимізації розподілу навчального навантаження, ресурсного забезпечення та прийнятті управлінських рішень, спрямованих на підвищення якості освіти [5].

Правове регулювання інформаційно-аналітичної діяльності в Україні формується сукупністю нормативно-правових актів, які комплексно визначають правові засади збору, обробки, зберігання, використання та захисту інформації в освітніх закладах. Базовим рівнем такого регулювання є конституційні норми, що гарантують право громадян на доступ до інформації, свободу отримання, використання та поширення відомостей, а також забезпечують захист приватного життя і персональних даних. Спеціальне правове поле створюють закони України у сфері інформації, захисту персональних даних, електронних документів та електронного документообігу, кібербезпеки й охорони інтелектуальної власності, які встановлюють вимоги до правомірності обробки даних, відповідальності суб'єктів інформаційних відносин і процедур інформаційної безпеки в освітньому процесі. Окреме значення мають підзаконні нормативні акти, стандарти та відомчі регламенти МВС і ДСНС, що конкретизують порядок ведення електронних баз даних, доступу до службової інформації та використання автоматизованих інформаційно-аналітичних систем у навчальній і адміністративній діяльності.

Наявність розвиненої та ієрархічно вибудуваної правової бази створює передумови для безпечного й легітимного впровадження інформаційно-аналітичних технологій у ВНЗ МВС та ДСНС, забезпечує захист персональних і службових даних, регламентує відповідальність користувачів інформаційних систем та сприяє автоматизації управлінських процесів. Це, у свою чергу, підвищує прозорість прийняття управлінських рішень, ефективність освітньої діяльності та відповідність інформаційно-аналітичних процесів вимогам національного законодавства і міжнародних стандартів.

Інформаційний процес в освітньому середовищі охоплює пошук і збір даних з різних джерел, їх накопичення та зберігання у базах даних і сховищах, подальше опрацювання й аналітичну обробку, передавання отриманих результатів у навчальний процес та забезпечення належного рівня інформаційної безпеки [3, 4]. У специфічних умовах функціонування вищих навчальних закладів МВС і ДСНС реалізація зазначених етапів ускладнюється низкою проблем, зокрема фрагментованістю даних, що

зберігаються в різних інформаційних системах, високим адміністративним навантаженням на викладачів, недостатньою інтеграцією інформаційних ресурсів і складністю персоналізації освітніх програм. Сукупність цих чинників зумовлює потребу в активному впровадженні сучасних інформаційних та інформаційно-аналітичних систем, спрямованих на підвищення якості навчання та ефективності управлінських рішень в освітньому процесі ВНЗ МВС і ДСНС.

Для її вирішення пропонується впровадження інтегрованої інформаційно-аналітичної системи управління освітнім процесом, яка передбачає:

– створення єдиного сховища даних (Data Warehouse) з навчальних, дисциплінарних та адміністративних показників;

– автоматизований збір даних з електронних журналів, систем дистанційного навчання та кадрових модулів;

– використання аналітичних панелей (dashboards) для візуалізації показників успішності, відвідуваності та дисципліни;

– застосування методів прогнозної аналітики для раннього виявлення ризиків академічної неуспішності.

Очікуваними результатами впровадження такої системи є скорочення часу на підготовку звітів, зниження адміністративного навантаження на викладачів, підвищення оперативності управлінських рішень та персоналізація освітніх траєкторій курсантів.

Висновки. Інформаційно-аналітичні технології є ключовим інструментом підвищення ефективності освітнього процесу у ВНЗ МВС та ДСНС України. Їх використання забезпечує автоматизацію збору та аналізу даних, підтримку прийняття управлінських рішень і адаптацію освітніх програм до індивідуальних потреб здобувачів освіти. Практична реалізація інтегрованих ІАТ дозволяє оптимізувати навчально-організаційні процеси, підвищити якість моніторингу успішності та забезпечити ефективне стратегічне управління навчальними закладами.

Література

1. Бех І. М. Інформаційні технології та їх застосування в освіті: навч. посіб. / І. М. Бех. – К., 2020. – 256 с.
2. Ковальчук О. В. Аналітичні інформаційні системи: теорія та практика / О. В. Ковальчук. – Львів, 2019. – 182 с.
3. Петренко С. В. Технології обробки інформації та прийняття рішень / С. В. Петренко. – Харків, 2021. – 214 с.
4. Іваненко Т. А. Інформаційно-аналітичні процеси в управлінні освітою / Т. А. Іваненко. – Київ, 2022. – 198 с.
5. Івануса А. І., Ткачук Р. Л., Маслова Н. О., Ящук В. І., Ткаченко А. М. Методи та моделі управління інформаційною безпекою та кіберзахистом у закладах вищої освіти. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 101–116. DOI: https://doi.org/10.32447/20784643.31.2025.11

Калин Софія Петрівна

здобувач вищої освіти освітнього ступеня «бакалавр» спеціальності «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Галайко Наталія Володимирівна

старший викладач кафедри інформаційних технологій Львівського державного університету внутрішніх справ

ЦИФРОВА КРИМІНАЛІСТИКА В РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Інтенсивне впровадження інноваційних технологій у різні сфери суспільного життя зумовило якісні зміни й у сфері криміналістичної експертизи. Результатом цього процесу стало формування окремої галузі криміналістики – цифрової криміналістики, яка забезпечує

дослідження та використання електронних (цифрових) доказів у кримінальному судочинстві.

Цифрова криміналістична експертиза розглядається як галузь криміналістичної експертизи, зосереджена на аналізі доказів, пов'язаних із комп'ютерами та іншими цифровими пристроями, зокрема мобільними телефонами, смартпристроями, мережевими та інтернет-орієнтованими системами. Вона охоплює процеси ідентифікації, збирання, фіксації, зберігання, аналізу та подання цифрових доказів з метою отримання слідчої інформації та розслідування, у тому числі кіберзлочинів.

Цифрова криміналістика упродовж усього періоду свого становлення пройшла чотири основні етапи розвитку, кожен з яких характеризується специфікою завдань, методів та інструментарію дослідження цифрових доказів.

Перший етап (1985–1995 рр.) має початковий характер і пов'язаний із зародженням цифрової криміналістичної експертизи. На цьому етапі її застосування зводилося переважно до зчитування даних з внутрішніх операційних систем та апаратних засобів персональних комп'ютерів за допомогою спеціалізованих програмних кодів і базових технічних засобів.

Другий етап (1995–2005 рр.) характеризується формуванням та активним розвитком кіберзлочинності, що зумовило необхідність створення ефективних механізмів протидії таким правопорушенням. Саме в цей період у криміналістичній науці формується поняття «розслідування кіберзлочинів», яке згодом стало одним із ключових напрямів діяльності цифрової криміналістики.

Третій етап (2005–2010 рр.) ознаменувався появою складних цифрових моделей розслідування злочинів, орієнтованих на систематизацію процесів збирання, аналізу та оцінювання цифрових доказів. Серед них найбільш поширеною є загальна модель комп'ютерних криміналістичних розслідувань, яка заклала методологічні основи сучасних цифрових експертиз.

Четвертий етап (2010–2022 рр.) пов'язаний з інтенсивним розвитком цифрових технологій, розширенням інформаційного простору та

ускладненням форм злочинної діяльності. У цей період цифрова криміналістика отримала нові напрями розвитку та інструментальні можливості у сфері протидії організованій і транснаціональній злочинності, а також терористичним загрозам.

Масштабна цифровізація діяльності правоохоронних органів України в умовах гібридної агресії зумовила трансформацію цифрової криміналістики на один із ключових інструментів забезпечення національної безпеки та ефективного розслідування злочинів. За таких умов змінюється не лише характер загроз, а й простір їх виникнення, який дедалі більше зміщується в інформаційний, кібернетичний та комунікаційний виміри.

Правоохоронна система, що традиційно ґрунтувалася на матеріально зафіксованих доказах, процесуальних гарантіях та інституційному контролі, стикається з необхідністю переосмислення доказових стандартів у цифровому середовищі. Актуалізуються проблеми легітимності та допустимості цифрових доказів, доступу до них, захисту персональних даних, а також недопущення необґрунтованого втручання у приватне життя.

Цифрова трансформація у сфері правопорядку спрямована як на модернізацію внутрішніх процесів, так і на підвищення спроможності правоохоронних органів оперативно виявляти, запобігати та нейтралізовувати загрози гібридного характеру. Вона охоплює перехід до електронного документообігу, створення інформаційно-аналітичних платформ, упровадження автоматизованих реєстрів, цифрових систем спостереження та вдосконалення міжвідомчої комунікації органів досудового розслідування. У теоретико-правовому аспекті ці процеси потребують оновлення нормативного забезпечення, запровадження ефективних механізмів контролю за використанням цифрових засобів і встановлення юридичної відповідальності за порушення у сфері цифрової діяльності правоохоронних органів. Водночас технологічна модернізація має подвійну природу: з одного боку, вона сприяє зміцненню правопорядку, з іншого — може породжувати нові вразливості у разі недотримання правових процедур або неналежного захисту даних.

Однією з ключових проблем діяльності правоохоронних органів залишається «крихкість» цифрових доказів і ризик визнання їх недопустимими через порушення процедур отримання та фіксації. Показовим у цьому контексті є питання допустимості скріншотів у кримінальному судочинстві, що зумовлено складністю встановлення авторства та зв'язку інформації з конкретною особою, а також високою вразливістю цифрових даних до редагування або видалення. Відсутність чітко визначених вимог до форми й змісту скріншотів зумовлює дискусійність їх віднесення до самостійних електронних доказів, оскільки вони здебільшого виступають електронними копіями первинних цифрових даних. Водночас оцінка таких доказів здійснюється судом з урахуванням обставин конкретної справи на підставі внутрішнього переконання, сформованого в результаті всебічного та безпосереднього дослідження доказової бази.

З метою мінімізації зазначених ризиків правоохоронні органи інтегрують міжнародні стандарти та спеціалізоване програмне забезпечення. Важливе значення у цьому контексті має міжнародний стандарт ISO/IEC 27037:2012, який визначає рекомендації щодо ідентифікації, збору, отримання та збереження потенційних цифрових доказів. Дотримання його положень забезпечує збереження цілісності цифрових даних і формування належної методології їх отримання, що безпосередньо впливає на допустимість доказів у судових та дисциплінарних провадженнях.

Практичну реалізацію зазначених підходів забезпечує використання спеціалізованого програмного забезпечення, зокрема Autopsy та FTK Imager, яке дозволяє створювати дзеркальні копії носіїв інформації, відновлювати видалене електронне листування та аналізувати дані про геолокацію.

Таким чином, ефективність діяльності правоохоронних органів значною мірою визначається рівнем їх технологічного оснащення та здатністю забезпечити автентичність цифрових доказів на всіх етапах — від моменту вилучення до судового розгляду. У зв'язку з цим актуальним є впровадження обов'язкової підготовки слідчих територіальних підрозділів щодо роботи з цифровими слідами відповідно до міжнародних стандартів, а не лише спеціалізованих підрозділів кіберполіції.

Література

1. Бутузов В. М., Користін О. Є. Проблеми збирання електронних доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2022. № 10. С. 627–629. URL: http://www.lsej.org.ua/10_2022/155.pdf
2. Омельченко О. М. та ін. Цифровізація кримінального провадження в Україні: сучасний стан та перспективи розвитку. Київський часопис права. 2022. № 2. С. 132. URL: https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/151/139
3. Корнейко О. В. Виклики та перспективи розвитку цифрової криміналістики в правоохоронній діяльності. Вісник Харківського національного університету внутрішніх справ. 2023. Вип. 2 (101). С. 154–165. URL: https://vca.univd.edu.ua/index.php/vca/article/view/433/451
4. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence : ISO/IEC 27037:2012. URL: https://www.iso.org/standard/44381.html

Коваль Ірина Ігорівна

курсант факультету №1 (з підготовки фахівців для органів досудового розслідування Національної поліції України) Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ПІД ЧАС ВИЯВЛЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ СТАТЕВОЇ СВОБОДИ ТА СТАТЕВОЇ НЕДОТОРКАНОСТІ ОСОБИ

Крізь часову призму кримінальні правопорушення проти статевої свободи та статевої недоторканості особи залишаються одними із найскладніших у виявленні. Оскільки, вказані кримінальні правопорушення є латентними, саме через це потерпілі особи зазвичай не заявляють про вчинення відносно них вказаної категорії злочинів. Злочинці активно слідкують за розвитком сучасних технологій, щоб використовувати їх у своїй протиправній діяльності. Саме тому інформаційно-аналітичне забезпечення відіграє важливу роль у діяльності правоохоронних органів задля швидкого та ефективного розслідування.

У 2022 році американські вчені проводили дослідження застосування аудіоаналітики в транспортних засобах. Суть цього дослідження полягає у вмонтуванні в систему автомобіля датчика, який розрізняє поведінку осіб, що перебувають в транспортному засобі. Зазначений датчик функціонує на основі алгоритмів машинного навчання та здатний ідентифікувати звуки, що можуть свідчити про загрозу життю чи здоров'ю особи, зокрема крики, плач, прояви паніки або використання нетипових фраз. У разі фіксації таких звукових маркерів система автоматично

формує повідомлення та передає його до відповідних диспетчерських служб або правоохоронних органів. Результати експериментального дослідження засвідчили високу ефективність запропонованої технології, оскільки чутливість виявлення тривожних звуків у змодельованих умовах сягала 91 %, що підтверджує доцільність використання аудіоаналітики як елементу сучасного інформаційно-аналітичного забезпечення правоохоронної діяльності [1]. Запровадження аудіоаналітики в нашій державі, набагато спростила б проблематику виявлення кримінальних правопорушень проти статевої свободи та статевої недоторканості особи і не тільки їх.

Сучасні міжнародні дослідження демонструють ефективність застосування мультимодальної аналітики у правоохоронній системі. Мультимодальна аналітика поєднує в собі одночасний аналіз відео, аудіо та текстових повідомлень, це допомагає створити картину поведінки особи у реальному часі та виявити потенційні ознаки протиправної поведінки. Використання таких засобів дозволяє автоматично ідентифікувати незвичні дії, прояви страху, паніку або агресію, а також інтегрувати текстові повідомлення та інші дані для формування аналітичного висновку. такі підходи здатні підвищити точність та оперативність реагування підрозділів Національної поліції України, зменшити ризик упущення критичних сигналів і забезпечити більш ефективну підтримку слідчих дій. Мультимодальна аналітика виступає інноваційним інструментом, що інтегрує різні джерела інформації і дозволяє перетворювати великі обсяги даних у практично значущі аналітичні висновки для оперативного реагування [2].

Згідно з міжнародними дослідженнями, інтеграція AI і Big Data у правоохоронну діяльність дозволяє не лише обробляти великі обсяги нерструктурованої інформації, а й автоматично виділяти критично важливі патерни, що суттєво підвищує ефективність превентивних та оперативних заходів. Використання автоматизованих систем дозволяє об’єднювати дані з різних джерел, зокрема із соціальних мереж, для виявлення прихованих зв’язків між підозрілими особами та потенційними жертвами [3]. Застосування штучного інтелекту та аналізу великих даних

підвищує точність і швидкість розкриття кримінальних правопорушень проти статевої свободи та статевої недоторканості особи.

Отже, впровадження в діяльність підрозділів Національної поліції України аудіоаналітики, мультимодальної аналітики та систем ШІ для обробки великих баз даних, суттєво підвищить ефективність інформаційно-аналітичного забезпечення у виявленні кримінальних правопорушень проти статевої свободи та статевої недоторканості особи. Такі підходи дозволяють швидко виявляти латентні злочини, своєчасно реагувати на потенційні загрози та ефективно розслідувати вказані кримінальні правопорушення.

Література

1. F. Al-Turjman, M. Abujayyab, M. Hammoudeh. Audio Analytics in Autonomous Vehicles to Detect Human Trafficking Indicators. arXiv preprint, 2022. Електронний ресурс URL: 10.48550/arXiv.2209.04071 (Дата звернення: 14.12.2025)
2. Towards AI Driven Policing: Interdisciplinary Knowledge Discovery from Police Body Worn Camera Footage (2025) Електронний ресурс URL: [2504.20007] Towards AI-Driven Policing: Interdisciplinary Knowledge Discovery from Police Body-Worn Camera Footage (Дата звернення: 14.12.2025)
3. Europol. AI and Policing: How Artificial Intelligence Supports Law Enforcement. 2024 . Електронний ресурс URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf (Дата звернення 14.12.2025)

Кривко Олена Вікторівна

курсантка навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

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

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА АНАЛІТИЧНИХ ПЛАТФОРМ У РОБОТІ ПОЛІЦІЇ

Цифровізація правоохоронної сфери є ключовим чинником модернізації Національної поліції України, оскільки дає можливість значно підвищити ефективність оперативно-службової діяльності, швидкість реагування та якість прийняття рішень. Перехід до цифрових інструментів підтримує курс держави на електронне врядування, а також відповідає викликам воєнного стану, який потребує швидкого обміну даними, прогнозування ризиків та виявлення загроз у реальному часі. Сучасні цифрові рішення дозволяють формувати більш комплексну систему безпеки, яка охоплює аналітику, превенцію, комунікацію, реагування та криміналістичне забезпечення.

Одним із пріоритетних напрямів розвитку є впровадження аналітичних платформ кримінального аналізу, що використовуються для систематизації великих масивів даних про правопорушення, оперативну обстановку та поведінкові моделі злочинців. Такі системи забезпечують можливість застосування інструментів кримінального профайлінгу, геоінформаційного аналізу (відстеження кримінальних «гарячих точок») та статистичного прогнозування. У підрозділах кримінального аналізу активно застосовуються системи типу i2 Analyst's Notebook, ESRI ArcGIS та інші рішення, що дозволяють інтегрувати інформацію з різних джерел – від внутрішніх баз поліції до відкритих реєстрів та OSINT-даних.

Внаслідок цього підвищується якість планування операцій, швидкість виявлення кримінальних зв'язків і ефективність розкриття злочинів [1, с. 537].

Значну роль у цифровізації поліції відіграють національні інформаційні системи, такі як Єдиний облік, автоматизовані бази даних про транспорт, розшук, зброю та осіб, що перебувають під слідством чи мають обмеження у правовому статусі. Інтеграція цих баз забезпечує можливість швидкого доступу до релевантної інформації під час патрулювання, оформлення матеріалів чи встановлення особи [2, с. 63]. Для патрульних поліцейських важливими інструментами стали мобільні додатки, планшети та термінали, які дозволяють проводити перевірки на місці, фіксувати правопорушення та передавати дані до централізованих систем без затримок.

Окремим напрямом розвитку є впровадження цифрових технологій відеофіксації, що включає нагрудні відеокамери, камери патрульних автомобілів, системи відеоаналітики та муніципальні відеонагляди. Відеоаналітичні комплекси, оснащені алгоритмами розпізнавання номерних знаків, облич або нестандартної поведінки, дозволяють оперативно виявляти транспортні засоби, що перебувають у розшуку, осіб, підозрюваних у злочинах, або небезпечні ситуації у місцях масового перебування. Такі системи виступають не лише інструментом доказування, а й важливим превентивним засобом, що зменшує рівень правопорушень завдяки постійному моніторингу.

У роботі підрозділів кіберполіції цифрові технології є основою практично всіх процесів. Використовуються спеціалізовані аналітичні комплекси для моніторингу мережі, відстеження криптовалютних транзакцій, аналізу darknet-ресурсів та виявлення шкідливих програм. Поєднання інструментів OSINT, аналізу цифрових слідів та штучного інтелекту дає можливість швидко встановлювати зловмисників, прогнозувати кібератаки та ідентифікувати джерела інформаційних операцій [3, с. 61].

В умовах повномасштабної війни особливої ваги набули системи ситуаційної обізнаності поліції. Завдяки інтеграції даних від ДСНС, Збройних Сил України, місцевих органів влади та громадянських

платформ (наприклад, «Дія») забезпечується комплексне бачення загальної безпекової ситуації. Такі системи підтримують координацію сил під час ліквідації наслідків ракетних ударів, охорони громадського порядку, евакуації та роботи блокпостів [4, с. 235].

Попри значні досягнення, існує низка проблем, що стримують повноцінне використання цифрових та аналітичних технологій у поліції. Серед них – фрагментарність інформаційних систем, недостатня інтегрованість між міністерствами та відомствами, потреба у висококваліфікованих аналітиках і програмістах, брак фінансування та залежність від іноземного програмного забезпечення. Також актуальними є питання захисту персональних даних, кіберзахисту державних реєстрів і мінімізації ризиків витоку службової інформації.

Перспективи розвитку цифрових технологій у Національній поліції України пов'язані з подальшою інтеграцією аналітичних платформ, створенням єдиної системи даних сектору безпеки, впровадженням національного програмного забезпечення, розвитком штучного інтелекту та big data. Очікується, що у найближчі роки буде посилено розвиток ситуаційних центрів, аналітичних лабораторій та систем автоматичного прогнозування криміногенної ситуації. Діджиталізація стане основою підвищення ефективності поліцейської діяльності, забезпечуючи швидкість, прозорість та високий рівень професійної взаємодії.

Література

1. Макаліш Б.Д. Використання сучасних досягнень у сфері інформаційних технологій діяльності національної поліції. The 9 th International scientific and practical conference «Scientific achievements of contemporary society»(April 4-6, 2025) Cognum Publishing House, London, United Kingdom. 2025. 537 С.
2. Жмуровська К. Р., Д. О. Грищенко. Роль сучасних технологій у розкритті та розслідуванні злочинів: виклики та перспективи для Національної поліції України. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали наук.-практ. конф.(м. Львів, 22 груд. 2023 р.). Львів: ЛьвДУВС, 2024.С. 62-64.

3. Жученко О. Д. Вплив сучасних інформаційних технологій на діяльність правоохоронних органів: основні тенденції та ризики. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. С. 59-65.
4. Будник Л. А., О. Г. Ронська, В. І. Будник. Застосування цифрових технологій при розслідуванні економічних правопорушень. Наукові заходи Юридичного факультету Західноукраїнського національного університету. 2023. С. 234-236.

Кулешник Тарас Яркович

викладач кафедри менеджменту мистецтва Львівської національної академії мистецтв

Кулешник Оксана Ігорівна

старший викладач кафедри менеджменту мистецтва Львівської національної академії мистецтв

ОСОБЛИВОСТІ ПОЛІТИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАКЛАДАХ ОСВІТИ

Штучний інтелект (ШІ) відкриває значні можливості для оновлення та розвитку освітнього процесу. Водночас його впровадження має бути зваженим, продуманим і послідовним. Обираючи інструменти ШІ, заклад освіти повинен враховувати їх відповідність освітнім цілям, безпеку персональних даних учасників освітнього процесу, рівність доступу для всіх здобувачів освіти, дотримання принципів академічної доброчесності, а також ризики надмірної залежності від технологій, що може негативно впливати на розвиток критичного мислення й творчих здібностей учнів.

Вибір інструментів штучного інтелекту.

У межах автономії заклад освіти самостійно визначає цифрові платформи, сервіси та інструменти, які доцільно використовувати в освітньому процесі. Під час відбору систем ШІ педагогічним колективам варто звертати увагу на такі аспекти:

– основне призначення інструменту (навчальна діяльність, підтримка інклюзії, управління освітнім процесом, професійний розвиток педагогів);
– принципи збору та використання даних;
– відсутність зв'язків із країною-агресором;
– зручність інтерфейсу та наявність україномовної версії;
– можливість роботи з запитами українською мовою;
– умови безоплатного або платного використання;
– необхідність створення облікового запису;
– наявність механізмів захисту від небезпечного контенту;
– вікові обмеження для користувачів;
– сумісність із різними пристроями та платформами;
– доступність технічної підтримки;
– оприлюднення політики конфіденційності;
– умови щодо авторських прав на створений контент.

Після аналізу зазначених характеристик важливо оцінити педагогічну доцільність використання ШІ, зокрема його здатність:

– відповідати освітнім цілям і очікуваним результатам навчання;
– розвивати аналітичне та критичне мислення;
– забезпечувати якісний формувальний зворотний зв'язок;
– враховувати індивідуальні освітні потреби учнів;
– підтримувати принципи інклюзивності;
– виконувати різні освітні функції (створення контенту, оцінювання, рекомендації);
– інтегруватися з наявними технічними рішеннями закладу;
– бути доступним для всіх здобувачів освіти незалежно від їх соціального становища.

Політика відповідального використання ШІ.

Для безпечного й ефективного застосування штучного інтелекту доцільно запровадити комплексний механізм управління, що передбачає:

– відповідність інструментів чинному законодавству;

– постійний моніторинг використання ШІ та аналіз результатів;
– чіткий порядок реагування на етичні та правові інциденти.

Ці положення мають бути закріплені у внутрішніх нормативних документах закладу освіти та схвалені педагогічною радою або іншим органом управління. Зокрема, вони можуть включати такі принципи:

– цільове застосування ШІ виключно в освітніх цілях із дотриманням цінностей поваги, інклюзії та доброчесності;
– законне та прозоре збирання й обробку персональних даних;
– недопущення введення до систем ШІ будь-якої конфіденційної інформації;
– відповідальність педагогів за вибір і використання сторонніх інструментів;
– критичну перевірку результатів, згенерованих ШІ, для запобігання упередженості та дезінформації;
– заборону створення чи поширення шкідливого, маніпулятивного або образливого контенту;
– використання ШІ як допоміжного інструменту, а не заміни самостійної роботи учнів;
– обов'язкове зазначення факту використання ШІ під час створення навчальних матеріалів або виконання робіт.

Права та обов'язки педагогічних працівників.

Педагогічні працівники мають право добирати інструменти ШІ для своєї професійної діяльності за умови дотримання загальної політики. Вони зобов'язані:

– застосовувати ШІ доречно та відповідально;
– використовувати його для розвитку в здобувачів умінь аналізу, аргументації та самостійного мислення;
– навчати здобувачів освіти безпечного й етичного використання ШІ;
– постійно вдосконалювати власні цифрові компетентності;
– сприяти підвищенню обізнаності здобувачів і батьків щодо можливостей та обмежень штучного інтелекту.

У межах освітнього процесу штучний інтелект може використовуватися за різними педагогічними сценаріями з урахуванням мети навчання, вікових особливостей учнів та специфіки навчальних предметів. Доцільним є застосування ШІ як інструменту підтримки та розширення можливостей навчання, а не як заміни діяльності педагога або самостійної роботи здобувача освіти.

ШІ може використовуватися для створення дидактичних матеріалів, підготовки завдань різного рівня складності, добору прикладів, тренувальних вправ, а також для аналізу типових помилок і навчальних труднощів здобувачів. Водночас педагог зобов'язаний здійснювати експертний контроль за змістом і якістю матеріалів, згенерованих із використанням ШІ.

Застосування інструментів штучного інтелекту повинно відповідати віковим, психологічним та пізнавальним особливостям здобувачів освіти.

Інструменти штучного інтелекту можуть використовуватися для підтримки формувального оцінювання, аналізу навчального прогресу здобувачів освіти та надання індивідуальних рекомендацій. Автоматизовані результати, отримані за допомогою ШІ, не можуть бути єдиною підставою для виставлення підсумкових оцінок.

Остаточне рішення щодо оцінювання навчальних досягнень приймає педагог, який несе відповідальність за об'єктивність і справедливість оцінювання. Здобувачів освіти також повинні бути поінформовані про використання ШІ в оцінювальних процедурах.

Штучний інтелект може бути ефективним інструментом підтримки інклюзивної освіти шляхом адаптації навчальних матеріалів, створення альтернативних форматів подання інформації та індивідуалізації навчання.

Використання ШІ для здобувачів освіти з особливими освітніми потребами здійснюється з урахуванням рекомендацій фахівців і не замінює педагогічної, психологічної чи корекційної підтримки.

Заклад освіти забезпечує формування культури відповідального, етичного та безпечного використання ШІ серед усіх стейкхолдерів освітнього процесу. З цією метою можуть організовуватися інформаційно-просвітницькі заходи, тематичні уроки, виховні години, семінари та обговорення.

Особлива увага приділяється питанням цифрової грамотності, критичного оцінювання інформації, дотримання авторського права та усвідомлення відповідальності за результати діяльності із застосуванням ШІ.

Політика використання штучного інтелекту в закладі освіти підлягає регулярному перегляду з урахуванням розвитку технологій, змін у законодавстві та результатів практичного застосування.

Адміністрація закладу освіти забезпечує моніторинг використання ШІ, збір зворотного зв'язку від учасників освітнього процесу та своєчасне оновлення внутрішніх нормативних документів.

Література

1. Концепція розвитку штучного інтелекту в Україні. (2020). Розпорядження Кабінету міністрів України №1556-р від 2 грудня 2020 року. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
2. Лубко, Д. В., Шаров, С. В. (2019). Методи та системи штучного інтелекту: навч. посіб. Розділ 1. Загальні поняття про штучний інтелект. http://eprints.mdpu.org.ua/id/eprint/5295/
3. Овчарук, О. В., Іванюк, І. В., Гриценчук, О. О., Малицька, І. Д. (2023). Результати он лайн-опитування «Готовність і потреби вчителів щодо використання цифрових засобів та ІКТ в умовах війни: 2023». Аналітичний звіт. ІЦО НАПН України. https://doi.org/10.13140/RG.2.2.25529.34402
4. Шишкіна, М., & Носенко, Ю. (2023). Перспективні технології з елементами штучного інтелекту для професійного розвитку педагогічних кадрів. Фізико-математична освіта, 38(1), 66–71. https://doi.org/10.31110/2413-1571-2023-038-1-010

Куликовська Владислава Олександрівна

здобувачка освіти магістратури спеціальності 124 «Системний аналіз» Одеського державного університету внутрішніх справ

Пядишев Володимир Георгійович

професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, доктор юридичних наук, професор

ШТУЧНИЙ ІНТЕЛЕКТ У ПУБЛІЧНОМУ ТА КОРПОРАТИВНОМУ УПРАВЛІННІ: ПРАВОВІ Й ЕТИЧНІ АСПЕКТИ

Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) трансформує підходи до організації управлінської діяльності як у публічному секторі, так і в корпоративному середовищі. Інтелектуальні системи дедалі активніше впливають на процеси прийняття рішень, аналітичне забезпечення управління, прогнозування ризиків, розподіл ресурсів і комунікацію з громадянами та стейкхолдерами. Однак упровадження ШІ, попри очевидні переваги, супроводжується комплексом правових, етичних та соціальних викликів, що потребують наукового осмислення та відповідного нормативного врегулювання.

Насамперед постає проблема визначення меж відповідальності за рішення, ухвалені із застосуванням алгоритмічних систем. У сфері публічного управління ця проблема ускладнюється вимогами законності, прозорості, підзвітності й недискримінаційності, які є фундаментальними принципами функціонування державної влади. Натомість корпоративні структури стикаються з ризиком порушення прав споживачів, недобросовісністю автоматизованих рішень, витоками даних та підривом довіри з боку партнерів і клієнтів. В обох секторах залишаються невирішеними питання алгоритмічної упередженості, належного захисту персональних даних, можливості аудиту й контролю інтелектуальних систем.

Правові режими, що регламентують використання ШІ, перебувають на стадії формування, а міжнародні стандарти лише окреслюють

загальні підходи до етичного застосування інтелектуальних технологій. Відсутність усталених дефініцій, єдиних підходів до сертифікації та оцінювання ризиків, а також механізмів зовнішнього контролю ускладнює впровадження ШІ на практиці. Це створює ризики для прав людини, рівності доступу до послуг, справедливості прийняття рішень і функціонування демократичних інститутів. Таким чином, актуалізується потреба у комплексному дослідженні правових вимірів та етичних орієнтирів інтеграції ШІ в управлінські системи, що стане основою для вироблення ефективних нормативних стратегій та інституційних механізмів його безпечного застосування.

Подальший розвиток систем управління пов'язаний із тим, що алгоритми ШІ дедалі частіше перебирають на себе значну частину аналітичних і прогностичних функцій, які раніше виконувались виключно людиною. У корпоративному управлінні ШІ уже продемонстрував здатність оптимізувати планування, розподіл ресурсів, управління ризиками, бюджетування та контроль виконання проєктів, що підтверджують дослідження В.М. Василенка та Т.А. Вакалюк [1, с. 63]. Використання методів машинного навчання, прогнозної аналітики та інтелектуальної обробки даних дає змогу виявляти приховані закономірності, формувати більш точні моделі проєктної діяльності та забезпечувати зменшення невизначеності в управлінських рішеннях [1, с. 65]. За таких умов ШІ розглядається не як замінник менеджера, а як інструмент інтелектуального підсилення його професійної діяльності.

У публічному управлінні застосування ШІ пов'язане, насамперед, із аналітикою великих масивів даних, оцінюванням суспільних потреб, прогнозуванням соціально-економічних тенденцій, а також автоматизацією адміністративних процедур. Д.М. Дриньов, К.П. Войтех і Р.Р. Тимошенко підкреслюють, що в органах державного управління та секторі безпеки алгоритмічні системи сприяють оперативнішому опрацюванню інформації та моделюванню альтернативних сценаріїв, але водночас підвищують ціну можливих помилок, особливо в умовах кризових ситуацій [2, с. 75]. Тому до впровадження ШІ у публічну сферу висуваються підвищені вимоги щодо забезпечення прозорості, підзвітності та можливості зовнішнього контролю над алгоритмічними рішеннями [2, с. 77].

Значною мірою спільною для публічного та корпоративного секторів є проблема визначення суб'єкта відповідальності за наслідки використання ШІ. О.А. Дороніна та В.О. Дядін акцентують, що у випадку автоматизованого прийняття управлінських рішень стає складнішим установити, хто саме несе відповідальність – розробник програмного продукту, його замовник чи конкретний користувач, який спирається на рекомендації системи [3, с. 55]. Така ситуація зумовлює необхідність деталізованих правових норм, які б чітко окреслювали обов'язки й межі відповідальності кожного учасника життєвого циклу системи ШІ: від розроблення та тестування до експлуатації й модернізації [3, с. 57].

Паралельно з цим постає питання захисту даних та кібербезпеки. Використання інтелектуальних систем пов'язане з обробкою значних обсягів інформації, у тому числі персональних даних, комерційної таємниці, стратегічно важливих відомостей щодо функціонування органів державної влади або бізнес-структур. Недостатній рівень захисту може призвести до витоків, маніпуляцій чи несанкціонованого доступу, що створює загрозу не лише для окремих суб'єктів, а й для суспільної безпеки в цілому.

Окремої уваги потребує проблема алгоритмічної упередженості. Алгоритми, навчені на нерепрезентативних чи викривлених масивах даних, можуть відтворювати та посилювати дискримінаційні практики в таких сферах, як кредитування, підбір персоналу, оцінювання благонадійності, надання соціальних послуг чи доступ до публічних сервісів. Г.М. Калач, О.І. Шпак та А.В. Круглянко справедливо звертають увагу на те, що подолання цих ризиків вимагає впровадження спеціальних процедур перевірки моделей, регулярного моніторингу їх результатів, а також застосування механізмів пояснюваності та верифікації алгоритмічних рішень [4].

Не менш важливим є етичний вимір використання ШІ. Йдеться передусім про збереження принципу людського контролю над критично значущими рішеннями. Хоча інтелектуальні системи здатні значною мірою автоматизувати рутинні операції, повне усунення людини з процесу прийняття рішень може призвести до розмивання персональної

відповідальності, зниження рівня довіри до інституцій та легітимності владних і корпоративних рішень. Тому оптимальною видається модель «людина–в–циклі», за якої інструменти ШІ доповнюють професійну компетентність управлінця, але не підмінюють собою його волевиявлення й моральний вибір [1, с. 64].

У наукових роботах, присвячених використанню ШІ в управлінні, простежується спільна тенденція: технічні можливості інтелектуальних систем уже випереджають рівень правового та етичного регулювання їх застосування. У публічному секторі це проявляється у ризиках порушення прав людини, непрозорості алгоритмічних рішень, ускладненні доступу до ефективних механізмів оскарження. У корпоративному середовищі – у підвищеному ризику зловживань із даними, прийнятті рішень, орієнтованих виключно на економічну доцільність без належного урахування соціальних наслідків, а також у потенційному знеціненні професійної автономії працівників [3, с.57; 4].

Узагальнюючи результати проаналізованих досліджень, можна стверджувати, що формування правових і етичних орієнтирів використання ШІ має комплексний характер і повинно охоплювати кілька взаємопов'язаних напрямів. По-перше, йдеться про розроблення стандартів алгоритмічної прозорості, які б забезпечували можливість відтворення логіки прийняття рішень системою ШІ та доступність інформації про основні принципи її функціонування. По-друге, особливої уваги набуває запровадження аудиту систем ШІ – як внутрішнього, так і зовнішнього – для регулярної перевірки коректності моделей, відповідності їх правовим нормам та етичним стандартам. По-третє, необхідним є встановлення чітких меж відповідальності розробників, замовників і користувачів інтелектуальних систем, що дозволить уникнути нівелювання відповідальності в технологічному ланцюгу. По-четверте, ключовою залишається вимога забезпечення належного захисту даних і кібербезпеки, без чого будь-які переваги цифрової трансформації втрачають реальну цінність. По-п'яте, важливою складовою правового регулювання є оцінка впливу алгоритмів на права людини, зокрема вразливих груп, а також запровадження процедур превентивного аналізу ризиків. Нарешті,

суттєвого значення набуває розроблення етичних кодексів застосування ШІ у публічному та корпоративному управлінні, які б конкретизували ціннісні орієнтири діяльності органів влади та бізнесу в умовах цифровізації.

Перспективним напрямом подальших досліджень і практичних розробок є формування моделей співуправління, у яких системи ШІ та управлінці здійснюють взаємодоповнювальні функції, забезпечуючи більш обґрунтовані, справедливі та прогнозовані управлінські рішення. У цьому контексті особливого значення набуває розвиток нормативних механізмів, що регламентують використання ШІ у критичних секторах – обороні, фінансах, охороні здоров'я, сфері зайнятості та соціального захисту. Саме поєднання технологічних інновацій із розвинутим правовим регулюванням та усталеними етичними стандартами створює підґрунтя для того, щоб штучний інтелект став не джерелом додаткових загроз, а потужним інструментом зміцнення демократичних інститутів, підвищення ефективності управління та забезпечення стійкого розвитку як публічної влади, так і корпоративного сектору.

Література

1. Василенко В.М., Вакалюк Т.А. Штучний інтелект в управлінні проєктами: аналіз сучасних досліджень та перспектив розвитку. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2024. Т. 35 (74), № 4. С. 60-67.
2. Дриньов Д.М., Войтех К.П., Тимошенко Р.Р. Штучний інтелект у процесі прийняття та реалізації управлінських рішень. Таврійський науковий вісник. Серія: Економіка. 2023. Вип. 18. С. 74-79.
3. Дороніна О.А., Дядін В.О. Використання штучного інтелекту у процесі прийняття управлінських рішень: ризики та переваги. Економіка і організація управління. 2024. № 3 (55). С. 53-61.
4. Калач Г.М., Шпак О.І., Круглянко А.В. Штучний інтелект в управлінні: автоматизація процесів та прийняття рішень. Соціальний розвиток: економіко-правові проблеми. 2025. № 5. DOI: 10.70651/3083-6018/2025.5.15.

Куліченко Єва Олександрівна

курсантка факультету №2 Львівського державного університету внутрішніх справ

Рудий Тарас Володимирович

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

СТВОРЕННЯ НЕСКІНЧЕННОГО WEB-СЛАЙДЕРА

Створення карусельних слайдерів з ефектом нескінченності який є одним із найпопулярніших інтерактивних компонентів для подання контенту, навігації, а також покращення досвіду користувача. Популярні застосунки, а саме Swiper.js та Slick.js, через недостатню кастомізацію та зовнішню залежність не завжди задовольняють потреби Web-проєкту.

HTML, CSS, JavaScript – це базові мови Web-проєктування, тому обмеження у реалізуванні проєкту лише їхнім використанням є легшим у супроводі та інтегруванні.

Матеріали та методи. Опис технологічного стеку подано у табл. 1.

Таблиця 1.

Опис технологічного стеку

Технологія	**Версія**	**Призначення**
HTML5	ES2020	Структура
SCSS	4.x	Стилізація
JavaScript	ES6+	Логіка анімацій
CSS 3D Transforms	-	3D-ефекти
Intersection Observer	Level 2	Відстежування

Структура коду.

1. HTML розмічування.

Слайдер розміщено в секції, слайди мають внутрішній контейнер для структури, яка забезпечує більшу адаптивність та варіативність

реалізування дизайну, а також блок зображення та два блоки для тексту. Також ця структура дозволяє додавати довільний контент та кількість слайдів, які автоматично стилізуються за допомогою класів.

2. SCSS основні класи.

У SCSS реалізовується дизайн центрального елементу та секції і може легко змінюватись за потреби.

3. Структуру нескінченного слайдера та алгоритм анімації повністю реалізовано мовою JavaScript. Основна логіка нескінченності базується на буферизації масиву, який створює для користувача відчуття нескінченності. Оригінальний масив (за приклад взято 7 слайдів) копіюється відповідну кількість разів, яка вказується у REPEAT_COUNT, потрібно раціонально підбирати значення для запобігання перевантаженню системи, що може гальмувати анімації та сайт. Діаграму візуалізування процесу копіювання подано на рис.1.

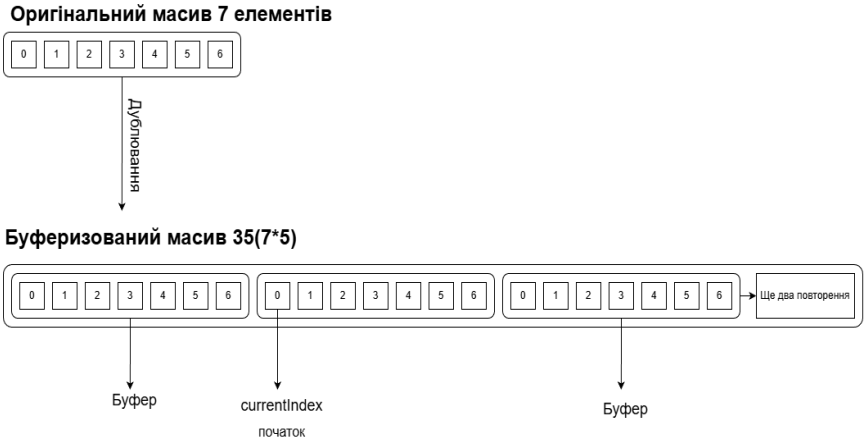

Рис. 1. Візуалізація процесу копіювання

4. Математика буферизації.

currentIndex відповідає за індекс в масиві, стартова позиція визначається формулою:

*currentIndex = (REPEAT_COUNT * originalCount) / 2*

де: *originalCount* –кількість слайдів у оригіналі. Це забезпечує початок з середини масиву, задля дотримання "безпечної зони" де є запас слайдів з кожної сторони. Також задається safeDistance (кількість копій до кінця, під час якої почнеться нормалізація), формулою:

*safeDistance = originalCount * x*

де *x* – потрібна кількість циклів.

Відстані до краю визначається перевіркою виконання умови:

if (distanceFromStart < sefeDistance || distanseFromEnd < sefeDistance)

де:

distanceFromStart = currentIndex, distanseFromEnd = totalItems -1 – currentIndex

Якщо умова виконується, тоді спочатку вимикається анімація, а також починається розрахунок позиції у безпечній зоні. Для цього потрібно, насамперед, визначити позицію, яка відповідає елементу в оригінальному масиві (7 елементів) за формулою:

$$positionInCycle=((currentIndex \% originalCount)+originalCount)\%originalCount$$

Потім розраховується новий *currentIndex* за формулою:

currentIndex = (totalItems / 2) - (originalCount / 2) + positionInCycle

Тепер на екрані користувача слайд має новий *currentIndex*, який знаходиться у безпечній зоні та відповідає вмісту того ж слайду який мав побачити користувач. Для користувача візуально нічого не змінюється – активний слайд і його оточення залишаються незмінними. Візуалізація нормалізацій подана на рис. 2.

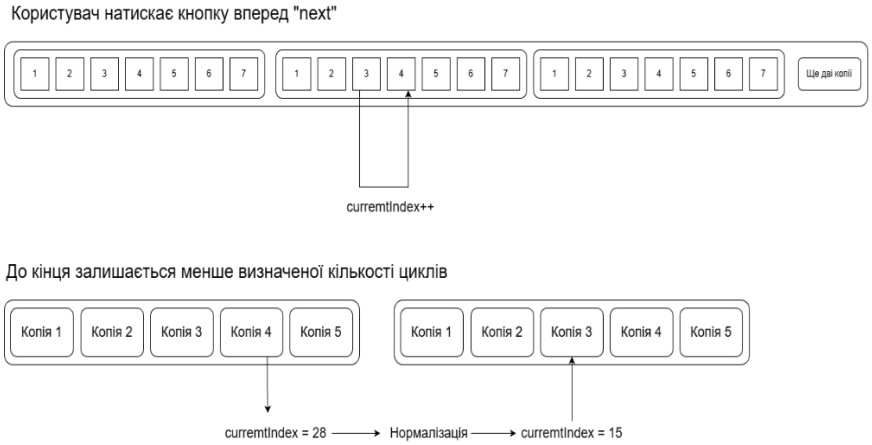

Рис. 2. Візуалізація нормалізації

5. Стилізація (JavaScript).

Застосування стилю відбувається у залежності від положення елементу, і реалізовано мовою *JavaScript* та подані на рис. 3.

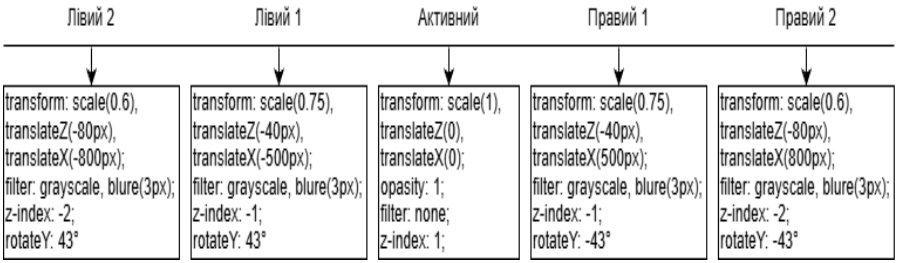

Рис. 3. Діаграма візуалізації підсумків стилю.

Реалізування тривимірного простору та перспективи. Для створення ефекту 3D у розробленому слайдері використано комплексне поєднання властивостей *CSS Transforms Module Level 2*. Основу 3D-сцени складають три ключові параметри:

1. Перспектива (*Perspective*) задає відстань між площиною екрана (*z=0*) та точкою огляду користувача. Це створює глибину, де елементи, які віддаляються вздовж осі *Z*, пропорційно зменшуються [1].

2. Просторові переміщення (*TranslateZ*) переміщують об'єкти вздовж оптичної осі глядача. У проєкті це використано для винесення активного слайда на передній план та візуального віддалення сусідніх елементів, що підсилює ефект ієрархії контенту [2].
3. Осьове обертання (*RotateY*) дозволяє розгортати слайди навколо вертикальної осі. У поєднанні з властивістю *perspective-origin* це формує ефект *"vanishing point"* (точки сходу), що робить перехід між слайдами схожим на руху елементів у реальному просторі [3].

Таке поєднання дозволяє застосування матриць трансформації (*matrix3d*), для плавного відтворення анімації при високих частотах оновлення екрана [4], а також створює необхідний 3D ефект.

Адаптивність слайдера. Для тестування вигляду на різних пристроях використано "Інструмент розробника" у браузері *Chrome* та особистий телефон. Результати подано на рис.4-8. Слайдер було наповнено інформацією, яка не містить комерційної таємниці. Підсумок відображення слайдера на різних пристроях подано у табл. 2.

Таблиця 2.

Підсумкова таблиця відтворення слайдера на різних пристроях

Ширина, px	**Кількість видимих слайдів**	**Результат**
2560	8	Оптимально
1920	7	Оптимально
1536	5	Добре
768	3	Задовільно
390	1, видимі краї сусідніх слайдів	Добре

Рис.4. Вигляд слайдера на моніторі шириною 2560px.

Рис. 5. Вигляд слайдера на моніторі шириною 1920px.

Рис. 6. Вигляд слайдера на моніторі шириною 1536px.

Рис. 7. Вигляд слайдера на моніторі шириною 768px

Рис. 8. Вигляд слайдера на моніторі шириною 390px

Висновки. Розроблено проєкт *Web*-сторінки з адаптивним слайдером, який добре кастомізується та коректно працює на різних пристроях (включаючи мобільні) і за різної роздільної спроможності екрана. Такий результат сприяє покращенню досвіду користувача, підвищенню якості дизайну та зручності навігації *Web*-сторінками.

У процесі розроблення використано лише *HTML*, *CSS* та *JavaScript* без залучення сторонніх бібліотек, що повністю усуває залежності від зовнішніх застосунків і забезпечує просте інтегрування слайдера у довільні *Web*-проєкти. Понад те, таке реалізування спрощує майбутній супровід проєкту, оптимізацію продуктивності та можливість розширення функціоналу відповідно до політики проєкту.

Література

1. perspective – CSS: Cascading Style Sheets. MDN Web Docs. 2024. URL: https://developer.mozilla.org/en-US/docs/Web/CSS/perspective (дата звернення: 15.12.2025).
2. Using CSS transforms. MDN Web Docs. 2024. URL: https://developer.mozilla.org/en-US/docs/Web/CSS/Guides/Transforms/Using (дата звернення: 14.12.2025).
3. CSS 3D Transforms. W3Schools. URL: https://www.w3schools.com/css/css3_3dtransforms.asp (дата звернення: 13.12.2025).
4. Atkins T., Etemad E. J., Baron D. CSS Transforms Module Level 2. W3C Working Draft. 2024. URL: https://www.w3.org/TR/css-transforms-2/ (дата звернення: 15.12.2025).

Курилишин Денис Іванович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОРД ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

В умовах трансформації безпекового середовища України та активізації оперативної злочинності зростає роль підвищення ефективності оперативно-розшукової діяльності органів сектору безпеки і оборони. Сучасні організовані злочинні угруповання характеризуються високою адаптивністю, конспіративністю, використанням інформаційних технологій і міжрегіональними зв'язками, що зумовлює необхідність

застосування системного інформаційно-аналітичного підходу. Результативність ОРД безпосередньо залежить від повноти, достовірності та своєчасності інформації, а також рівня її аналітичної обробки. У цьому контексті інформаційно-аналітичне забезпечення виступає ключовим елементом ОРД, який забезпечує прийняття обґрунтованих оперативних і управлінських рішень у протидії організованій злочинності.

Оперативно-розшукова інформація, як вказує О. М. Бандурка, являє собою отримані оперативними підрозділами передбаченими законом гласними і негласними методами фактичні дані, що мають безпосереднє або перспективне (потенційне) значення для вирішення завдань оперативно-розшукової та кримінально-процесуальної діяльності. Така інформація, зауважують А. С. Овчинський і В. С. Овчинський, відображає не тільки ті явища, події, обставини, зміни у середовищі, які виникають в результаті злочинів, але й широке коло явищ і обставин, подій, що впливають на злочинну поведінку окремих осіб. До оперативно-розшукової інформації слід віднести фактичні дані, що мають безпосереднє або перспективне значення для вирішення завдань ОРД, які одержані гласними і негласними методами з різноманітних джерел або отримані в ході аналітичного опрацювання первинних відомостей. Джерела інформації також пов'язують із обізнаними особами, документами, засобами безпровідного і провідного зв'язку, електронними системами обробки інформації та іншими обставинами. Особливу увагу слід приділити інформації, отриманої з матеріальних джерел, яка формується в при застосуванні оперативно-технічних засобів [1, с. 9].

Законом України «Про національну безпеку» врегульовано й поняття сили безпеки – це правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту й інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України (п. 17 ст. 1). Сили оборони в Законі України «Про національну безпеку» визначені як Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні й розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які

Конституцією та законами України покладено функції із забезпечення оборони держави (п. 18 ст. 1). Сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складників: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки (ч. 1 ст. 12) [2, с.42].

З метою здійснення постійного і системного моніторингу й аналізу закритих і відкритих джерел інформації та збору відомостей, що становлять оперативний інтерес у боротьбі з організованою злочинністю, у складі ГУБОЗ МВС України також були створені підрозділи аналітичної розвідки. Працівниками інформаційно-аналітичних підрозділів «Скорпіон» ГУБОЗ розроблено технології, які покращують пошук і використання інформації оперативного характеру, що має суворо обмежений доступ. Тут збираються дані про кримінальних «авторитетів», їхні зв'язки, минуле, сьогодення і навіть прогнозоване майбутнє. Зокрема, активно відпрацьовуються соціальні мережі (Одноклассники, ВКонтакте, Facebook тощо) і загалом Інтернет. Це дає безліч можливостей, від отримання відео- фото- матеріалів і до цікавих повідомлень. На форумах обговорень і обміну думками щодо різних тем можна виокремити неймовірно корисні посилання [3, с.447].

Особливостями проведення ОРЗ, які тимчасово обмежують права і свободи людини, є їх попереднє узгоджене санкціонування на трьох рівнях, залежно від видів ОРЗ: відомче санкціонування; проведення ОРЗ, що потребують рішення прокурора; ОРЗ, що потребують дозволу слідчого судді. Отримання дозволу на проведення ОРЗ від відповідальних посадових осіб залежить саме від спроможності оперативних працівників (або аналітичних працівників) привести чіткі аргументи щодо виключної необхідності проведення саме запланованого оперативним підрозділом заходу. Тому саме від репрезентації результатів аналітичного дослідження первинних оперативно-розшукових даних буде залежати прийняття відповідного рішення-дозволу на проведення ОРЗ [4, с.34].

Важливою умовою ефективності кримінального аналізу є налагоджена взаємодія між різними правоохоронними органами, включаючи

Службу безпеки України, Державне бюро розслідувань, Офіс Генерального прокурора та Національну гвардію України. Така співпраця передбачає обмін аналітичними матеріалами, координацію дій у межах спільних оперативних планів, узгодження підходів до виявлення, документування та притягнення винних осіб до відповідальності. З огляду на це, Указ Президента України No473/2021 «Про рішення Ради національної безпеки і оборони України» щодо посилення протидії організованій злочинності містить рекомендації щодо розширення функцій аналітичної діяльності поліції, у тому числі з використанням інформаційних технологій [5, с.125].

Інформаційно-аналітичне забезпечення є визначальним чинником ефективності оперативно розшукової діяльності органів сектору безпеки і оборони України, оскільки забезпечує своєчасне отримання, систематизацію та аналітичну обробку інформації, необхідної для прийняття обґрунтованих оперативних рішень. Його застосування сприяє підвищенню результативності виявлення, документування та нейтралізацію організованих злочинних угруповань, оптимізації планування оперативно-розшукових заходів і зменшенню ризиків у діяльності правоохоронних органів.

Література

1. Атмажитов, В. М., Бєлкін, Р. С., Вінберг, А. І., Вінер, Н., Євтушок, В. П., Журавльов, В. Ю., Регульський В. Л. Сутність оперативно розшукової інформації та її місце в забезпеченні інформаційної безпеки поліції. Інформаційна безпека в діяльності поліції , с.7. Електронний ресурс URL: https://repo.dli.donetsk.ua/jspui/bitstream/123456789/732/1/%D0%A1%D0%B5%D0%BC%D1%96%D0%BD%D0%B0%D1%80_%D0%B7%D0%B1%D1%96%D1%80%D0%BA%D0%B0.pdf#page=7
2. Гончаренко, Г. А. (2020). Управління сектором безпеки: поняття й сутність. Вчені записки, 31(70), 40-46. Електронний ресурс URL: https://juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/2-2_2020.pdf#page=48

3. Ахтирської, Н. М., Бєлоглазова, Є. Г., Бурьяка, А., Бусол, О. Ю., Горбачевського, В. Я., Долженкова, О. Ф., ... & Сальникова, В. П. Поняття та сутність аналітичної розвідки як особливої форми інформаційно-аналітичної роботи в ОРД. Електронний ресурс URL:.https://dspace.lvduvs.edu.ua/bitstream/1234567890/2167/1/%D0%9C%D0%BE%D0%B2%D1%87%D0%B0%D0%BD.pdf
4. Господарець, А. А. (2023). Значущість якості аналітичної продукції під час планування проведення оперативно-розшукових заходів Електронний ресурс URL: .https://elar.navs.edu.ua/server/api/core/bitstreams/c3b60f46-2505-4cf8-a40f-2004ae11917b/content
5. Тарасов, Р., Хара, А., Соколюк, А., & Кисельов, А. (2025). Актуальні питання протидії кримінальним правопорушенням за допомогою використання кримінального аналізу під час воєнного стану. (21), 121–128. Електронний ресурс URL : https://archive.liga.science/index.php/universum/article/view/1966

Лисеюк Андрій Миколайович

професор кафедри фінансово-економічної безпеки Навчально-наукового гуманітарного інституту Національної академії Служби безпеки України, кандидат юридичних наук, доцент

ПРОБЛЕМИ ЗАХИСТУ ВІД ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ СИСТЕМ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

В умовах повномасштабної збройної агресії російської федерації, що супроводжується інтенсивними інформаційно-психологічними операціями, забезпечення інформаційної безпеки у всіх сферах суспільних відносин набуває стратегічного значення. Цілеспрямоване та скоординоване поширення державою-агресором недостовірної інформації, маніпулятивних наративів та деструктивної пропаганди, на жаль, стало

частиною української інформаційної реальності. Такі дії, спрямовані на підрив легітимності органів державної влади, маніпулювання суспільною свідомістю та створення умов для обмеження реалізації конституційних прав і свобод громадян, вимагають негайного та системного реагування з боку суб'єктів інформаційної безпеки. Особливо небезпечними такі дії є для систем інформаційно-аналітичного забезпечення сектору безпеки і оборони України, які наповнені чутливою інформацією, виток якої може негативно вплинути на стан інформаційної, воєнної та національної безпеки.

Забезпечення інформаційної безпеки проголошено одним із напрямів інформаційної політики в Законі України «Про інформацію» [1]. Про існування органічного зв'язку між інформаційною безпекою та протидією деструктивним інформаційним впливам свідчать положення Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021. Цей документ визначає, що інформаційна безпека України – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [2].

Деструктивні інформаційні впливи у правовому аспекті доцільно розуміти як протиправні або потенційно протиправні інформаційні дії, що здійснюються суб'єктами комунікації з метою порушення гарантованих Конституцією та законами України прав і свобод людини та громадянина, зокрема права на достовірну інформацію, права на свободу думки і слова, а також права на захист честі, гідності та ділової репутації, при

цьому такі впливи кваліфікуються як загроза інформаційній безпеці держави та суспільства. Стосовно функціонування систем інформаційно-аналітичного забезпечення сектору безпеки і оборони України деструктивні інформаційні впливи мають наступну специфіку.

По-перше, найбільш вразливою частиною системи забезпечення інформаційної безпеки завжди є людина, вплив на свідомість, почуття та настрої якої потребує менше зусиль, ніж подолання бар'єрів кібербезпеки. Тому постійний розвиток інформаційної культури та інформаційної грамотності персоналу сектору безпеки і оборони України має стати невід'ємною частиною їх професійної підготовки [3].

По-друге, уразливим елементом систем інформаційно-аналітичного забезпечення сектору безпеки і оборони України є інформаційні ресурси, що містять дані з обмеженим доступом, витік яких може призвести до серйозних загроз для функціонування державних інституцій та обороноздатності країни. Деструктивні інформаційні впливи у цьому контексті проявляються через спроби несанкціонованого доступу, модифікації або блокування інформаційних потоків, що ускладнює процес прийняття управлінських рішень та створює ризики для стратегічної стабільності. Саме тому правові механізми повинні передбачати комплексну систему захисту, яка поєднує юридичні норми з технічними та організаційними заходами, спрямованими на забезпечення цілісності та конфіденційності інформаційних ресурсів.

По-третє, особливу небезпеку становить використання деструктивних інформаційних впливів для дискредитації органів сектору безпеки і оборони України, що здійснюється шляхом поширення фейкових повідомлень, маніпулятивних інтерпретацій та діпфейків. Такі дії спрямовані на підрив довіри суспільства до військово-політичного керівництва та створення уявлення про хаос і непрофесіоналізм у системі управління. У правовому аспекті це потребує розробки чітких процедур виявлення та спростування неправдивої інформації, а також встановлення відповідальності за її поширення, що дозволить мінімізувати негативний вплив на суспільну свідомість та міжнародний імідж держави.

По-четверте, деструктивні інформаційні впливи можуть мати економічний вимір, оскільки поширення неправдивих даних щодо стану економіки чи фінансової стабільності держави здатне викликати несприятливі наслідки для міжнародної фінансової допомоги. Це, у свою чергу, негативно позначається на фінансуванні сектору безпеки і оборони та ускладнює реалізацію стратегічних програм розвитку. Тому правові механізми протидії повинні включати не лише регулювання інформаційної сфери, а й заходи економічного та фінансового характеру, спрямовані на підтримку стабільності та захист від маніпуляцій, що здійснюються через інформаційний простір.

Література

1. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.
2. Стратегія інформаційної безпеки: затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
3. Бєляков К.І., Онопрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір: монографія / за заг. ред. К.І. Бєлякова. Київ: КВІЦ, 2018. 169 с.

Лілікович Микита Павлович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

АНАЛІЗ ТРАФІКУ ТА ЕЛЕКТРОННИХ КОМУНІКАЦІЙ У ПРОТИДІЇ ОНЛАЙН-НАРКОТОРГІВЛІ

Онлайн-наркоторгівля сьогодні охоплює як відкриті платформи, так і приховані ринки в даркнеті, а також месенджери й соціальні мереж, це робить аналіз мережевого трафіку та електронних комунікацій ключовим інструментом розслідувань і превенції [1]. Інтеграція даних з різних джерел (мережеві логи, метадані повідомлень, блокчейн-транзакції, публічні оголошення) дозволяє відновлювати ланцюги постачання, ідентифікувати операторів і виявляти моделі розповсюдження [2].

Даркнет-маркетплейси: значна частка торгівлі наркотиками відбувається через спеціалізовані маркети, що використовують Tor/інакші анонімні мережі та криптовалюти для приховування транзакцій і комунікацій [3]. Месенджери та соціальні мережі: закриті групи, канали в Telegram та інші платформи використовуються для реклами, зв'язку з клієнтами та організації доставки; ці канали часто поєднуються з «офлайн» логістикою для завершення угод [4]. Технічні засоби приховування: VPN, проксі, мікснети, шифрування повідомлень і використання «платіжних міксерів» ускладнюють трасування, але залишають метадані й поведінкові сліди, які можна аналізувати [5].

Пакетний та потоковий аналіз: захоплення мережевих пакетів (pcap) і агрегація у флоу-записи (NetFlow/IPFIX) дають змогу відновити часові лінії з'єднань, обсяги трафіку, IP-пари та аномалії в поведінці хостів [5]. Фінгерпринтинг сайтів (website fingerprinting): навіть при

використанні Tor або VPN, аналіз розмірів пакетів, інтервалів і шаблонів передачі може дозволити ідентифікувати відвідувані сервіси чи ринки, сучасні атаки з ML підвищують точність таких висновків [6].

Аналіз метаданих повідомлень: час відправлення, розмір повідомлення, частота контактів і мережеві шляхи – усе це дає корисні індикатори для побудови соціальних графів і виявлення ключових вузлів мережі торгівлі [7].

OSINT і соціальний аналіз: збір відкритих даних (оголошення, пости, профілі) дозволяє відстежувати оголошення про продаж, шаблони мови, часові вікна активності та зв'язки між акаунтами, це корисно для попередньої ідентифікації цілей розслідування [8]. Крипто-трейлінг: аналіз блокчейн-транзакцій допомагає відстежувати потоки оплати від покупців до продавців і сервісів-посередників, поєднання блокчейн-даних з мережею і OSINT дає змогу зв'язати анонімні адреси з реальними особами або сервісами [9]. Лінгвістичний та поведінковий аналіз: стилометрія, шаблони формулювань, використання кодових слів і часові патерни допомагають групувати оголошення й повідомлення, відокремлювати бот-активність від людської та виявляти повторювані «торгові» профілі [11]. Розгортання сенсорів і honeypot-систем: створення контрольованих середовищ і «фейкових» оголошень дозволяє виявляти поведінку покупців/продавців, збирати метадані і тестувати канали зв'язку без ризику для реальних користувачів [10] . Координація з платформами та провайдерами: оперативні запити до хостинг-провайдерів, реєстраторів доменів, платіжних сервісів і операторів зв'язку часто дають критичні дані (логі з'єднань, IP-адреси, KYC) для ідентифікації організаторів [1].

Дотримання законодавства та ланцюга доказів: збір мережевих доказів має відбуватися з урахуванням процедур збереження цілісності даних, часових міток і документування джерел, щоб матеріали були прийнятні в суді [5]. Міжнародна співпраця: оскільки онлайн-наркоторгівля часто має транскордонний характер, важлива координація між правоохоронними органами, обмін технічною експертизою та спільні операції проти маркетплейсів і платіжних каналів [2]. Баланс приватності і безпеки: аналіз метаданих може зачіпати права на приватність; тому

необхідні чіткі правові підстави, пропорційність заходів і механізми контролю за доступом до чутливих даних [8].

Шифрування і анонімні мережі: Tor, VPN і end-to-end шифрування ускладнюють доступ до вмісту, залишаючи лише метадані; проте сучасні методи трафік-фінгерпринтингу і кореляції подій підвищують шанси на успіх розслідувань [6]. Обсяг і швидкість даних: великі обсяги мережевого трафіку вимагають масштабованих систем збору, зберігання та аналізу (стрімінг-аналітика, Big Data, ML-моделі) для виявлення релевантних індикаторів в реальному часі [11]. Адаптація злочинців: продавці швидко змінюють канали, використовують одноразові акаунти, «шахрайські» схеми доставки; це потребує постійного оновлення індикаторів і тактик розслідування. [7].

Інвестиції в інфраструктуру аналізу трафіку: розгортання сенсорів, систем збереження pcap/flow, інструментів для кореляції подій і ML-платформ для аномалійної детекції [11]. Розвиток компетенцій: навчальні програми з OSINT, блокчейн-аналітики, мережевої криміналістики та методів фінгерпринтингу для слідчих і аналітиків [8]. Стандарти обміну даними: створення міжвідомчих протоколів для швидкого обміну метаданими, запитів до провайдерів і координації транснаціональних операцій [2]. Етичні рамки і прозорість: впровадження процедур аудиту доступу до мережевих доказів і механізмів захисту прав громадян при проведенні цифрових розслідувань [5].

Аналіз трафіку та електронних комунікацій є потужним інструментом у протидії онлайн-наркоторгівлі, але його ефективність залежить від поєднання технічних можливостей, правових підстав, міжвідомчої координації та постійного оновлення методик у відповідь на адаптацію злочинних мереж. Інтеграція OSINT, мережевої криміналістики та блокчейн-аналітики створює мультидисциплінарний підхід, здатний зменшити шкоду від онлайн-торгівлі наркотиками та розірвати ключові ланцюги постачання.

Література

1. Europol – EU Drug Markets Report. Огляд ринків, онлайн-модулі та методологія (див. розділ «online modules», Executive summary) –

https://www.europol.europa.eu/publications-events/publications/eu-drug-markets-report .
2. Europol – Highlights of 2021. Приклади координації операцій і міжвідомчої співпраці (розділ «highlights») – https://www.europol.europa.eu/media-press/newsroom/news/europol%E2%80%99s-highlights-of-2021-year-in-review .
3. Europol – The trade in illicit drugs. Опис загроз, зв'язків з іншими злочинами (сторінка «trade in illicit drugs») – https://www.europol.europa.eu/crime-areas/trade-in-illicit-drugs .
4. UNODC – OSINT Open source intelligence investigations (Toolkit on Synthetic Drugs). Методики OSINT для розслідувань (розділ «OSINT») – https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/OSINT.html .
5. WCO – Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement (Study Report, July 2024). Рекомендації щодо застосування OSINT (Executive summary, розділ I) – https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/security-programme/osint-report_final.pdf .
6. UNODC – In Focus: Trafficking over the Darknet (World Drug Report 2020 booklet, PDF). Оцінка частки наркотиків у даркнет-активностях та виклики (див. PDF, розділ «Trafficking over the darknet») – https://www.unodc.org/documents/Focus/WDR20_Booklet_4_Darknet_web.pdf .
7. UNODC – CND63 speech / darknet trafficking. Опис загроз даркнету та криптовалют (текст промови) – https://www.unodc.org/unodc/en/speeches/2020/cnd63-sco-020320.html .
8. UNODC – Cryptocurrencies and darknet investigations (training story, 2022). Практичні тренінги та висновки щодо крипто-трейлінгу (стаття) https://www.unodc.org/roseap/en/2022/02/cryptocurrencies-darknet-investigations/story.html .
9. IEEE / ACM публікації – Website fingerprinting and Tor traffic analysis. Дослідження методів фінгерпринтингу та їх застосування (див.

статті в IEEE Xplore: «Website fingerprinting using traffic analysis», «Website Fingerprinting Attacks with Advanced Features on Tor Networks») –; https://ieeexplore.ieee.org/document/10778686 .
10. Data Capture & Analysis of Darknet Markets – Matthew Ball et al., 2019 (ANU Cybercrime Observatory, PDF). Методики збору даних з даркнет-маркетів та приклади результатів (див. розділ «method for collecting and analysing») – https://gwern.net/doc/darknet-market/2019-ball.pdf .
11. Forensic Focus – Network Forensics: A Short Guide. Практичні поради щодо збору мережевих доказів, збереження pcap/flow і процедур (гайд) – https://www.forensicfocus.com/guides/network-forensics-a-short-guide-to-digital-evidence-recovery-from-computer-networks/ .

Луньо Христина Романівна

курсант факультету №2 Львівського державного університету внутрішніх справ

Мусійовська Мар'яна Михайлівна

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ТЕКСТОВОЇ ІНФОРМАЦІЇ

У сучасних інформаційних системах текстова інформація залишається одним із найпоширеніших форматів зберігання та передачі даних. Вона використовується для збереження службової документації, персональних даних, фінансової та комерційної інформації. У зв'язку з цим виникає необхідність забезпечення надійного захисту текстових файлів від несанкціонованого доступу, копіювання та модифікації.

Одним із найбільш ефективних методів захисту інформації є криптографічний захист, який ґрунтується на математичних перетвореннях

даних із використанням криптографічних алгоритмів і ключів. В Україні криптографічний захист інформації є предметом активних наукових досліджень та нормативного регулювання [1].

Сучасні наукові дослідження та практичний досвід свідчать, що використання застарілих або неправильно реалізованих алгоритмів шифрування не забезпечує належного рівня безпеки інформації. Тому дослідження сучасних симетричних, асиметричних і гібридних криптографічних методів захисту текстових файлів, а також аналіз можливостей їх практичного застосування, є актуальним завданням у сфері інформаційної безпеки [2][3].

Особливої актуальності проблема криптографічного захисту набуває в умовах сучасних викликів інформаційній безпеці під час війни, коли зловмисники застосовують складні методи атак, а витоки текстових даних можуть мати серйозні правові, економічні та соціальні наслідки. Крім того, швидкий розвиток обчислювальних технологій та поява нових методів криптоаналізу зумовлюють необхідність постійного перегляду та вдосконалення підходів до захисту інформації.

У зв'язку з цим дослідження сучасних криптографічних методів захисту текстової інформації, їх ефективності та можливостей практичного застосування є особливо важливим саме сьогодні, оскільки дозволяє підвищити рівень інформаційної безпеки та забезпечити надійний захист цифрових даних у сучасних інформаційних системах.

Криптографічний захист інформації — це комплекс методів і засобів, що забезпечують конфіденційність, цілісність, автентичність та невідмовність даних. Симетричні алгоритми (AES) забезпечують швидке шифрування великих текстових файлів, тоді як асиметричні алгоритми (RSA) дозволяють безпечно передавати ключі та створювати цифрові підписи. Гібридні підходи поєднують переваги симетричних і асиметричних методів, що робить їх оптимальними для сучасних інформаційних систем.

Основні криптографічні методи включають:

1. Симетричне шифрування — AES, Blowfish;

2. Асиметричне шифрування — RSA, ECC;
3. Хешування та цифрові підписи — SHA-256, SHA-3;
4. Гібридні схеми — симетричний ключ шифрується асиметрично.

Теоретично криптографія дозволяє забезпечити захист текстових файлів як на рівні зберігання, так і під час передачі інформації у мережах.

На сучасному етапі активне використання електронного документообігу, хмарних сервісів і віддаленої роботи підвищує ризики несанкціонованого доступу до текстової інформації. Українські наукові дослідження показують, що найбільш поширеним методом захисту є AES у поєднанні з RSA у гібридних системах [4].

Практичні проблеми включають:

1. недостатню обізнаність користувачів щодо безпечного зберігання ключів;
2. використання застарілих або слабких алгоритмів шифрування;
3. складність інтеграції криптографічних методів у корпоративні та хмарні системи.

Незважаючи на наявність ефективних алгоритмів, їхнє неправильне впровадження може призвести до витоку конфіденційної інформації або втрати цілісності текстових даних.

Для підвищення ефективності криптографічного захисту текстових даних пропонуються наступні заходи:

1. Використання гібридних криптосистем, що поєднують швидкодію симетричного шифрування та безпечну передачу ключів асиметричними методами.
2. Впровадження сучасних хеш-функцій та цифрових підписів для контролю цілісності та автентичності файлів.
3. Розробка методичних рекомендацій для безпечного зберігання ключів і налаштування систем шифрування.
4. Інтеграція криптографічного захисту у корпоративні та хмарні інформаційні системи.

5. Підвищення обізнаності користувачів щодо безпечного використання текстових файлів і криптографічних засобів.

Отже, криптографічний захист текстової інформації є невід'ємною складовою сучасної інформаційної безпеки. Аналіз теоретичних основ та сучасного стану розвитку методів шифрування показав, що найбільш ефективними є гібридні підходи, які поєднують швидкодію симетричних алгоритмів і безпечну передачу ключів за допомогою асиметричних методів. Використання сучасних алгоритмів шифрування (AES, RSA), хеш-функцій та цифрових підписів дозволяє забезпечити конфіденційність, цілісність і автентичність текстових даних, мінімізуючи ризики несанкціонованого доступу та втрати даних.

Впровадження запропонованих рекомендацій та напрямків удосконалення криптографічного захисту сприятиме підвищенню рівня безпеки інформації в організаціях та ефективному використанню текстової інформації, у сучасних інформаційних системах. Дослідження підтверджує, що постійний розвиток і адаптація криптографічних технологій до нових загроз є ключовим фактором забезпечення надійного захисту інформації сьогодні та в майбутньому.

Література

1. Криптографічний захист інформації. Енциклопедія сучасної України. 2023–2025. Онлайн-ресурс. URL: https://esu.com.ua/article-1575
2. Мулько І. Сучасні методи криптографічного захисту інформації. Матеріали міжнародної науково-практичної конференції. 2025.
3. Староста Б. Р. Застосування алгоритму AES для захисту текстової інформації. Львів. НУ «Львівська політехніка». 2024.
4. Жилін А. В., Корнейко О. В., Мохор В. В. Асиметричні криптографічні алгоритми в системах захисту інформації. Захист інформації. 2025.

Магеровська Тетяна Валеріївна
доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

ТЕХНОЛОГІЧНІ ОСНОВИ BIG DATA ТА ЇХ ПОТЕНЦІАЛ У СФЕРІ БЕЗПЕКИ

У XXI столітті інформація набула статусу одного з ключових стратегічних ресурсів держави. Масштабна цифровізація суспільства, активне використання мережевих сервісів, мобільних пристроїв, систем відеоспостереження, сенсорних та кіберфізичних систем зумовили стрімке зростання обсягів даних. Важливою є не лише кількісна сторона цього процесу, а й якісна трансформація самих даних: вони дедалі частіше відображають поведінкові, соціальні, економічні та безпекові процеси у реальному часі. У такому контексті технології Big Data поступово вийшли за межі бізнес-аналітики й стали важливим елементом сучасної системи безпеки.

Для сфери національної та громадської безпеки здатність оперативно аналізувати великі масиви різнорідної інформації має принципове значення. Традиційні аналітичні підходи, орієнтовані на обмежені та заздалегідь структуровані набори даних, дедалі частіше виявляються недостатніми для виявлення складних загроз, прогнозування кризових ситуацій або аналізу динамічних соціальних процесів. Натомість Big Data формує гнучке аналітичне середовище, у якому можливе поєднання різних джерел інформації, експериментальний пошук нових кореляцій і формування гіпотез без жорстких попередніх обмежень.

Інформаційна база безпекової аналітики формується з широкого спектра джерел. До них належать:

– **державні інформаційні системи та реєстри**, які містять структуровані дані про населення, економічну діяльність, транспорт, фінансові операції;

– **телекомунікаційні та мережеві дані**, що відображають комунікаційні зв'язки, трафік і мережеву активність;

– системи відеоспостереження та технічного моніторингу, які генерують великі обсяги мультимедійних даних;

– **соціальні та цифрові платформи**, що формують масиви текстової, візуальної та поведінкової інформації;

– **сенсорні, IoT та кіберфізичні системи**, які забезпечують безперервний потік даних у реальному часі.

Технологічний виклик полягає не лише у збиранні цих даних, а й у забезпеченні їх сумісності, синхронізації та коректної інтерпретації в єдиному аналітичному просторі.

Ключову складову технологічних основ Big Data становлять аналітичні та інтелектуальні методи, оскільки саме завдяки їм великі обсяги неструктурованої інформації перетворюються на осмислені аналітичні результати, придатні для практичного використання. У сфері безпеки ці методи охоплюють інструменти класифікації для впорядкування об'єктів і подій за визначеними характеристиками, кластерний аналіз для виявлення прихованих структур і взаємозв'язків у даних, алгоритми виявлення аномалій для ідентифікації нетипових або потенційно загрозливих ситуацій, а також прогнозні моделі, що ґрунтуються на аналізі часових рядів і поведінкових патернів. При цьому інтелектуальні алгоритми не підміняють собою експертне судження, а виконують функцію інструменту підтримки аналітиків і управлінців, підвищуючи обґрунтованість і своєчасність прийняття рішень.

Не менш значущим чинником ефективності Big Data-систем є якість даних, оскільки неточна, застаріла або фрагментарна інформація здатна призвести до помилкових аналітичних висновків, що у сфері безпеки може мати критичні наслідки. Саме тому технологічні основи Big Data передбачають впровадження комплексних механізмів очищення та нормалізації даних, контролю достовірності джерел, управління метаданими, а також забезпечення цілісності й актуальності інформації. В умовах безпекових систем ці процеси тісно поєднуються з питаннями регламентації доступу, класифікації інформації та захисту від несанкціонованого втручання.

Таким чином, технологічні основи Big Data створюють передумови для якісно нового рівня аналітики у сфері безпеки, оскільки дозволяє перейти від фрагментарного аналізу окремих подій до системного розуміння процесів, ризиків і загроз, у якому безпекові явища розглядаються як результат взаємодії багатьох факторів — соціальних, економічних, поведінкових, технологічних.

Однією з ключових можливостей Big Data є виявлення закономірностей, які не є очевидними при використанні класичних методів аналізу. Завдяки роботі з великими обсягами даних з різних джерел аналітичні системи здатні встановлювати кореляції між подіями, суб'єктами та часовими інтервалами, що раніше залишалися поза увагою.

Робота з великими масивами даних із різних джерел дозволяє ідентифікувати стійкі моделі поведінки, пов'язані з правопорушеннями або загрозами, виявляти неформальні зв'язки між окремими особами, групами чи подіями та аналізувати просторово-часову динаміку ризиків. Важливою перевагою є те, що такі закономірності формуються не на основі окремих випадків, а на сукупності даних, що зменшує вплив суб'єктивного чинника та підвищує надійність аналітичних висновків.

Окреме місце в аналітиці великих даних посідає виявлення аномалій — нетипових змін або поведінкових патернів, які можуть сигналізувати про потенційні загрози чи початок кризових процесів. Завдяки аналізу великих масивів даних можливо фіксувати нетипові зміни у фінансових, комунікаційних або інформаційних потоках, виявляти підозрілу активність у цифровому середовищі та розпізнавати відхилення в поведінці окремих груп або регіонів. На відміну від жорстко заданих правил, аналітичні моделі Big Data здатні адаптуватися до змін середовища, що особливо важливо в умовах швидкої еволюції загроз.

Не менш важливою складовою аналітичного потенціалу Big Data є прогнозування. Аналіз історичних даних у поєднанні з поточними потоками інформації дозволяє будувати сценарії розвитку подій і оцінювати ймовірність настання певних ризиків. У сфері безпеки прогнозна аналітика використовується для оцінки ймовірності загострення криміногенної ситуації, передбачення соціальних або інформаційних криз, аналізу

вразливостей інфраструктури. При цьому прогнозування не слід розглядати як точне передбачення майбутнього. Йдеться про формування імовірнісних моделей, які дозволяють заздалегідь готувати управлінські рішення та ресурси.

Аналітичні результати Big Data безпосередньо інтегруються у системи підтримки прийняття рішень. Завдяки інтеграції аналітики у процеси управління керівники та аналітики отримують змогу оперувати не лише інтуїтивними оцінками, а й обґрунтованими даними. У безпекових структурах це дозволяє підвищити обґрунтованість стратегічних рішень, оптимізувати розподіл ресурсів, скоротити час реагування на події. Важливо підкреслити, що Big Data-аналітика не замінює людину у процесі прийняття рішень. Її роль полягає у формуванні аналітичної основи, яка зменшує рівень невизначеності та підвищує якість управління.

Практичне значення технологій Big Data у сфері безпеки проявляється насамперед у здатності інтегрувати великі обсяги різнорідної інформації в єдине аналітичне середовище та використовувати результати аналізу для запобігання загрозам, реагування на кризові ситуації й підтримки управлінських рішень. На відміну від фрагментарних підходів минулого, сучасні Big Data-рішення дозволяють розглядати безпекові процеси як динамічні системи, що постійно змінюються під впливом зовнішніх і внутрішніх факторів.

Застосування Big Data у сфері безпеки охоплює кілька взаємопов'язаних рівнів — від стратегічного планування до оперативної діяльності та тактичного реагування. У контексті національної безпеки Big Data використовується для комплексного аналізу загроз, що мають багатофакторний характер. Йдеться не лише про військові або політичні ризики, а й про економічні, інформаційні, соціальні та технологічні виклики. Завдяки цьому формується аналітична основа для стратегічного прогнозування та довгострокового планування, що є критично важливим для державної політики у сфері безпеки.

Однією з найбільш практично орієнтованих сфер застосування Big Data є правоохоронна діяльність. Аналіз великих масивів даних дозволяє перейти від реагування на вже вчинені правопорушення до проактивної

моделі запобігання злочинності. У цьому контексті Big Data використовується для аналізу криміногенної ситуації на основі просторово-часових даних, виявлення стійких моделей злочинної поведінки, дослідження соціальних зв'язків між учасниками протиправної діяльності. Тут важливою перевагою є можливість поєднання даних з різних джерел, що дозволяє формувати більш повну картину подій та зменшувати ризик помилкових висновків.

У сфері протидії організованій злочинності та терористичним загрозам Big Data відіграє ключову роль завдяки здатності аналізувати складні мережеві структури та приховані зв'язки. Традиційні методи аналізу часто не дозволяють охопити всю мережу взаємодій між учасниками таких структур. Застосування Big Data дозволяє виявляти латентні зв'язки між окремими суб'єктами, аналізувати фінансові, інформаційні та комунікаційні потоки, ідентифікувати ключові вузли у злочинних мережах. Такий підхід підвищує ефективність оперативно-розшукової діяльності та сприяє більш цілеспрямованому використанню ресурсів.

У сфері кібербезпеки Big Data стає основою для виявлення для виявлення аномальної мережевої активності, аналізу поведінки користувачів і систем, прогнозування потенційних атак на основі історичних даних. Завдяки цьому формується багаторівнева система захисту, здатна адаптуватися до нових типів загроз і мінімізувати наслідки інцидентів.

Big Data також відіграє важливу роль у системах управління кризовими та надзвичайними ситуаціями. Інтеграція даних з різних джерел — сенсорів, супутникових систем, соціальних платформ — дозволяє отримувати оперативну інформацію про розвиток подій. У практичному вимірі це забезпечує швидке виявлення осередків криз, оцінку масштабів і наслідків надзвичайних ситуацій, підтримку координації між різними службами. Таким чином, Big Data сприяє підвищенню ефективності реагування та зменшенню людських і матеріальних втрат.

Значний потенціал мають і міжвідомчі аналітичні платформи, які дозволяють об'єднувати дані різних органів у єдиному інформаційно-аналітичному просторі, що підвищує узгодженість дій, зменшує дублювання функцій та сприяє більш комплексному аналізу загроз.

Поряд із перевагами використання Big Data супроводжується низкою обмежень. Йдеться про залежність від якості даних, складність інтерпретації результатів і ризики алгоритмічної упередженості. Окрім технологічних викликів, особливої уваги потребують етичні та правові аспекти, пов'язані із захистом персональних даних і прав людини. Саме баланс між ефективністю аналітики та дотриманням правових і етичних гарантій визначає легітимність використання Big Data у сфері безпеки.

У підсумку можна стверджувати, що технології Big Data є потужним інструментом трансформації сучасної системи безпеки. Вони відкривають нові можливості для аналізу, прогнозування та управління ризиками, однак потребують виваженого підходу до впровадження. Поєднання технологічного розвитку з етичними та правовими гарантіями є ключовою умовою ефективного та відповідального використання великих даних у сфері безпеки.

Література

1. Mantelero A., Esposito M. S. An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems // arXiv. – 2024.
2. Latonero M. Big Data Analytics and Human Rights: Privacy Considerations in Context / In: Land M. K., Aronson J. D. (eds.). New Technologies for Human Rights Law and Practice. – Cambridge: Cambridge University Press, 2018. – С. 149–161.

Мартинюк Владислав Віталійович

курсант факультету підготовки фахівців для підрозділів кримінальної поліції Національної поліції України

Рижков Едуард Володимирович

професор кафедри Інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ВИЯВЛЕННЯ ТА ДОКУМЕНТУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ

В умовах тотальної інформатизації суспільства та переходу значної частини соціальних комунікацій у цифровий простір, кардинально змінюються підходи до оперативно-розшукової діяльності (ОРД). Злочинна діяльність дедалі частіше планується, супроводжується або безпосередньо вчиняється з використанням Інтернету, залишаючи величезні масиви інформації у відкритих джерелах.

Сучасна правоохоронна діяльність зазнає фундаментальних трансформацій під впливом цифрової революції та експоненційно го зростання обсягів загальнодоступної інформації. Глобально спо стерігається тенденція до все ширшого використання розвідки на основі відкритих джерел (Open Source Intelligence, OSINT) як не від'ємного інструменту в поліцейській роботі [1].

Соціальні мережі, форуми, блоги, месенджери, публічні реєстри та навіть «темний» сегмент Інтернету (DarkNet) стали невичерпним джерелом оперативно-значущої інформації. У зв'язку з цим, провідну роль починають відігравати технології OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел, що являє собою сукупність інформаційно-комунікаційних технологій (ІКТ) для збору, аналізу та обробки таких даних.

Однак, незважаючи на величезний потенціал, ефективне впровадження OSINT в ОРД стикається з низкою проблем. Для ефективної роботи з OSINT недостатньо навичок звичайного інтернет-користувача.

Необхідні спеціалізовані ІКТ: програмне забезпечення для парсингу (автоматизованого збору) даних, інструменти аналізу соціальних графів (зв'язків), сервіси для деанонімізації, програми для аналізу метаданих (напр., EXIF у фото) [1]. Відсутність у оперативних підрозділах відповідної технічної бази та, що важливіше, належного рівня підготовки фахівців, створює «технологічний розрив» між можливостями злочинців та правоохоронців.

І тут слід погодитись з думкою Телійчука В. Г., що у сучасному суспільстві Інтернет є простором, де користувачі можуть залишатися анонімними, приховувати джерело походження повідомлення або мати псевдоніми [2]. Саме технології OSINT є тим ІКТ-інструментарієм, що дозволяє долати цю анонімність та встановлювати реальні особистості злочинців та їхні зв'язки.

Проблема поглиблюється специфікою самих даних. Інформація в Інтернеті є вкрай волатильною (мінливою): профілі, пости та фотографії можуть бути видалені чи змінені у будь-який момент. Це ставить під сумнів достовірність таких даних і створює складнощі для їх подальшої легалізації та використання у кримінальному провадженні як доказу [3]. Як процесуально закріпити інформацію, що існувала лише кілька годин?

Чинне законодавство, насамперед Закон України «Про оперативно-розшукову діяльність», було сформоване в доцифрову еру і не містить чітких норм, що регламентують процедуру роботи з відкритими даними [4]. Це створює правову невизначеність: який процесуальний статус має інформація, отримана оперативним працівником з Telegram-каналу чи профілю у Facebook.

Наразі відсутні чіткі відомчі інструкції та методичні рекомендації, які б детально регламентували тактику та процедуру документування OSINT-даних. Це призводить до того, що цінна інформація, здобута оперативним шляхом через OSINT, згодом може бути визнана судом недопустимим доказом. Певним кроком у напрямку вирішення суміжних проблем є спроби законодавчо врегулювати статус «електронних доказів» (напр., законопроєкт № 4004) [5].

Як підсумок, можемо стверджувати, що технології OSINT є одним з найпотужніших сучасних ІКТ-інструментів для виявлення та документування злочинної діяльності. Проте їхній потенціал значною мірою не реалізований через суттєві прогалини у законодавстві та методичному забезпеченні ОРД. Для ефективного впровадження OSINT необхідний комплексний підхід: розробка та внесення змін до Закону України «Про оперативно-розшукову діяльність» та відомчих нормативних актів, що чітко визначать поняття «розвідка на основі відкритих джерел» та процедуру фіксації, перевірки та легалізації отриманої інформації; впровадження у систему службової підготовки оперативних працівників поглиблених курсів з використання спеціалізованих ІКТ для OSINT; належне матеріально-технічне забезпечення підрозділів кримінальної поліції відповідним програмним забезпеченням.

Література

1. Рижков Е. В. Методика «OSINT+»: синергія відкритих та відомчих інформаційних ресурсів у діяльності оперативних підрозділів Національної поліції України. Матеріали круглого столу «Роль OSINT-досліджень у підвищенні рівня національної безпеки України м. Львів 7 травня 2025 року. С. 192-199
2. Коваль А. П. OSINT: теорія та практика застосування в ОРД. Навчальний посібник. Київ: Юрінком Інтер, 2023. 215 с.
3. Телійчук В. Г. Оперативно-розшукова протидія наркозлочинності в мережі інтернет як стратегія протидії наркозлочинності в Україні. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2018. №1. С. 115-122.
4. Петренко І. І. Проблеми використання інформації з відкритих джерел як доказу у кримінальному провадженні. Право і кібербезпека. 2024. № 1. С. 78-85.
5. Закон України «Про оперативно-розшукову діяльність»: від 18.02.1992 р. № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303.
6. Проєкт Закону «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з

кіберзлочинністю та використання електронних доказів» № 4004 від 01.09.2020 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69695.

Мандзюк Дмитро Олексійович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Йосифович Данило Ігорович

професор кафедри оперативно-розшукової діяльності, ННІПФПКП Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В БІОМЕТРИЧНИХ СИСТЕМАХ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Розвиток інформаційних систем в Україні на сучасному етапі, на жаль, поки що перебуває на низькому рівні, оскільки впроваджені інформаційні системи ще не здатні в повному обсязі реалізувати своє призначення у процесі діяльності правоохоронних органів.

У сьогоднішніх реаліях неможливо собі уявити ефективну роботу правоохоронних органів без використання сучасних інформаційних технологій. Величезна кількість статистичної, аналітичної та довідкової інформації використовується в діяльності судових органів, прокуратури, нотаріальних та адвокатських контор, юридичних офісів, і, звичайно ж, в оперативно-розшуковій, слідчій та експертній роботі органів і підрозділів Національної поліції. Для цього застосовують не лише універсальне, але й спеціальне програмне забезпечення. Ті темпи, з якими нові інформаційні технології зараз створюються та впроваджуються в

практичну діяльність правоохоронних органів, настільки високі, що іноді навіть фахівці у галузі інформаційних технологій, а тим більше, інші категорії користувачів не встигають оцінити масштаби й глибину всього, що відбувається.

Базовими елементами та засобами реалізації інформаційно-аналітичної діяльності виступають інформаційні системи, системи зв'язку та передачі даних, сучасна інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Це знайшло відображення у ст. ст. 25–27 Закону України «Про Національну поліцію» [4; 5].

Інформаційно-аналітична робота в ОРД – це передбачена законодавством України й урегульована відомчими нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, зокрема й обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави. Основними засобами інформаційно-аналітичної роботи в ОРД є: оперативна техніка та спеціальні технічні засоби, призначені для гласного та негласного отримання інформації; відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи тощо) і різні технічні пристрої, за допомогою яких здійснюється обробка, систематизація та аналіз оперативно-розшукових та інших відомостей фактографічного і криміналістичного характеру [1, с. 38-39].

Інформаційно-аналітична діяльність – це сукупність дій на основі концепцій, методів, засобів, нормативно-методичних матеріалів для збору, накопичення, обробки та аналізу даних з метою обґрунтування та прийняття рішень [10, с. 242].

Варто зауважити, що інформаційно-аналітична діяльність та її результати є ключовими не тільки для ефективного управління органами поліції, а й для розроблення та реалізації різних програм протидії злочинності, перспективного моделювання правоохоронної та правозастосовної діяльності у конкретних соціально-економічних і демографічних умовах та з урахуванням даних оперативної обстановки.

Базовими елементами та засобами реалізації інформаційно-аналітичної діяльності виступають інформаційні системи, системи зв'язку та передачі даних, сучасна інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Це знайшло відображення у ст. ст. 25-27 Закону України «Про Національну поліцію» [4; 5].

Департамент інформаційно-аналітичного забезпечення МВС Україні формує оперативно-довідкові обліки, автоматизовані інформаційно-пошукові системи й банки даних. На сьогодні в оперативно-службовій діяльності успішно використовується інтегрований банк даних регіонального рівня (ІБДР), причому практичні працівники відзначають зручність обміну загальнодоступною інформацією. Обмін інформацією між різними підрозділами Міністерства базується на використанні програмного комплексу «Діоніс». За твердженням багатьох фахівців, він відстає від сучасних вимог і має численні недоліки (низька швидкість передачі даних, невідповідність вимогам інформаційної безпеки, відсутність продуманого інтерфейсу користувача та ін.). Ефективним засобом інформаційного забезпечення оперативно-розшукової роботи розглядається Єдина інформаційно-телекомунікаційна система, яка ще до 2010 р. повинна була охопити всі підрозділи Національної поліції України. Завданнями були автономізація збору, зберігання й обробки інформації, організація віддаленого доступу співробітників усіх правоохоронних служб до інформаційних ресурсів системи, організація взаємодії з інформаційними системами всіх правоохоронних і державних органів України, а також з Інтерполом [2, с.171].

Отже, інтеграція біометричних технологій у інформаційно-аналітичне забезпечення оперативно-розшукової діяльності висвітлює важливість. Основною перевагою біометричної ідентифікації є її здатність забезпечувати точну і швидку ідентифікацію осіб, що значно підвищує ефективність виконання завдань ОРД.

У сьогоденні зростання складності глобальних викликів, зокрема кіберзагроз, військових конфліктів, терористичних актів, природних катастроф та соціальних криз створює необхідність впровадження новітніх

технологій для їх прогнозування та ефективного реагування. Штучний інтелект стає ключовим інструментом, який здатен змінити підходи до аналізу, планування і реалізації операцій у різних сферах, починаючи від національної безпеки до цивільної оборони.

Література

1. В. Г. Севрук «Інформаційно-аналітичні аспекти протидії етнічно організованій злочинності» 2021. [Електронний ресурс]. – Режим доступу : http://www.law.stateandregions.zp.ua/archive/2_2021/2_2021 pdf#page=104
2. А. Є. Стах «Біометричні технології в оперативно-розшуковій діяльності» 2025. [Електронний ресурс]. – Режим доступу : https://sci.ldubgd.edu.ua/bitstream page115
3. Мельнікова О. О. «Правові основи інформаційно-аналітичного забезпечення правоохоронної діяльності» 2023.[Електронний ресурс]. – Режим доступу : http://sulj.oduvs.od.ua/archive/2023/2/7.pdf

Мацкевич Вадим Віталійович

курсант ФПФПКП НПУ Дніпровського державного університету внутрішніх справ

Рижков Едуард Володимирович

професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ІНФОРМАЦІЙНО-ПОШУКОВІ СИСТЕМИ У СФЕРІ ЗАКОНОДАВСТВА

В умовах стрімкої цифровізації суспільства та правової системи України, інформаційно-пошукові системи набули особливого значення як інструмент забезпечення оперативного доступу до нормативно-правових актів, судової практики, аналітичних матеріалів і правових коментарів.

Вони стали невід'ємним елементом правового середовища, без якого неможливо здійснювати ефективну юридичну діяльність чи правозастосування. Використання сучасних інформаційних ресурсів як діючими, так і майбутніми працівниками правоохоронних органів є важливою складовою підвищення ефективності їх професійної діяльності. Сьогодні різні міністерства та державні органи розробляють і підтримують велику кількість інформаційних систем, серед яких ключове місце посідають Єдиний державний реєстер [1].

Під інформаційно-пошукові системи розуміють комплекс технологічних, організаційних і програмних засобів, призначених для зберігання, систематизації, пошуку та актуалізації правових документів. Ці системи виконують не лише довідкову функцію, а й є інструментом правової аналітики та підтримки управлінських рішень. Саме завдяки інформаційно-пошукові системи державні службовці, юристи та науковці мають змогу працювати з достовірними та чинними версіями нормативних актів, що підвищує рівень правової безпеки та правомірності дій у публічній і приватній сферах [2].

Нормативно-правове регулювання функціонування інформаційно-пошукових систем формується в межах ширшого інформаційного права. Основу правового регулювання становить Закон України «Про інформацію», який визначає принципи інформаційних відносин. Ключовим актом є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 р.. Його положення зобов'язують суб'єктів, що експлуатують інформаційно-пошукові системи , забезпечувати захист інформації від несанкціонованого доступу, що має безпосереднє значення для підтримання достовірності та правового значення нормативних матеріалів [3].

З технічного та організаційного боку, інформаційно-пошукові системи становлять багаторівневу структуру, що включає бази даних нормативних актів, матеріали судової практики та коментарі фахівців. Системи, як-от ЛІГА:ЗАКОН, МЕГА-НАУ, а також державні платформи на зразок веб-порталу Верховної Ради України, функціонують на принципах постійного оновлення, індексування та логічного зв'язку між документами. Це

створює єдиний інформаційний простір, де користувач може дослідити історію змін акта, що суттєво підвищує рівень якості юридичної роботи та дозволяє мінімізувати помилки у тлумаченні норм [4].

Також застосовуються норми Закону України «Про електронні комунікації», «Про електронні документи та електронний документообіг» та «Про доступ до публічної інформації». Сукупність цих документів формує правовий режим інформаційно-пошукові системи як елементу інформаційної інфраструктури держави, що має забезпечувати прозорість, доступність і безпечність правових даних для громадян і юридичних осіб [5].

У практичній площині інформаційно-пошукові системи є незамінним інструментом для представників правничої професії, державних службовців та дослідників. Вони дозволяють за лічені секунди віднайти потрібний документ серед тисяч нормативних актів, звірити чинність редакції, перевірити зміни, визначити правові колізії або суперечності між документами. Таким чином, інформаційно-пошукові системи забезпечують ефективність, швидкість і юридичну точність у роботі, що є критично важливим у правовій діяльності.

Одним із найважливіших аспектів є забезпечення достовірності, повноти й актуальності правової інформації. Будь-яка затримка в оновленні даних може спричинити суттєві юридичні наслідки. Тому сучасні правові бази використовують алгоритми синхронізації з офіційними джерелами, зокрема порталом Верховної Ради України, що забезпечує безпосередню перевірку автентичності документів.

Інформаційно-пошукові системи також відіграють значну роль у здійсненні правового моніторингу. За їх допомогою можна аналізувати тенденції у правотворчості, виявляти дублювання норм або прогалини у законодавстві. Окрему увагу слід приділити питанню доступності: в Україні забезпечується безкоштовний доступ до нормативних актів через офіційні державні ресурси, проте професійні користувачі переважно працюють із комерційними системами. Такі рішення, як ЛІГА:ЗАКОН чи Право.UA, дозволяють проводити правовий аналіз текстів за допомогою алгоритмів обробки природної мови, що підвищує рівень автоматизації правової роботи та забезпечує кращу якість юридичного супроводу.

У рамках правоохоронної діяльності особливе місце посідає використання інформаційно-пошукових систем Управлінням стратегічних розслідувань Національної поліції України. Робота Управлінь стратегічних розслідувань сфокусована на протидії організованій злочинності, корупції, а також захисті економічної безпеки держави. Ефективність цих розслідувань безпосередньо залежить від здатності швидкого та глибокого аналізу великих масивів даних. інформаційно-пошукові системи є критично важливим інструментом для Управлінням стратегічних розслідувань, дозволяючи інтегрувати інформацію з різних реєстрів (наприклад, майнових, фінансових) та оперативних баз. Це забезпечує можливість побудови складних схем зв'язків, ідентифікації прихованих активів та встановлення фактичних бенефіціарів злочинних угруповань. Таким чином, інформаційно-пошукові системи є основою для стратегічного аналізу та прийняття обґрунтованих рішень у боротьбі з транснаціональною та організованою злочинністю.

Системи розшуку, які є ключовим компонентом інформаційно-пошукові системи, працюють на основі складних алгоритмів індексування та пошуку тексту. Вони використовують методи обробки природної мови (NLP) для розуміння семантики (змісту) і контексту правових документів. Системи розшуку застосовують різні типи пошуку: від реквізитного (за номером, датою) до повнотекстового (з урахуванням синонімів, словоформ) та контекстуального (зв'язок між документами через посилання або судову практику). Ефективність системи розшуку критично залежить від якості тезаурусів (словників правових термінів) та рубрикаторів (систем класифікації), які дозволяють користувачу знайти документ навіть за неточним запитом і дослідити взаємопов'язані норми в межах галузі права.

Інформаційно-пошукові системи у сфері законодавства є вирішальними для сучасного правового процесу, оскільки вони забезпечують стабільність правового простору та гарантують громадянам доступ до актуальної інформації. Ці системи також мають критичне значення для інформаційно-аналітичного забезпечення правоохоронної діяльності;

їхня важливість для боротьби зі злочинними угрупованнями підтверджена статтею 14 Закону України «Про боротьбу з організованою злочинністю», яка вимагає їх використання для збору та аналізу даних. Для подальшого розвитку потрібне вдосконалення нормативної бази, інтеграція штучного інтелекту для аналітики та посилення стандартів кібербезпеки. Розбудова цієї потужної інфраструктури - це необхідний етап у формуванні цифрової держави та утвердженні принципу верховенства права в Україні.

Література

1. Інформаційні та комунікаційні технології: навч. посіб. / О. А. Дісковський, Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов. - Дніпро: ДДУВС, 2025. - 272 с.
2. Білущак Т. М., Пелещишин А. М. Використання інформаційно-пошукової системи в менеджменті архівної справи закладами вищої освіти. Бібліотекознавство. Документознавство. Інформологія. 2020. № 1. С. 118–126.
3. Сачковська В. І. Інформаційно-пошукові системи: ґенеза та еволюція : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 029 Інформаційна, бібліотечна та архівна справа / наук. кер. О. Б. Герасимчук ; Волинський національний університет імені Лесі Українки. Луцьк, 2025. 50 с.
4. Шаповаленко І. В. Формування та функціонування інформаційно-пошукових систем у державних архівах. Період трансформаційних процесів в світовій науці: 2024р. 545 – 547с.
5. Зведений словник термінів з інформаційної, бібліотечної та архівної справи / [авт. кол.: М. М. Головченко та ін.]. Херсон : ОЛДІ-ПЛЮС, 2020. 166 с.

Мовчан Анатолій Васильович

професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

Рішко Василь Васильович

здобувач ступеня доктора філософії у галузі права Львівського державного університету внутрішніх справ

ВІД OSINT ДО ШТУЧНОГО ІНТЕЛЕКТУ: НОВІ ІНСТРУМЕНТИ БОРОТЬБИ З ТОРГІВЛЕЮ ЛЮДЬМИ

Виявлення фактів торгівлі людьми є вкрай складним процесом через латентний характер цього явища та різноманітність його форм. Ефективне розпізнавання таких злочинів потребує застосування не лише класичних оперативно-розшукових і криміналістичних методів, а й сучасних аналітичних та інформаційних технологій.

Важливою складовою виявлення торгівлі людьми є інформаційний обмін з іноземними партнерами та міжнародними організаціями (INTERPOL, EUROPOL, FRONTEX, IOM). Через ці канали отримується інформація про переміщення потенційних жертв, координуються транскордонні операції та реалізуються спільні профілактичні ініціативи, зокрема інформаційні кампанії в аеропортах і на вокзалах.

Останнім часом активно застосовуються алгоритми машинного навчання для виявлення шаблонів злочинної діяльності, аналітика великих даних (Big Data) – для прогнозування ризикових зон, нейромережі – для аналізу зображень і текстових повідомлень на предмет прихованих ознак торгівлі людьми, а також системи раннього попередження, інтегровані у прикордонні бази даних.

У сучасних умовах торгівля людьми дедалі частіше переміщується у цифровий простір, використовуючи анонімність, швидкість та глобальність мережевих комунікацій. У зв'язку з цим інформаційні технології

відіграють ключову роль не лише у виявленні, а й у документуванні злочинної діяльності, пов'язаної з торгівлею людьми.

Одним із найефективніших інструментів сучасної криміналістики є OSINT (Open Source Intelligence) – розвідка з відкритих джерел. Аналітики та правоохоронні органи можуть здійснювати моніторинг соціальних мереж (Facebook, Instagram, Telegram, TikTok), онлайн-дошок оголошень (наприклад, OLX, Slando), тематичних форумів, у тому числі розташованих у Dark Web, а також відеохостингів (YouTube, TikTok, спеціалізовані ресурси).

Інструменти на кшталт Maltego, Social Links, SpiderFoot дають змогу візуалізувати зв'язки між обліковими записами, IP-адресами, доменами, номерами телефонів та іншими цифровими ідентифікаторами [1].

Під час спілкування через месенджери (Viber, WhatsApp, Signal) торговці людьми залишають цифрові сліди, які можуть бути проаналізовані: метадані листування, геолокація фото та відео, активність у хмарних сховищах (Google Drive, iCloud), логи підключень та IP-активності. Слідчі дії можуть охоплювати доступ до облікових записів на підставі судового рішення, а також вилучення інформації з мобільних пристроїв із використанням методів цифрової криміналістики.

Зокрема, Верховний Суд у постанові від 12 червня 2024 року визнав, що електронні (цифрові) докази, включно з матеріалами приватних месенджерів та особистого листування, є допустимими у кримінальних провадженнях за умови, що їх отримано з дотриманням вимог процесуального законодавства [2].

Отже, правоохоронні органи активно застосовують цифрові сліди, залишені в месенджерах, для розслідування злочинів, у тому числі торгівлі людьми.

Великі масиви даних дають змогу виявляти підозрілі шаблони поведінки. Наприклад, масове розміщення оголошень про «роботу за кордоном» з однаковими контактними даними, незвичні маршрути подорожей окремих осіб, аналіз банківських транзакцій у ризикових регіонах, розпізнавання облич на фото чи відео для ідентифікації можливих жертв.

Штучний інтелект і технології машинного навчання здатні автоматично виокремлювати потенційні випадки експлуатації, зокрема у порнографічному контенті, шляхом аналізу відеоматеріалів та аудіозаписів [3].

Технології відстеження переміщень за допомогою GPS, GSM-сигналів чи Wi-Fi-локацій дозволяють відтворювати маршрути жертв або підозрюваних, фіксувати перебування у місцях можливої експлуатації (публічні будинки, підвали, закриті об'єкти), а також документувати незаконне переміщення осіб через кордон. Серед інструментів, що застосовуються у правоохоронній практиці, – Cellebrite, XRY, GrayKey [4].

Інформаційні технології створюють як нові ризики використання цифрових платформ злочинцями, так і потужні можливості для протидії таким проявам. Поєднання OSINT, AI, аналітики Big Data та цифрової криміналістики значно підвищує ефективність виявлення й документування торгівлі людьми, проте потребує належного законодавчого регулювання та високого рівня технічної підготовки фахівців.

В умовах цифровізації особливу роль відіграє цифрова криміналістика, яка дає змогу вилучати й аналізувати інформацію з мобільних пристроїв, месенджерів і соціальних мереж; ідентифікувати IP-адреси, геолокацію та інтернет-активність; застосовувати автоматизовані засоби аналізу візуальних і текстових даних (AI/ML). Серед поширених інструментів – Cellebrite, Magnet AXIOM, FTK, EnCase, а також OSINT-системи для моніторингу онлайн-активності [4].

Попри значний потенціал доказової бази, типовими проблемами під час документування торгівлі людьми залишаються: втрата або знищення доказів на етапі розслідування (особливо електронних); порушення правил їх вилучення та фіксації, що унеможливлює використання здобутої інформації в суді; відсутність уніфікованих алгоритмів дій слідчого щодо роботи з цифровими слідами; обмежений доступ до закритих ресурсів і хмарних серверів. Усе це потребує нормативного врегулювання та інституційної підтримки з боку експертних і технічних служб [5].

Сучасні злочинні угруповання активно застосовують технології шифрування, анонімні браузери (Tor), криптовалюти, VPN і хмарні

сервіси для комунікації та фінансових операцій. Це суттєво ускладнює ідентифікацію виконавців, відстеження транзакцій та збереження доказів. Крім того, дані, розміщені на іноземних серверах, часто залишаються недоступними без міжнародної правової допомоги, що сповільнює розслідування.

Документування фактів торгівлі людьми із застосуванням ІТ-технологій стикається й з проблемою недостатньої правової регламентації цифрових доказів. Серед основних труднощів – відсутність єдиних стандартів вилучення та збереження електронних доказів; високий ризик зміни чи втрати даних без належного процесуального оформлення; складність доведення автентичності цифрових доказів у суді; обмеженість фахівців-експертів у галузі ІТ [6].

Наявні правові норми не завжди враховують специфіку кіберпростору та роль новітніх технологій у вчиненні злочинів, пов'язаних із торгівлею людьми. Зокрема, в українському законодавстві все ще бракує деталізації процедур вилучення даних із соціальних мереж, месенджерів, криптовалютних гаманців та інших цифрових платформ. Крім того, міжнародні процедури правової допомоги (наприклад, запити до Facebook чи Google) є тривалими та не завжди результативними.

У зв'язку з цим процеси виявлення та документування злочинів, пов'язаних із торгівлею людьми, потребують системного підходу: удосконалення законодавства, розбудови сучасної технічної інфраструктури, посилення міжвідомчої координації, підвищення кваліфікації персоналу та одночасного забезпечення дотримання основоположних прав людини. Подолання цих викликів є критично важливим для формування дієвої системи протидії торгівлі людьми.

ІТ-технології вже стали невід'ємною складовою розслідування та фіксації злочинів у сфері торгівлі людьми: аналітика даних, мобільна криміналістика, системи розпізнавання й автоматизованого аналізу інформації значно підвищують ефективність реагування на такі загрози. Водночас зберігається низка проблем – від недостатнього рівня технічної підготовки персоналу до обмеженого нормативного регулювання цифрових доказів.

Таким чином, результативна протидія торгівлі людьми в умовах цифровізації потребує не лише оновлення законодавства та вдосконалення технічних засобів виявлення і документування злочинів, а й сталого міжвідомчого та міжнародного співробітництва, спрямованого на захист найбільш уразливих категорій населення.

Література

1. OSINT – розвідка з відкритих джерел та інформаційна безпека URL: https://prometheus.org.ua/prometheus-free/osint-open-source-intelligence/
2. Верховний Суд висловився щодо використання листування у месенджерах як доказу в кримінальному провадженні URL: https://wrt.sud.ua/uk/news/publication/308137-verkhovnyy-sud-vyskazalsya-ob-ispolzovanii-perepiski-v-messendzherakh-v-kachestve-dokazatelstva-v-ugolovnom-proizvodstve?utm_source=chatgpt.com#google_vignette
3. Використання штучного інтелекту для виявлення торгівлі людьми https://www.psychologytoday.com/us/blog/why-bad-looks-good/202412/using-artificial-intelligence-to-detect-human-trafficking?utm_source=chatgpt.com
4. Як ФБР та інші державні агенції зламують смартфони URL: https://techtoday.in.ua/news/yak-fbr-ta-inshi-derzhavni-agentsiyi-zlamuyut-smartfony-173421.html?utm_source=chatgpt.com
5. Авдєєва, Г., Живуцька-Козловська, Е. (2023). Проблеми використання цифрових доказів у кримінальному судочинстві України та США. Теорія та практика судової експертизи і криміналістики. Вип. 1 (30). С. 126-143. DOI: //10.32353/khrife.1.2023.07.
6. Хахановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. Криміналістичний вісник, 2020. 31(1), 13-19. https://doi.org/10.37025/1992-4437/2019-31-1-13

Надич Денис Миколайович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Баб'як Андрій Васильович

завідувач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У ВИКРИТТІ ТА ЗАПОБІГАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ОБІГУ НАРКОТИЧНИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН, ЇХ АНАЛОГІВ АБО ПРЕКУРСОРІВ ТА ІНШИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ЗДОРОВ'Я НАСЕЛЕННЯ

У 2024 році підрозділи Національної поліції України (НПУ) задокументували понад 47 тис. правопорушень, пов'язаних із незаконним обігом наркотичних засобів. У межах цих проваджень близько 20 тис. осіб отримали повідомлення про підозру, а до суду було скеровано обвинувальні акти майже у 39 тис. кримінальних справ. Правоохоронці ліквідували 74 нарколабораторії та 968 наркопритонів, які використовувалися не лише для вживання наркотиків, а й для їхнього нелегального виготовлення та поширення. У ході комплексних оперативних заходів поліція вилучила приблизно 5,5 т наркотичних засобів, що еквівалентно понад 20 млн доз, а також понад 24 т прекурсорів [1].

Ефективна боротьба з цим явищем ґрунтується на застосуванні сучасних інструментів та методів оперативно-розшукової діяльності (ОРД). В умовах активного використання інформаційних технологій у незаконному обігу наркотиків особливого значення набуває інформаційно-аналітичне забезпечення ОРД. На думку О. Бандурки, саме воно

забезпечує своєчасне виявлення, аналіз та узагальнення інформації про наркозлочини, що є необхідною передумовою для прийняття ефективних управлінських і оперативних рішень у діяльності правоохоронних органів [2].

Ю. Буковський характеризує інформаційно-аналітичну діяльність підрозділів НПУ боротьби з наркозлочинністю як комплекс «організаційних правових і технологічних засобів, які забезпечують процес збирання, отримання, обробку, поширення, аналізу та використання інформаційних ресурсів, необхідних для виконання визначених законодавством завдань та функцій» [3] цих підрозділів.

А. Мовчан визначає основні форми інформаційно-аналітичної роботи в ОРД. Це – отримання оперативно-розшукової інформації, систематизація оперативно-розшукової інформації, оперативно-розшукова ідентифікація, оперативно-розшукова діагностика, оперативно-розшукове прогнозування, аналітична розвідка [4].

Стрімкий розвиток інформаційних технологій суттєво впливає на протидію незаконному обігу наркотиків. Сучасні цифрові засоби використовують як правоохоронні органи, так і злочинні угруповання, які все частіше переносять протиправну діяльність у мережу Інтернет. У цьому сенсі одним із перспективних напрямів удосконалення інформаційно-аналітичної діяльності стає впровадження технологій великих даних в ОРД та досудове розслідування.

С. Пеньков та В. Шендрик зазначають, що використання таких технологій забезпечує можливість комплексного пошуку, збирання та систематизації інформації про осіб, причетних або потенційно причетних до незаконного обігу наркотиків, аналіз їх соціальної активності та мережевих зв'язків, а також своєчасне виявлення в мережі Інтернет ознак підготовки чи вчинення наркозлочинів з подальшим оперативним реагуванням. Крім того, застосування великих даних сприяє ідентифікації кримінальних угруповань, визначенню рівня їх організованості, розподілу ролей і неочевидних зв'язків між учасниками, формуванню поведінкових профілів правопорушників, удосконаленню планування оперативно-

розшукових заходів та виробленню обґрунтованих управлінських рішень на основі моделювання розвитку оперативно-тактичних ситуацій [5].

Як свідчить практика, пошуково-аналітична діяльність працівників кримінальної поліції, повноваження яких полягають у викритті та запобіганні кримінальних правопорушень у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших кримінальних правопорушень проти здоров'я населення, переважно пов'язана з виявленням та аналізом протиправного контенту в мережі Інтернет. Водночас актуальною залишається протидія так званим «закладникам», які здійснюють збут наркотичних засобів шляхом розміщення заздалегідь підготовлених доз у різних локаціях. У цьому сенсі обґрунтованою є необхідність впровадження в практичну діяльність правоохоронців технологій штучного інтелекту, здатних забезпечити аналіз значних масивів даних та ідентифікацію осіб, причетних до розповсюдження наркотиків, за сукупністю поведінкових ознак.

Крім того, використання технологій обробки та аналізу інформації в режимі реального часу, зокрема даних із систем відеоспостереження, суттєво розширює можливості запобігання та протидії незаконному обігу наркотиків. До таких можливостей належать автоматизоване розпізнавання номерних знаків транспортних засобів, ідентифікація осіб за зображенням обличчя, виявлення підозрілих моделей поведінки, а також проведення аналітичного супроводу пошукових заходів у громадських місцях щодо осіб, причетних до наркозлочинів [6].

Отже, інформаційно-аналітична робота в ОРД є важливою частиною системи протидії наркозлочинності.

Розвиток цифрових технологій та зміна форм наркобізнесу вимагають постійного вдосконалення ОРД, зміцнення аналітичних підрозділів, міжнародної співпраці та зниження корупційних ризиків.

Лише комплексний підхід надасть змогу ефективно захищати здоров'я населення та забезпечувати національну безпеку України.

Література

1. Нацполіція: результати боротьби з наркозлочинністю у 2024 році. Національна поліція України. URL: https://surl.li/jpjlkq (дата звернення 04.12.2025).
2. Бандурка О. М. Оперативно-розшукова діяльність. Частина І : Підручник. Харків: Вид-во Нац. ун-ту внутр. справ, 2002. 244 с.
3. Буковський Ю. Д. Аналітична діяльність підрозділів боротьби з наркозлочинністю Національної поліції України. Юридичний науковий електронний журнал. 2023. № 3. С. 369–372. DOI: https://doi.org/10.32782/2524-0374/2023-3/86 (дата звернення: 15.12.2025).
4. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції : навч. посібник / А. В. Мовчан. Львів: ЛьвДУВС, 2017. 244 с.
5. Пеньков С. В., Шендрик В. В. Впровадження інтернет-технологій у діяльність Національної поліції України для отримання оперативно-розшукової інформації. Право і безпека. 2017. № 2 (65). С. 80–85. URL: http://pb.univd.edu.ua/ ?action= publications&pub_id=411139&mid=8&year=2017 (дата звернення: 15.12.2025).
6. Федоренко О. А., Стрільців О. М., Тарасенко О. С. Використання технологій штучного інтелекту у правоохоронній діяльності : аналіт. огляд. Київ : Нац. акад. внутр. справ, 2022. 106 с. DOI: https:// elar.navs.edu.ua/handle/123456789/29185 (дата звернення: 15.12.2025).

Надич Тарас Миколайович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Баб'як Андрій Васильович

завідувач кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ЗАСОБИ, МЕТОДИ ТА АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У ВИКРИТТІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ВЛАСНОСТІ

Протиправні посягання на власність суттєво дестабілізують соціальні та економічні процеси в державі. Майнові правопорушення є однією з найпоширеніших категорій злочинності. Відповідно до розділу VI Кримінального кодексу України, до них належать крадіжки, грабежі, розбої, вимагання, шахрайство, привласнення та інші посягання [1]. Ефективність розкриття таких правопорушень значною мірою залежить від якісної оперативно-розшукової діяльності (далі – ОРД).

Метою дослідження є аналіз можливостей і меж застосування засобів та методів ОРД у процесі викриття злочинів проти власності та оцінка супутніх корупційних ризиків.

ОРД регламентується такими основними нормативно- правовими актами, як Закон України «Про оперативно-розшукову діяльність» [2] (далі – Закон), Кримінальний процесуальний кодекс України [3] (далі – КПК), а також відомчими нормативними актами, які регулюють порядок проведення оперативних заходів.

Із засобів ОРД, що застосовуються в процесі викриття злочинів проти власності, можна виділити наступні:

Оперативно-технічні засоби. До цієї групи належать засоби фіксації, спостереження, зняття інформації з каналів зв'язку та інші

технічні інструменти, передбачені ст. 8 Закону. У майнових злочинах вони застосовуються з метою встановлення місцеперебування підозрюваних, фіксації домовленостей між співучасниками; відстеження збуту викраденого майна. Наприклад, негласне спостереження (§ 3 КПК) дозволяє документувати підготовку до крадіжки або передачу викрадених речей.

Використання інформаційно-аналітичних баз. Оперативні підрозділи активно застосовують бази даних Міністерства внутрішніх справ, державного підприємства «Національні інформаційні системи», інформацію з систем відеоспостереження тощо.

Робота з негласними джерелами інформації. Ключовими методами у протидії крадіжкам, грабежам та шахрайству є залучення конфідентів, контрольована закупка, оперативні комбінації тощо. Ці негласні джерела дозволяють проникнути в середовище злочинців, отримати інформацію про канали збуту, викривати групову злочинність. Закон прямо дозволяє використання конфіденційного співробітництва (ст. 8).

У процесі викриття кримінальних правопорушень проти власності підрозділи, які здійснюють ОРД, користуються такими методами, як:

Оперативне спостереження. На нашу думку, це один із найефективніших методів документування злочинної діяльності. У справах про крадіжки чи розбої спостереження дозволяє фіксувати маршрути підозрюваних, встановлювати місця зберігання викраденого, виявляти співучасників.

Оперативний експеримент. Цей метод полягає у створенні умов для перевірки поведінки підозрюваної особи, наприклад, під час спроби збуту викраденого майна. Його проведення можливе лише за умови документування і без провокування злочину (ч. 3 ст. 271 КПК).

Контроль за вчиненням злочину. Це комплекс негласних дій, спрямованих на фіксацію правопорушення, що готується або триває. У справах проти власності найчастіше застосовується контрольована поставка або контрольована закупка, коли документується рух викрадених товарів (ст. 271 КПК).

Аналітичні та криміналістичні методи. До них відносять кримінальний аналіз (побудова профілю злочинця), аналіз modus operandi, трасологічні та техніко-криміналістичні дослідження, структурний аналіз серійних злочинів. Ці методи дозволяють виявляти серійність та груповий характер злочинів [4]. Зупинимося на них детальніше.

Комплекс заходів із збору, аналізу та інтерпретації інформації, який становить основу аналітичного методу, дозволяє правоохоронним органам своєчасно виявляти, документувати, розслідувати та запобігати майновим правопорушенням (крадіжкам, шахрайству, рейдерству, присвоєнню майна тощо). Серед них можна виокремити такі:

– системний аналіз криміногенної ситуації, схем, зв'язків між фігурантами, каналів постачання чи відпуску майна (кримінальний аналіз) [5];

– моніторинг інформаційних джерел, в тому числі відкритих (OSINT), соціальних мереж, оголошень, оглядів ринку нерухомості чи рухомого майна (застосовується для виявлення підозрілих схем) [6];

– логістичний та просторовий аналіз, який використовується для виявлення маршрутів перевезення, складів, місць зберігання чи перерозподілу майна. Особливого значення цей захід набуває у справах рейдерства, масштабних схемах крадіжок чи розкрадань [7];

– фінансово-економічний аналіз, що комплексно вивчає рух коштів, джерел формування майна та операцій з активами, виявляє схеми легалізації незаконних доходів і протиправного перетворення власності. Цей аналітичний метод набуває ваги під час розслідування шахрайських схем, корупційних діянь і масштабних розкрадань [8] тощо.

Водночас науковці та правоохоронці-практики зазначають низку проблемних питань щодо аналітичного забезпечення ОРД. Це, зокрема, – несистемне використання аналітики на практиці, переважно через брак кадрів; недостатня публічність і документування кейсів злочинів проти власності, особливо дрібних, що ускладнює аналіз практики; зміна законодавством порогів для кримінальної відповідальності за крадіжку робить частину дрібних крадіжок адміністративними, що знижує число кримінальних проваджень, а відтак змінює статистичні та аналітичні дані.

Також фахівці підкреслюють, що для запобігання злочинам проти власності важливе значення має кримінологічна профілактика – використання превентивних методів, оцінювання ризиків та здійснення аналітичної роботи ще до того, як правопорушення буде скоєне [4, 5, 7].

Засоби та методи оперативно-розшукової діяльності відіграють ключову роль у виявленні та розкритті злочинів проти власності. Найбільш ефективними виявляються ті, що поєднують технічні можливості, інформаційні ресурси та роботу з негласними джерелами.

Правильне та правомірне застосування ОРД забезпечує швидке документування злочинної діяльності, виявлення співучасників, повернення викраденого майна та притягнення винних осіб до відповідальності.

Аналітична діяльність відіграє значну роль у сучасній системі протидії злочинам проти власності. Завдяки застосуванню кримінального аналізу, моніторингу інформаційних потоків, а також логістичного й фінансового аналізу, правоохоронні органи здатні не лише оперативно реагувати на правопорушення, а й запобігати їхньому вчиненню, встановлювати організовані групи, викривати складні шахрайські та рейдерські механізми та ефективно захищати майнові інтереси громадян і держави.

Література

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III : станом на 17.07.2025. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 02.12.2025).
2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII : станом на 09.08.2024. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 02.12.2025).
3. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI : станом на 01.08.2025. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 02.12.2025).

4. Шевчук В. М. Структура окремої криміналістичної методики: сучасні наукові підходи та перспективи досліджень. Вчені записки ТНУ імені В.І. Вернадського. Серія «Юридичні науки». 2020. Т. 31 (70), № 4. С. 256–260. URL: https://surl.lu/hlcgoi (дата звернення: 03.12.2025).
5. Гончарук, О. М., Ісмайлов, К. Ю. Кримінальний аналіз у системі правоохоронних органів України : поняття, мета й завдання. Правовий часопис Донбасу, 2023. № 2. С. 3–9. DOI: https://doi.org/10.32782/2523-4269-2023-83-3-9 (дата звернення: 03.12.2025).
6. Кластерний аналіз телефонного трафіку : практ. посібн. / [за заг. ред. В. Школьнікова та О. Корнейка]. К. : Вид-во Нац. акад. внутр. справ, 2020. 40 с.
7. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А. В. Мовчан. Львів: ЛьвДУВС, 2017. 244 с.
8. Мисник К. П. Форензік як метод економічних розслідувань: теоретичні засади. Економічний вісник Донбасу. 2022. №3 (69). – С. 41-46. URL: https://surl.li/ybjayk (дата звернення: 03.12.2025).

Наконечний Єгор Вячеславович

курсант ФПФКП НПУ Дніпровського державного університету внутрішніх справ

Рижков Едуард Володимирович

професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

АВТОМАТИЗАЦІЯ ПІДГОТОВКИ ЮРИДИЧНИХ ДОКУМЕНТІВ ЗА ДОПОМОГОЮ ОНЛАЙН СЕРВІСУ GOOGLE DOCS СТОСОВНО ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКОГО

Цифровізація діяльності Національної поліції України вимагає пошуку нових інструментів для зменшення паперової роботи, що

відповідає затвердженій Концепції інформатизації МВС [1]. На практиці значну частину зміни поліцейський витрачає на складання однотипних процесуальних та адміністративних матеріалів, що забирає час, необхідний для безпосередньої охорони правопорядку. У цій роботі пропонується розглянути функціонал хмарного сервісу Google Docs як засобу автоматизації діловодства, з обов'язковим урахуванням вимог інформаційної безпеки.

Використання хмарних інструментів може суттєво спростити виконання службових завдань та оптимізувати адміністративну діяльність [2, с. 341]. Аналіз можливостей Google Docs дозволяє виділити кілька напрямів, корисних для поліцейської роботи. По-перше, це створення бібліотеки шаблонів. Замість набору тексту «з нуля», співробітник може використовувати уніфіковані бланки рапортів, пояснень чи протоколів, які вже відформатовані згідно з чинним законодавством. Достатньо лише внести змінні дані (фабулу, дату, відомості про особу), що значно знижує ризик помилок при оформленні.

Окремо варто виділити функцію голосового набору тексту. Для патрульних поліцейських або слідчих, які працюють на місці події, це критично важливо. Можливість надиктувати текст рапорту або опис обстановки прямо в смартфон дозволяє зафіксувати інформацію в рази швидше, ніж при ручному введенні, особливо в польових умовах [3, с. 112].

Також важливою є можливість спільної роботи над документами. Це актуально, коли необхідна взаємодія кількох служб, наприклад, слідчого та оперативника. Керівник підрозділу може дистанційно перевірити проєкт документа, внести правки або погодити його в режимі реального часу. Більш просунуті користувачі можуть застосовувати інструменти Google Apps Script для автоматичного перенесення даних з таблиць у текстові файли, що зручно при формуванні статистичних зведень.

Водночас необхідно чітко розуміти межі використання таких сервісів. Оскільки сервери Google є публічними, категорично заборонено вносити до них відомості, що становлять державну таємницю або службову інформацію [3]. Цей інструментарій підходить виключно для роботи з

відкритими даними, підготовки навчальних матеріалів або чернеток документів, які не містять персональних даних громадян до моменту їх офіційної реєстрації в захищених системах.

Важливість цифрової грамотності підкреслюється і в наукових працях. Зокрема, дослідники Дніпровського державного університету внутрішніх справ наголошують, що сучасний правоохоронець повинен впевнено володіти хмарними технологіями, адже це є вимогою часу [4, с. 146].

Отже, впровадження Google Docs у повсякденну діяльність поліцейського дозволить автоматизувати рутинні процеси та пришвидшити обмін інформацією. Проте ефективність такого підходу напряму залежить від дотримання правил кібергігієни та розробки чітких інструкцій щодо того, яку саме інформацію дозволено обробляти у хмарному середовищі.

Література

1. Про затвердження Концепції інформатизації МВС України : Наказ МВС України від 10.02.2022 № 112. URL: https://zakon.rada.gov.ua/laws/show/z0988-23#Text
2. Копан Т. М., Скулиш В. Є. Цифровізація адміністративної діяльності поліції: сучасний стан та перспективи. Юридичний науковий електронний журнал. 2022. № 8. С. 340–343. URL: https://nals.com.ua/wp-content/uploads/2023/06/zvit_naprnu_2022.pdf
3. Цілвик А. В. Використання хмарних технологій у професійній діяльності працівників Національної поліції України. Інформаційні технології в правоохоронній діяльності. 2023. № 1. С. 110–115.
4. Копилов Е. В., Рибальченко Л. В. Інформаційне забезпечення діяльності підрозділів Національної поліції: сучасні виклики. Науковий вісник Дніпровського державного університету внутрішніх справ. 2023. № 2. С. 145–150. URL: https://er.dduvs.edu.ua/bitstream/123456789/15020/5/%D0%BC%D0%B0%D0%BA%D0%B5%D1%82_%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%2002.11.23.pdf

Обертайло Олександр Юрійович
здобувач другого «магістерського» рівня вищої освіти Одеського державного університету внутрішніх справ

ЕВОЛЮЦІЯ КРИМІНАЛЬНОГО АНАЛІЗУ

Розглядаючи становлення кримінального аналізу в його сучасному розумінні необхідно дослідити процес формування та еволюції цього напряму.

Одні вчені вважають, що кримінальний аналіз з'явився у Великобританії в середині XIX століття і полягав у класифікації злочинців та злочинів та розробці концепції методики роботи аналітиків щодо розслідування злочинів, пов'язаних із вбивствами. І історично його концепція полягала в порівнянні вчиненого правопорушеннями з іншими подібними випадками на основі наявної інформації та особистого досвіду правоохоронців [1, с. 11].

Так, у зв'язку зі зростанням злочинності та потребою у більш ефективних механізмах її протидії, частиною діяльності детективів лондонської поліції стало проведення класифікації злочинів і злочинців, розробка методики здійснення аналітичної діяльності під час розслідування вбивств.

У 1887 році досвід використання аналітичної діяльності поліцейських Великобританії почав розповсюджуватися та впроваджуватися в США.

Інші науковці прийшли до висновків, що практика аналізу злочинів і злочинності складалася задовго до цього, ще в часи давніх цивілізацій, адже підтримання правопорядку в містах тих часів також неможливо було б реалізувати без певного спостереження, моніторингу інформації та її осмислення, що по суті і було кримінальним аналізом в його сучасному розумінні. Саме на це вказує Гончарук О.М. «зерно аналізу злочинності – зерно настільки базове, що знадобилося десять тисяч років – від світанку

цивілізації до 1960-х років – щоб завдання отримало назву та професію» [2].

У витоків сучасної системи організації діяльності поліції та використання кримінального аналізу стоїть начальник поліції м. Берклі, що знаходиться в Сполучених штатах Америки, А. Вольмер, який на основі вивчення статистики минулих років запровадив картографічний метод для визначення місць концентрації злочинців та їх угруповань (1906 р.) [1, с. 11; 3]. Завдяки цьому методу, правоохоронці отримували інформацію, що давала змогу оптимізувати зусилля поліцейських підрозділів під час боротьби зі злочинними проявами, концентруючи їх в криміналь-них районах. Окрім того, слід відмітити і його заслуги по створенню системи обліку правопорушень, яка забезпечувала впорядкування поліцейської звітності, що полегшувало подальший аналіз інформації.

Зростання рівня злочинності, особливо організованої злочинності після Другої світової війни в США вплинуло на методи боротьби з нею і викликало зміни в законодавстві. Урядом були прийняті ряд законів, зокрема: 1946 рік – Hobbs Antiracketeering Act (закон Гоббса про боротьбу з рекетом), 1968 рік – Omnibus Crime Control and Safe Street Act (Закон про контроль над злочинністю та безпекою на вулицях); 1970 рік – Закон про контроль над організованою злочинністю. Така ситуація в країні призвела до поступового підвищення потреб в аналітичній підтримці правоохоронної діяльності, тому до штату поліцейських відділів поліції США включаються розвідувальні підрозділи, або аналітичні групи. Зокрема в цей період за ініціативи Р. Рейгана створено Національну комісію з вивчення діяльності організованої злочинності та надання рекомендацій при підготовці Національної стратегії боротьби з: організованою злочинністю.

У 1968 році у складі Міністерства юстиції США створюється Адміністрація сприяння правоохоронним органам (LEAA), яка забезпечувала спрямування федеральних коштів правоохоронним органам штатів та місцевій поліції, а також фінансування освітніх програм та досліджень. Завдяки таким ініціативам штати правоохоронних органів доповнювалися відділами кримінального аналізу.

В 1990 тих роках розвиток кримінального аналізу отримує новий поштовх, якому сприяла публікація професора Університету Вісконсіна Германа Гольдштейна (Herman Goldstein), «Проблемно-орієнтована поліцейська діяльність» (Problem Oriented Policing (POP)). Проблемно-орієнтована поліцейська діяльність стала інноваційною моделлю, яку активно впроваджували в свою діяльність поліцейські підрозділи. Її метою було підвищення ефективності поліцейських операцій шляхом зосередження уваги на проблемі злочинності загалом, а не на окремому злочині, і на способах усунення причин, які сприяли злочинності. Гольдштейн відмітив, «розглядаючи інциденти, поліцейські зазвичай мають справу з найбільш очевидними, зовнішніми проявами глибшої проблеми, а не з самою проблемою. Вони можуть припинити бійку, але не брати участь у дослідженні факторів, які сприяли цьому... Вони можуть розслідувати злочин, але не досліджувати чинники, які могли сприяти його вчиненню, за винятком тих випадків, коли вони стосуються ідентифікації правопорушника...» [4, с. 33].

В подальшому у 1985 році Бюро сприяння правосуддю (Bureau of Justice Assistance (BJA)) Національного інституту правосуддя США розробляє Комплексну програму затримання злочинців (Integrated Criminal Apprehension Program – ICAP). Ця комплексна програма планування, патрулювання та розслідувань, спрямованої на покращення затримання правопорушників поліцією – містила цілі та завдання, критичні елементи, етапи, можливі проблеми впровадження, а також досвід та очікувані результати.

Метою Програми ICAP стало навчання керівників поліції використовувати та аналізувати інформацію для сприяння ефективному прийняттю рішень.

Метод прийняття рішень ICAP включає: збір даних; аналіз (аналіз злочинності, аналіз розвідувальних даних та аналіз операцій); планування; надання послуг.

Цілями програми ICAP є підвищення рівня розкриття насильницьких злочинів та збільшення кількості арештів та переслідувань рецидивістів, на основі покращення практичної діяльності завдяки використанню

аналізу даних та вдосконалення управлінських можливостей, підвищення ефективності спрямування ресурсів та акцентом на боротьбу з тяжкими злочинами [5].

В 90-х роках XX ст. з розквітом науки та технологій, активного розвитку інформаційного суспільства продовжили змінюватися методи діяльності поліції. Протидія злочинності потребувала нових масштабів та співробітництва тож було утворено Міжнародну асоціацію кримінальних аналітиків – International Association of Crime Analysts (IACA) [6], Дана асоціація це організація заснована на волонтерських некомерційних засадах задля навчання та наданням професійних можливостей аналітикам кримінальної розвідки всього світу та налагодженням зв'язків у спільноті.

Основною метою діяльності IACA є надання допомогти аналітикам правоохоронних органів для боротьби зі злочинністю, підвищення їх кваліфікації, підвищення стандартів роботи та техніки в професії кримінального аналітика.

Діяльність Міжнародної асоціації кримінальних аналітиків вплинула на формування глобальної стратегії та напрямів діяльності кримінальних аналітиків, а також сприяла оформленню кримінального аналізу як окремої професії.

В результаті цих процесів, такі організації як Інтерпол, Європол мають в своїй структурі підрозділи кримінального аналізу та ґрунтують свою діяльність на аналітичних технологіях і результатах.

Основою діяльності Європолу є саме аналіз. Цей правоохоронний орган в своїй діяльності користується сучасними спеціалізованими системами для швидкого та безпечного зберігання, пошуку, візуалізації та зв'язування інформації. Кримінальні аналітики Європолу щодня використовують найсучасніші інструменти для супроводу розслідувань, що проводяться правоохоронними органами держав-членів та вважаються найкращими у Європі [7].

В Європейському союзі (далі – ЄС) еволюція правоохоронної діяльності призвела до появи нового підходу у протидії організованій

злочинності, якому наразі віддали перевагу та який ґрунтується на інформації, яка є продуктом проведеного аналізу – Intelligence Led Policing (далі – ILP) та в подальшому використовується як інструмент у боротьбі та попередженні злочинності.

Правоохоронна діяльність, керована аналітикою є внутрішньою філософією сучасної поліцейської діяльності, яка зміщує акцент роботи поліції від роботи по факту (реагування на злочини) до превентивних заходів, дій на недопущення чи попередження злочинної діяльності. ILP та використання кримінального аналізу пов'язуючи різні компоненти (ознаки, місця, об'єктів, суб'єктів, злочини), визначати тенденції та певний стиль чи почерк злочинної діяльності, розширяє правоохоронцям горизонт, дозволяючи бачити картину повністю [8].

Як зауважив І. А. Федчак «традиційно термін «intelligence» у нас перекладають як «розвідка» чи «розвідувальний», хоча його реальний сенс набагато глибший, адже йдеться про здобуття первинних розвідувальних, оперативних даних у результаті аналітичної обробки та формулювання аналітичних висновків. У світі існують різні моделі та стратегії поліцейської розвідки, наприклад, у Великобританії - National Intelligence Model, у США - National Criminal Intelligence Sharing Plan, є канадська модель SLEIPNIR тощо [1, с. 13].

В основу ILP лягли праці плеяди фахівців та спеціалістів. Наприклад, E. Drexel Godfrey, який був дослідником в сфері соціальних наук та мав ступінь доктора. В період з 1957 по 1970 рік він керував відділом поточної розвідки ЦРУ. В подальшому з 1974 року в Університеті Рутгерса заснував програму магістратури з державного управління та очолював її.

У співавторстві з Don R. Harris E. Drexel Godfrey у 1971 році розробив і підготував видання «Basic Elements of Intelligence: A Manual of Theory, Structure and Procedures for Use by Law Enforcement Agencies Against Organized Crime» (Основні елементи розвідки: Посібник з теорії, структури та процедур для використання правоохоронними органами у боротьбі з організованою злочинністю) [9].

За авторством Marilyn B. Peterson, Robert C. Fahlman, Simon Robertson, Leo M. Jacques, Danny L. Taylor, Міжнародною асоціацією аналітиків розвідки правоохоронних органів (International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA)) опубліковано посібник «Intelligence Led Policing: Getting Started» (Поліцейська діяльність на основі розвідки: Початок роботи) [10].

Howard Atkin опублікував «Intelligence 2000: revisando los elementos básicos» (Розвідка 2000: огляд основ) [11].

Асоціація підрозділів розвідки правоохоронних органів Law Enforcement Intelligence Unit (LEIU) розробила «Criminal Intelligence File Guidelines» (Керівні принципи щодо файлів кримінальної розвідки), завданням яких стало сприяння професіоналізму, забезпечення захисту конфіденційності громадян та надання правоохоронним органам можливості збирати інформацію для переслідування організованих злочинних утворень. Ці рекомендації окреслюють стандарти структури файлів, які органи можуть використовувати як систему стримувань і противаг. Керівні принципи щодо роботи з файлами включають визначення файлу кримінальної розвідки; його вміст, критерії, статус; оцінку інформації, класифікацію та джерела; контроль якості, а також поширення, перегляд, очищення та безпеку файлів [12].

Управління Організації Об'єднаних Націй з питань наркотиків та злочинності (United Nations Office on drugs and crime) підготовили свою версію Посібника з кримінальної розвідки для керівників (Criminal Intelligence Manual for Managers) [13]. В Посібнику розглянуто: процес розвідки, приклад національної моделі розвідки Великобританії, оцінку джерел та даних, аналіз та його види, аналітичний процес, питання управління розвідувальним підрозділом, стандарти діяльності та надано рекомендації.

В свою чергу Посібник ОБСЄ з поліцейської діяльності на основі розвідувальних даних (OSCE Guidebook Intelligence-Led Policing) детально досліджує Процес кримінальної розвідки, Проблеми та ключові вимоги до впровадження ILP, механізм кримінальної розвідки на різних рівнях, розглядає різні національні моделі, приділяє увагу особливостям ILP у запобіганні та протидії тероризму та екстремізму [14].

Зазначені та інші наукові розробки та практичні напрацювання підтвердили необхідність залучення фахівців з кримінальної розвідки до боротьби зі злочинністю, сприяли формуванню та розвитку нових підходів і стандартів як кримінального аналізу та і загалом правоохоронної діяльності, керованої аналітикою.

Для забезпечення ефективності діяльності правоохоронних органів залучення фахівців з кримінального аналізу дозволяє отримати глибше розуміння кримінального середовища, оперативної ситуації, підібрати дієві методи протидії злочинності. Отримана аналітична інформація дозволяє ефективно використовувати наявні активи та ресурси, допомагає побудувати стратегію майбутніх дій, працювати на упередження.

В результаті аналітичного процесу формуються знання, які слід брати за основу під час вироблення і прийняття рішення та визначення відповідних цілей (суб'єктів, злочинних груп або організацій) для ініціювання кримінальних розслідувань. Отримана інформація (дані) використовуються не лише для забезпечення відповідної підтримки оперативних операцій та кримінального провадження, а й задля забезпечення раціонального управління та розподілу ресурсів правоохоронних структур, прогнозування загроз для суспільства [1, с. 14].

Література

1. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.
2. Гончарук О.М. Зародження та еволюція формування кримінального аналізу в світовій парадигмі правоохоронної діяльності. Південноукраїнський правничий часопис. 2023. №1. С. 130-137. DOI https://doi.org/10.32850/sulj.2023.1.23
3. Oliver, Willard M. August Vollmer: the father of American policing / Willard M. Oliver. Description: Durham : Carolina Academic Press, LLC. 2017. URL: https://cap-press.com/pdf/9781611635591.pdf
4. Goldstein H. ProblemOriented Policing. New York: McGrawHill. 1990. 33 p.

5. U.S.Department of Justice. Office of Justice Programs. Integrated Criminal Apprehension Program (ICAP) URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/integrated-criminal-apprehension-program-icap
6. International Association of Crime Analysts. URL: https://www.iaca.net/about
7. About Europol. URL: https://www.europol.europa.eu/about-europol
8. EUAM-Ukraine. URL: https://www.euam-ukraine.eu/news/opinion/intelligence-led-policing-the-cutting-edge-of-modern-law-enforcement/
9. Edwin Drexel Godfrey, Don R. Harris Basic Elements of Intelligence: A Manual of Theory, Structure and Procedures for Use by Law Enforcement Agencies Against Organized Crime. URL: https://books.google.com.ua/books?id=gjY3hQ5M6UcC&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
10. Marilyn B. Peterson, Robert C. Fahlman, Simon Robertson, Leo M. Jacques, Danny L. Taylor, «Intelligence Led Policing: Getting Started». URL: https://www.ialeia.org/docs/Intelligence_Led_Policing-Getting_Started.pdf
11. Atkin, H. (2009). Intelligence 2000: revisando los elementos básicos. In C. Reppalli (Ed.), Inteligencia Criminal en el Siglo XXI (pp. 119-126). Grafica Sur Editora SRL, Buenos Aires. URL: https://pure.hud.ac.uk/en/publications/intelligence-2000-revisando-los-elementos-b%C3%A1sicos/
12. Law Enforcement Intelligence Unit (LEIU) «Criminal Intelligence File Guidelines». URL: https://ncirc.bja.ojp.gov/sites/ g/files/xyckuh326/files/media/document/criminal_intel_file_guidelines.pdf
13. Criminal Intelligence Manual for Managers. United Nations Office on drugs and crime. 2011 URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf
14. OSCE Guidebook Intelligence-Led Policing) URL: https://www.osce.org/sites/default/files/f/documents/d/3/327476.pdf

Овдійчук Денис

здобувач вищої освіти ступеня бакалавр факультету №1 (з підготовки фахівців для органів досудового розслідування Національної поліції України) Львівського державного університету внутрішніх справ

Баб'як Андрій Васильович

завідувач кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

В умовах глобалізації злочинності, швидкого розвитку інформаційних технологій та зростання обсягів даних, що підлягають обробці, ефективність досудового розслідування безпосередньо залежить від якості його інформаційно-аналітичного забезпечення. Національна поліція України, як основний орган у сфері протидії злочинності, стикається з необхідністю постійного вдосконалення методів збору, обробки, аналізу та використання оперативної та слідчої інформації. Це особливо актуально з огляду на вимоги Кримінального процесуального кодексу України щодо розумних строків розслідування та забезпечення принципу законності та справедливості, а також досягнення цілей кримінального провадження у частині всебічного, повного та неупередженого розслідування.

Історія розвитку інформаційно-аналітичної роботи в правоохоронних органах становить понад триста років і умовно її можна поділити на п'ять основних етапів: початок XVIII ст. – жовтень 1917 р.; жовтень 1917 р. – середина 50-х рр. XX ст.; середина 50-х рр. XX ст. – початок 90-х рр. XX ст.; початок 90-х рр. XX ст. – 19 листопада 2012 р.; 20 листопада 2012 р. – наші дні.

Нормативною базою для ІАЗ слугують Конституція України, Кримінальний процесуальний кодекс України (КПК) та Закон України «Про

Національну поліцію». Основним інструментом фіксації та обліку інформації є Єдиний реєстр досудових розслідувань (ЄРДР), який, згідно з дослідженнями, є не лише обліковою, а й потужною аналітичною платформою. Проте, як зазначає В.В. Ковальчук, чинне законодавство потребує деталізації щодо використання непроцесуальних джерел інформації та аналітичних продуктів у процесі доказування [1].

Організаційна структура ІАЗ передбачає створення спеціалізованих аналітичних груп або залучення аналітиків для підтримки слідчих та детективів [2, с. 14]. Основні форми аналізу включають:

1. Поточний аналіз (моніторинг відомостей, що надходять у ході розслідування).
2. Стратегічний (прогнозний) аналіз (виявлення тенденцій злочинності, профілювання та моделювання).
3. Криміналістичне профілювання та аналіз зв'язків (Link Analysis), особливо важливі при розслідуванні організованої та економічної злочинності [3].

Ефективне ІАЗ неможливе без впровадження новітніх інформаційних технологій. Актуальним є використання систем, що працюють з великими даними (Big Data) та елементами штучного інтелекту (ШІ) для:

– Автоматизованої ідентифікації зв'язків між об'єктами (особи, події, фінансові операції) [4].

– Прогнозного моделювання місця та часу вчинення майбутніх злочинів (геоінформаційний аналіз) [5, с. 22].

– Аналізу фінансових потоків та відновлення електронної комунікації (*Digital Forensics*) [6].

Впровадження таких інструментів, як зазначають експерти, дозволяє перевести досудове розслідування на якісно новий рівень, мінімізуючи вплив людського фактору на етапі обробки великих масивів інформації.

Незважаючи на певний прогрес у розвитку інформаційно-аналітичного забезпечення (ІАЗ), підрозділи досудового розслідування Національної поліції України зіштовхуються з низкою системних проблем.

Передусім, це стосується кадрового забезпечення: спостерігається гострий дефіцит кваліфікованих аналітиків, а також недостатній рівень ІТ-компетентності слідчого складу, що ускладнює ефективне використання наявних інформаційних ресурсів. Додатковою перешкодою є технічні та програмні недоліки, які проявляються у застарілому обладнанні, значній несумісності відомчих баз даних та, що є критично важливим, відсутності єдиної інтегрованої аналітичної платформи для консолідації всієї оперативної та слідчої інформації. Нарешті, ефективність ІАЗ істотно знижується через недостатню міжвідомчу взаємодію, що виражається у слабкому обміні інформацією між підрозділами НПУ та іншими ключовими правоохоронними структурами (СБУ, НАБУ, ДБР), що, у свою чергу, призводить до втрати цінних даних та дублювання функцій [7].

Для забезпечення суттєвого якісного стрибка в інформаційно-аналітичному забезпеченні (ІАЗ) досудового розслідування необхідно реалізувати комплекс взаємопов'язаних заходів. Насамперед, ключовим організаційним кроком є створення Єдиного Аналітичного Центру у структурі Національної поліції України, який функціонуватиме на засадах уніфікованих стандартів збору, верифікації та обробки даних, що дозволить ефективно інтегрувати розрізнені масиви інформації в єдине аналітичне поле. Не менш важливим є вирішення кадрової проблеми через розробку та впровадження спеціалізованих освітніх програм для підготовки нового типу фахівців — так званих слідчих-аналітиків. Ці спеціалісти повинні мати поглиблені знання не лише в кримінальному процесі, а й у критично важливих галузях, таких як кібербезпека, Big Data та методи прогнозної аналітики. Крім того, задля забезпечення прозорості та ефективності використання ресурсів доцільно запровадити систему регулярного аудиту, яка б оцінювала результативність застосування наявних інформаційних ресурсів та якість підготовлених аналітичних продуктів у щоденній практиці досудового розслідування [8]. І, нарешті, необхідна гармонізація чинного законодавства, що передбачає чітке врегулювання процесуального статусу аналітичних звітів, дозволяючи використовувати їх як обґрунтовану основу для прийняття процесуальних рішень та планування комплексу слідчих (розшукових) дій.

Ефективність досудового розслідування в сучасних умовах критично залежить від якості інформаційно-аналітичного забезпечення (ІАЗ), яке використовує як традиційні інструменти (ЄРДР), так і новітні технології (Big Data, ШІ, Link Analysis). Незважаючи на значний потенціал, впровадження ІАЗ стримується системними проблемами, зокрема кадровим дефіцитом, несумісністю технічних платформ та недостатньою міжвідомчою взаємодією. Для кардинального підвищення ефективності розслідування необхідно здійснити комплексні реформи: створити Єдиний Аналітичний Центр, запровадити спеціалізовану підготовку слідчих-аналітиків та гармонізувати законодавство для надання аналітичним звітам належного процесуального статусу.

Література

1. Ковальчук В. В. Використання аналітичної інформації в досудовому розслідуванні: питання правового регулювання. Право України. 2022. № 1. С. 102–110.
2. Лисенко В. В. Організація аналітичної роботи в підрозділах досудового розслідування: монографія. Київ: Атіка, 2021. 230 с.
3. Клименко А. М. Link Analysis як метод виявлення організованої злочинності. Форум права. 2019. № 54. С. 34–40. URL: http://nbuv.gov.ua/j-files/FP_index.htm
4. Шевченко М. І. Big Data у кримінальному процесі: перспективи та ризики. Тези доповідей Міжнародної науково-практичної конференції. Одеса: Видавництво ОДУВС, 2021. С. 15–17..
5. Савченко О. Л. Прогнозна аналітика злочинності на основі геоінформаційних систем. Науковий вісник публічного та приватного права. 2020. № 3. С. 20–25.
6. Вереша Р. В. Digital Forensics у розслідуванні кіберзлочинів: практ. посіб. Львів: СПОЛОМ, 2019. 350 с
7. Петров С. А. Міжвідомча взаємодія у сфері інформаційного обміну: адміністративно-правові аспекти. Вісник Харківського національного університету внутрішніх справ. 2019. № 2. С. 120–126.
8. Бабенко А. І. Аудит ефективності використання інформаційних ресурсів у поліції. Вісник Національної академії прокуратури України. 2021. № 4. С. 90–98.

Огірко Ольга Ігорівна
професор кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ШТУЧНИЙ ІНТЕЛЕКТ В ОПТИМІЗАЦІЇ ВИКЛАДАННЯ ДИСЦИПЛІН СПЕЦІАЛЬНОСТІ F6 ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ У ЗВО ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Впровадження штучного інтелекту (ШІ) у навчальний процес є одним із найбільш перспективних напрямів трансформації сучасної вищої освіти. У контексті підготовки фахівців зі спеціальності F6 Інформаційні системи і технології, ШІ виступає не лише об’єктом вивчення, а й потужним інструментом інтелектуальної підтримки, що дозволяє оптимізувати взаємодію між викладачем та здобувачем вищої освіти.

Особливого значення це набуває у ЗВО зі специфічними умовами навчання, де освітній процес поєднує сувору регламентацію з інтенсивною практичною підготовкою. Технології ШІ дозволяють персоналізувати навчання, автоматизувати рутинну навчально-методичну роботу та підвищити ефективність засвоєння складного теоретичного матеріалу в межах чітко структурованого середовища.

Адаптивні системи на основі ШІ забезпечують індивідуальний темп вивчення тем, автоматизований підбір завдань різного рівня складності та миттєвий зворотний зв’язок. Для системної інтеграції цих технологій важливо враховувати як переваги автоматизації, так і виклики, пов'язані з етикою, кібербезпекою та технічною реалізацією. Це важливо для закладів, де вимоги до об'єктивності оцінювання та захисту даних є пріоритетними. Порівняльний аналіз ключових аспектів використання ШІ наведено у таблиці.

Таблиця 1

Аналіз ефективності та ризиків використання ШІ в освітньому процесі

Категорія	**Переваги**	**Недоліки та ризики**
Ефективність та оцінювання	Використання стандартизованих алгоритмів забезпечує високу об'єктивність, повністю виключаючи суб'єктивні упередження. Автоматизація дозволяє досягти значної економії часу при перевірці великих обсягів робіт. Системи демонструють високу надійність, оскільки вони не піддаються впливу втоми чи емоцій.	Існує ризик помилок та надання неадекватних відповідей на складні завдання, що потребують глибокого розуміння. Низька якість даних може призвести до системних помилок через залежність результату від точності вхідної інформації.
Індивідуалізація навчання	ШІ дозволяє будувати персональні траєкторії, адаптуючи рівень складності завдань під можливості кожного студента. Функція прогнозування допомагає вчасно виявляти здобувачів, які потребують додаткової допомоги.	Спостерігається відсутність гнучкості, оскільки ШІ менш адаптивний до специфічних ситуацій порівняно з викладачем. Існує загроза обмеження креативності, бо система часто пропонує лише набір

		готових, алгоритмічних рішень.
Доступність та інклюзія	Забезпечується цілодобовий доступ (24/7) до навчальних матеріалів у будь-якому місці. Технології пропонують підтримку особливих потреб.	Виникає технічний розрив і нерівність через різний рівень доступу студентів до сучасних гаджетів. Висока вартість інтеграції та підтримки інфраструктури може бути обтяжливою для бюджету закладу.
Мотивація та взаємодія	Впровадження елементів гейміфікації значно підвищує зацікавленість та залученість студентів. Миттєвий зворотний зв'язок дозволяє швидко отримувати рекомендації та коригувати процес навчання.	Можлива втрата соціальних навичок через обмежену взаємодію всередині групи. Відсутність емпатії.
Етика та безпека	Забезпечується повна прозорість критеріїв, оскільки всі стандарти оцінювання є чітко визначеними та незмінними.	Виникають серйозні ризики щодо конфіденційності та безпеки персональних даних. Існують етичні питання щодо можливої прихованої дискримінації в алгоритмах ШІ.

Роль викладача	Педагог отримує звільнення від рутини, що дає змогу зосередитися на творчих, наукових та менторських аспектах роботи.	Можливе відчуття зниження статусу викладача та ризик деградації педагогічних навичок через надмірну залежність від технологій.

(складено автором на основі [1-3])

Представлений аналіз підтверджує, що для спеціальності F6 Інформаційні системи і технології інтеграція ШІ є необхідною, оскільки дозволяє здобувачам вищої освіти опановувати інструменти розробки та аналітики безпосередньо в освітньому процесі.

У ЗВО зі специфічними умовами навчання впровадження ШІ сприяє зміцненню дисципліни та прозорості оцінювання, водночас вимагаючи підвищеної уваги до кібербезпеки та захисту персональних даних. Оптимальною моделлю є синергія (гібридне навчання): ШІ виконує функцію адаптивного тренажера та інструменту автоматизації рутинних завдань, тоді як викладач зберігає ключову роль ментора. Це дозволяє зосередитися на формуванні у здобувачів критичного мислення та здатності приймати відповідальні рішення у складних ситуаціях, де технології не можуть замінити глибоку професійну взаємодію.

Література

1. Запорожець Т.В. Застосування інтелектуальних технологій та систем штучного інтелекту для підтримки прийняття управлінських рішень. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. 2020. Т.31 (70), No2. С.79–85
2. Пікуляк М.В., Савка І.Я, Дутчак М.С. Використання апарату нейромереж для дослідження адаптивної навчальної траєкторії. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2022. Вип.47. С. 91–97
3. Трифонова О.М., Садовий М.І. Інформаційні технології в наукових дослідженнях. Педагогічні науки. Херсон, 2022. Вип.98. С.27–34

Остапів Назар Вікторович

здобувач освіти ліцею імені Тараса Городецького Шептицької міської ради

Корольчук Світлана Ярославівна

завідувач лабораторії програмування кафедри програмування Львівського національного університету імені Івана Франка

Мельничин Дмитро Володимирович

асистент кафедри програмування Львівського національного університету імені Івана Франка

ДО ПИТАННЯ ПІДВИЩЕННЯ ЯКОСТІ ОСВІТИ ШЛЯХОМ ПЕРСОНАЛІЗАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний стан справ в Україні негативно впливає не тільки різні соціальні галузі, а й на систему освіти. У зв’язку з цим багато закладів освіти змушені були перейти на змішаний чи дистанційний формат навчання. Це призвело до значного погіршення якості освіти та створило нові виклики для вчителів: як ефективно передавати знання онлайн, утримувати увагу учнів та персоналізувати навчання в умовах обмежених ресурсів.

З огляду на сказане виникає потреба в інноваційних рішеннях для покращення ситуації. Метою даної роботи було створення інструменту, який допомагає вчителям, використовуючи можливості штучного інтелекту та сучасних інформаційних технологій, якісніше подавати навчальний матеріал та зменшує обсяг часу для його підготовки.

У ході роботи було проведено порівняльний аналіз наявних освітніх платформ та технологій, опитано вчителів щодо необхідного функціоналу та викликів, з якими вони стикаються в процесі підготовки та проведення уроків, проаналізовано значну кількість технологій і обрано краще рішення для забезпечення стійкої роботи в умовах нестабільного інтернет-з'єднання. Опитування щодо актуальності продукту та затребу-

ваного функціоналу проводилося на базі ліцею імені Тараса Городецького Шептицької міської ради. Воно проводилось серед учнів десятих-одинадцятих класів та різних вчителів-предметників. Метою опитування було визначення рівня затребуваності проєкту серед цільових аудиторій, поширення проблеми при використанні існуючих освітніх технологій та виявлення рівня комфортності використання вчителями наявних освітніх технологій.

На рис. 1 наведено результати опитування щодо корисності запропонованого додатку для педагогічної практики. (в опитуванні взяли участь двадцять три респонденти).

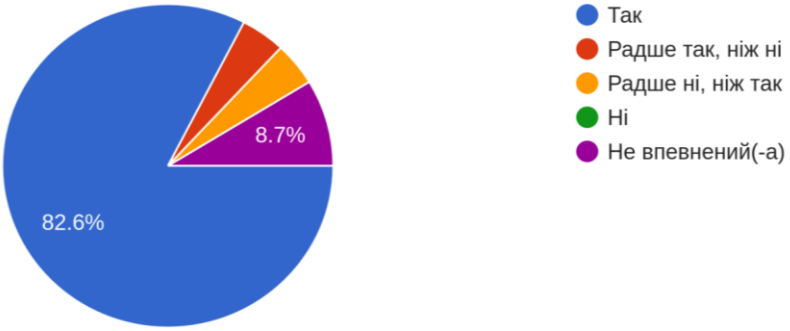

Рис. 1. Затребуваність додатку серед учителів

Також користь використання даного застосунку оцінили тридцять п'ять учнів. Результати можна побачити на діаграмі (див. рис. 2).

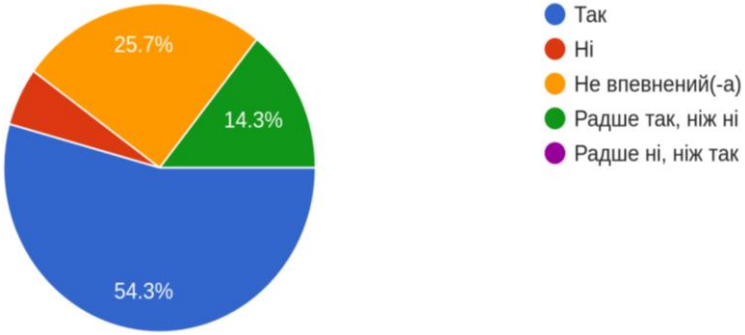

Рис. 2. Затребуваність додатку серед учнів

Наступне опитування, для усіх респондентів загалом, стосувалося ергономіки та комфорту використання існуючих новітніх освітніх технологій (див. рис. 3).

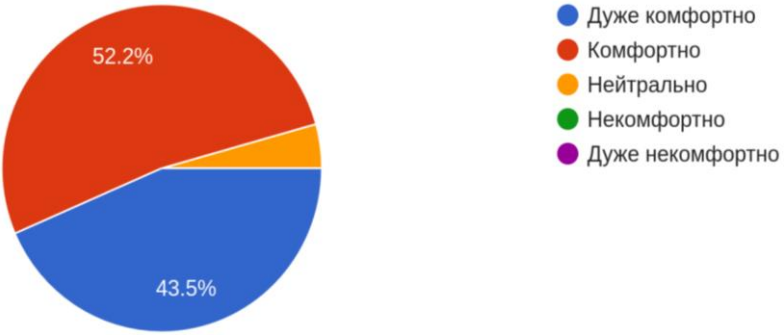

Рис. 3. Результати опитування щодо комфорту використання запропонованих на ринку освітніх технологій

Результати опитування яскраво демонструють гостру потребу педагогічної спільноти у спеціалізованому освітньому застосунку. Ґрунтовний аналіз відповідей респондентів виявив системну проблему – хоча на ринку присутні різноманітні освітні платформи загального призначення, жодна з них не пропонує комплексного рішення для специфічних потреб вчителів. Зокрема, педагоги відзначили відсутність інструментів для швидкого створення інтерактивного контенту з актуальними даними, неможливість ефективної персоналізації матеріалів відповідно до різних рівнів підготовки учнів, та брак механізмів для підтримки активного дослідження через необмежену кількість запитань.

Ця нестача критично важливого функціоналу у існуючих рішеннях обґрунтовує необхідність створення спеціалізованої навчальної платформи.

Головним функціоналом даної розробки є:

– автоматичне структурування тексту, взятого з презентації або субтитрів відео з мережі YouTube, або ж наданого вручну вчителем;
– створення конспектів та цифрових подкастів на основі тексту;
– відповіді на запитання учнів та відображення їх вчителеві;

– створення тестів на базі запитань учнів та текстових версій уроків;
– створення відео на основі презентацій;
– створення презентації на основі наданого тексту.

Для такого додатку надважливим є інтуїтивний інтерфейс, оскільки в іншому випадку використання даного продукту буде доволі низьким через високий поріг входу. Крім того, особливу увагу приділено відображенню інформації. Так, для кращої візуалізації текстової та графічної інформації, використовується технологія *markdown*, яка дозволяє доволі гнучко редагувати вигляд тексту, додавати різноманітні додаткові матеріали до цього за типом зображення.

Приклади основних сторінок розробленої вебплатформи наведено на рис. 1-2.

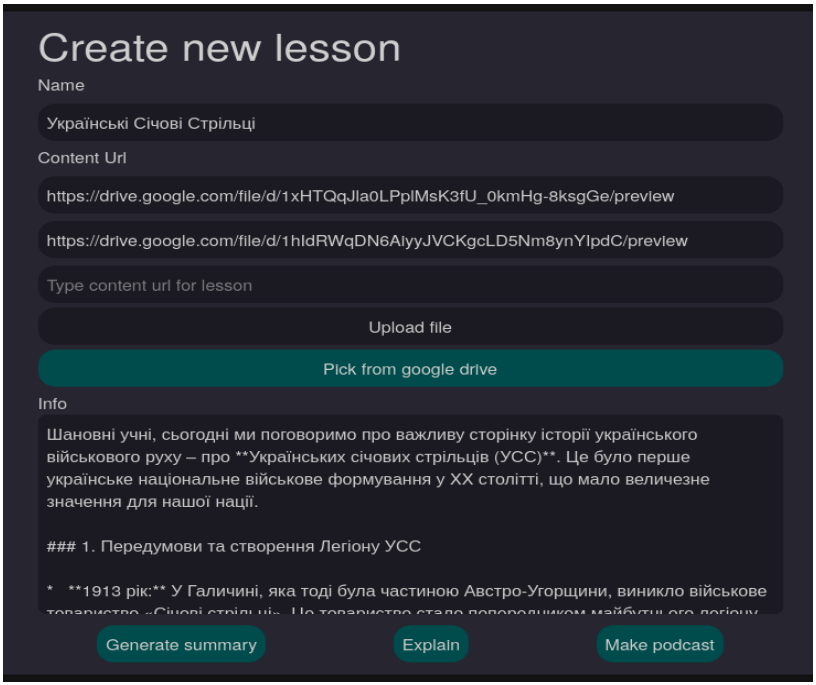

Рис. 4. Приклад сторінки створеного уроку з структурованим текстом.

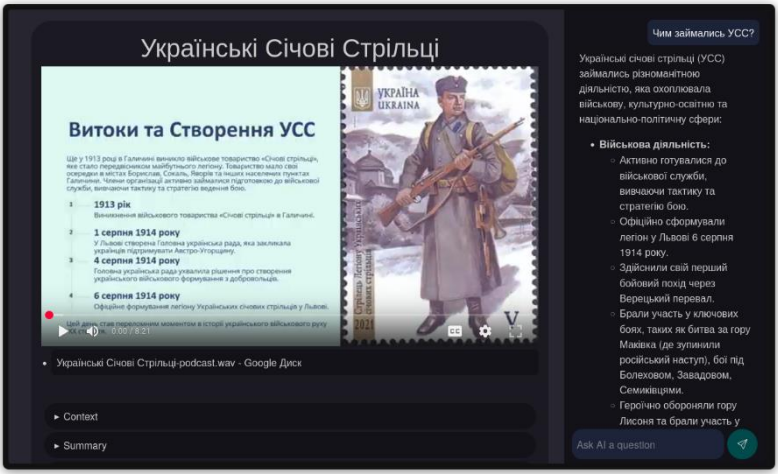

Рис. 5. Приклад сторінки перегляду уроку з відповіддю на запитання

Основним засобом реалізації продукту є фреймворк *Blazor WebAssembly* від *Microsoft*. Використання цієї технології дає можливість використання сервісу з обмеженим доступом до інтернету, оскільки він необхідний тільки для завантаження контенту. В якості штучного інтелекту було використано *Gemini*, що є моделлю від компанії *Google*.

Запропонована розробка – це веб платформа для вчителів, що автоматизує рутинні задачі в створенні уроків та допомагає їх персоналізувати. Вона дозволяє автоматично генерувати конспекти, подкасти та презентації, інтегрується з наявними презентаціями та *YouTube* відео, забезпечує *AI*-асистента для відповідей на запитання учнів з автоматичним аналізом проблемних тем, а також створює та перевіряє тести різних типів.

Література

1. Han S. (2022). Flipped classroom: Challenges and benefits of using social media in English language teaching and learning. Frontiers in Psychology, 13, 996294. Режим доступу URL : https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.996294/full.

2. O. Zawacki-Richter, V. I. Marín, M. Bond & F. Gouverneur (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? International Journal of Educational Technology in Higher Education, 16(1), 39. Режим доступу URL : https://link.springer.com/article/10.1186/s41239-019-0171-0.
3. UNESCO. (2021). AI and education: guidance for policy-makers. Режим доступу URL : https://unesdoc.unesco.org/ark:/48223/pf0000376709
4. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). Intelligence Unleashed: An argument for AI in Education. Pearson Education. Режим доступу URL : https://www.pearson.com/content/dam/corporate/global/pearson-dot-com/files/innovation/Intelligence-Unleashed-Publication.pdf.

Остапчук Дарія Миколаївна

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ДЕФІЦИТ ПРОГНОЗІВ: ПРОБЛЕМНІ АСПЕКТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Розвиток інформаційних технологій впливає на всі сфери людської діяльності. Не є виключенням й державна політика у сфері забезпечення національної безпеки. Інформаційно-аналітична підтримка дій сил безпеки дає змогу виконувати їх з достатньою ефективністю та як результат – забезпечити державну безпеку на потрібному рівні. Розвиток

інформаційно-аналітичного забезпечення складових сектору безпеки і оборони України має відповідати сучасним і прогнозованим геостратегічним, соціально-політичним, економічним і військово-технічним загрозам та забезпечувати максимальну ефективність і здатність давати адекватну відповідь реальним і потенційним викликам державній безпеці України [1, с. 379].

До основних тенденцій державного управління у сфері державної безпеки можна віднести:

а) модернізацію сил безпеки і оборони за допомогою цифрових технологій, що дає їм змогу швидко обмінюватися інформацією; координувати дії та підвищувати ефективність дій за призначенням; унеможливити негативні кібернетичні впливи, які здатні впливати на роботу критично важливих інфраструктур, та вести інформаційні операції;

б) використання штучного інтелекту для аналізу великих обсягів даних, управління системами зброї та моделювання службово-бойових дій;

в) стрімкий розвиток інформаційних технологій, що дає змогу зібрати точну і актуальну інформацію про стан сил безпеки, їх службово-бойову діяльність, підвищуючи оперативну обізнаність і реактивність сил;

г) використання інтелектуальних систем високоточного озброєння, що дає змогу ефективно вражати цілі з мінімальними колатеральними втратами [2].

Інформаційні технології охоплюють широкий спектр технологій та систем, які використовуються для створення, зберігання, обміну та обробки інформації. До ключових властивостей, які характеризують інформаційні технології, належать: швидкість обробки інформації; зберігання та доступ до даних; комунікація; автоматизація; масштабованість; складні заходи безпеки; інтегрованість різних систем і програм, поліпшуючи взаємодію між різними відділами та оптимізуючи робочі процеси; підтримка прийняття рішень. Реалізація властивостей інформаційно-аналітичної системи забезпечення процесів управління сил безпеки дає змогу додати потрібних якостей управлінській інформації.

Отриманий ефект безпосередньо характеризується відповідними показниками інформаційних складових, що використовуються у ході інформаційно-аналітичного забезпечення процесів управління військами (силами) [3, с. 64].

Критичні ситуації в зонах воєнно-політичного зіткнення зобов'язують керівників органів державного управління ухвалювати сміливі рішення щодо організації заходів безпеки за умов браку часу, обмеження фінансових та матеріальних ресурсів та проблематичності ситуації. До того ж, відбуваються процеси щодо зростання ризиків виникнення надзвичайного стану природного, техногенного соціального та військового характеру. За цих обставин, значно зростає роль інформаційного забезпечення як для органів державного управління, під час прийняття управлінських рішень, так і для населення, яке має бути навченим щодо поведінки в екстремальних ситуаціях [4].

До основних проблем забезпечення інформаційної безпеки системи публічного управління належать, зокрема:

– відсутність усталеного поняття «інформаційна безпека»; забезпечення дієвого механізму функціонування систему електронного врядування, яка, на даний час не діє;

– формування інноваційних інформаційних небезпек, які потребують термінового та ефективного вирішення; забезпечення підготовки якісного кадрового складу систему публічного управління у сфері забезпечення інформаційної безпеки;

– відсутність дієвих механізмів забезпечення інформаційної безпеки; відсутність інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в публічному управлінні.

Однією з актуальних проблем планування та управління в сфері забезпечення національної безпеки й одночасно перспективним напрямом їхнього розвитку є проблема розробки та включення в ці процеси процедур адаптації до змін ситуації, оскільки заздалегідь передбачити всю сукупність факторів впливу на безпеку, їхні взаємозв'язки та динаміку змін у стратегічній перспективі принципово неможливо. Згідно з базовим принципом «гнучкості» («безупинної адаптації») планування й управління

повинні мати здатність уточнювати спрямованість рішень при зміні умов діяльності сектору безпеки, включати механізми коригування планових величин для їхньої адаптації до зовнішніх обставин. Визначальну роль у вирішенні цієї проблеми відіграють процедури моніторингу та аналізу, а також зворотні зв'язки процесів планування та управління [5].

Зменшення рівня невизначеності при стратегічному плануванні та управлінні, а також надбання цими процедурами адаптивних якостей можна вирішити шляхом застосування керованих процедур стратегічного моніторингу та аналізу, генерування одночасно декількох альтернативних варіантів стратегічних рішень, включення механізмів призупинення та корекції стратегій, передбачення декількох режимів роботи системи стратегічного управління (одночасного застосування декількох методів стратегічного планування та управління) з оперативним переключенням на найбільш адекватний реальній обстановці режим тощо. Але найбільший позитивний ефект можна отримати тільки в разі комплексного використання вищевказаних процедур, хоча це й потребує додаткових часових та ресурсних витрат, а також наявності відповідного теоретико-методологічного апарату. Необхідність у корегуванні структури або/та параметрів системи ІАЗ може виникати як у ході формування стратегічних рішень, так і на етапі їхньої реалізації. При цьому необхідно враховувати відмінності «раціональних» і «надзвичайних» режимів формування та реалізації державно – політичних рішень [6].

Ефективне функціонування системи національної безпеки і оборони України критично залежить від оперативного та якісного інформаційно-аналітичного забезпечення. Наявні проблеми – відсутність єдиної інтегрованої системи, недосконалість правової бази та кадровий дефіцит – створюють значні ризики і знижують стійкість держави перед сучасними гібридними загрозами. Тому усунення цих проблемних аспектів є не просто питанням технічної модернізації, а нагальною стратегічною необхідністю, що вимагає комплексного державного підходу, належного фінансування та невідкладного впровадження стандартів і передового досвіду країн-партнерів для гарантування суверенітету та перемоги України.

Література

1. Sporyshev K. Theoretical basis of the information and analytical support development of the security forces of Ukraine: aspects of state governance. International security studios: managerial, technical, legal, environmental, informative and psychological aspects : international collective monograph. Oslo, Kingdom of Norway, 2024. Vol. I. Pp. 379-407.
2. Споришев К. О. Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України: теорія, методологія, практика : монографія. Одеса : Олді+, 2024. 314 с.
3. Споришев К. О. Аналіз стану системи інформаційно-аналітичного забезпечення сил безпеки України. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку : матеріали XLI Міжнар. наук.-практ. конф., м. Анкара, 07 лют. 2024 р. Київ : ГО «ВАДНД», 2024. С. 64–68.
4. Барило О. Г., Потеряйко С. П., Тищенко В. О. Інформаційне забезпечення органів державного управління у надзвичайних ситуаціях. Наук. вісн. Акад. муніцип. упр. Сер. Упр. : зб. наук. праць. Київ : АМУ. 2013. Вип. 4. С. 77–84.
5. Богданович В.Ю, Семенченко А.І. Метод обґрунтування варіантів стратегічних рішень у сфері забезпечення національної безпеки / Вісник державної служби. – 2007. – № 1. – С. 7-17.
6. Брайсон Джон М. Стратегічне планування для державних та неприбуткових організацій / Пер. з англ. Анжела Кам'янець. – Львів: Літопис, 2004. –352 с.

Палій Богдан

здобувач вищої освіти ступеня бакалавр факультету №1 (з підготовки фахівців для органів досудового розслідування Національної поліції України) Львівського державного університету внутрішніх справ

Баб'як Андрій Васильович

завідувач кафедрі оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ OSINT (РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ) В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Інформаційне забезпечення ОРД вийшло на новий рівень завдяки інтеграції сучасних ІТ-рішень. Особливої ваги набула технологія OSINT, яка перетворює масиви відкритих даних на розвідувальну інформацію. Джерелом такої бази слугують як соціальні платформи та медіа-ресурси, так і відкриті реєстри й супутникові знімки, що дозволяє формувати доказову базу без втручання в приватне життя.

Розвідка з відкритих джерел (OSINT) – це процес збирання, аналізу й використання інформації, отриманої із загальнодоступних джерел, для вирішення різних спеціальних завдань. У контексті ОРД (OSINT) є допоміжним інструментом, який дає змогу оперативним підрозділам швидко одержувати й перевіряти інформацію без залучення складних дозвільних процедур, які обмежують права і свободи громадян [1].

Розвідка з відкритих джерел є одним з методів що застосовується в комплексному напрямку ОРД – кіберрозвідки. У цьому розумінні такі методи застосовуються в:

– комп'ютерній розвідці – оперативно-розшуковий захід, який полягає у цілеспрямованому пошуку та отриманні інформації з комп'ютерних систем та мереж, доступ до яких не обмежується їх власником, володільцем чи розпорядником або не пов'язаний з подоланням системи

логічного захисту, що здійснюється працівниками оперативних та оперативно-технічних підрозділів з метою виявлення відомостей криміногенного та кримінального характеру;

– кримінологічній розвід, яка полягає у легальному зборі, аналізі, оцінці та інтерпретації інформації про криміналізацію суспільних відносин, загрози та ризики кримінального та криміногенного змісту, реальний стан злочинності, криміналітету, його статус і можливості протидіяти правопорядку, з метою забезпечення національної, громадської, групової та особистої безпеки [3].

Таким чином на відміну від традиційних способів ОРД, котрі обмежують певні права, OSINT використовує виключно доступні дані, такі, як відкриті бази даних і реєстри, засоби масової інформації (онлайн- та друковані видання), соціальні мережі (SOCMINT), аналітичні звіти та публічні дослідження, супутникові знімки та геопросторові дані (GEOINT). OSINT дає змогу виявляти зв'язки між особами, групами та подіями, оцінювати рівень загроз і відстежувати діяльність підозрюваних осіб без необхідності безпосереднього контакту з ними.

Розвідка з відкритих джерел часто інтегрується з іншими напрямами збирання оперативних даних, які застосовуються західними партнерами, зокрема: HUMINT (HumanIntelligence) – агентурна розвідка, що базується на особистих контактах; SIGINT (SignalsIntelligence) – перехоплення комунікаційних сигналів; COMINT (Communications-Intelligence) – аналіз змісту перехоплених повідомлень; IMINT (Imagery-Intelligence) – аналіз зображень, отриманих із супутників або безпілотних систем [6. 4]. Хоча відкриті джерела легше опрацьовувати, проте вони можуть бути менш точними, ніж інформація, здобута оперативним шляхом із закритих каналів.

Застосування технологій OSINT у сфері оперативно-розшукової діяльності спирається на комплекс методів, що дозволяють отримувати розвідувальну інформацію з відкритих джерел. До ключових інструментів збору даних належать:

– Медіа-моніторинг: системний аналіз контенту друкованих та інтернет-ЗМІ з метою виявлення індикаторів протиправної діяльності, суспільних тенденцій або загроз безпеці.

– SOCMINT (Social Media Intelligence): вивчення профілів та активності фігурантів у соціальних мережах (Facebook, Instagram, Telegram тощо) для встановлення їхніх контактів, планів та локації.

– Робота з реєстрами та базами даних: опрацювання відомостей із державних реєстрів, судових архівів та корпоративних баз для перевірки юридичних осіб, фінансових транзакцій та біографічних даних громадян.

– GEOINT (Geospatial Intelligence) (PeakFinder, PeakVisor): аналіз геопросторової інформації, включно із супутниковими знімками та геолокаційними мітками, для прив'язки об'єктів чи подій до конкретної місцевості.

– Веб-скрейпінг (Web Scraping): застосування автоматизованих алгоритмів для масового збору даних із сайтів, форумів та онлайн-платформ.

– Реверсивний пошук зображень: верифікація фотоматеріалів та ідентифікація зображених на них осіб чи предметів через спеціалізовані пошукові сервіси.

– Dark Web OSINT: моніторинг ресурсів тіньового сегмента інтернету для виявлення прихованої інформації, що становить оперативний інтерес [1. 6].

За ст. 1 Закону України «Про оперативно-розшукову діяльність» завданням оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України. Саме поняття пошук і фіксація передбачає здобуття інформації шляхом певних дій, включаючи хоч і не в законодавчому але в практичному розумінні застосування методів розвідки OSINT [2].

В результаті застосування цього методу пошуку здійснюється в межах загального законодавства: Конституцією України, яка гарантує правона захист особистої інформації, зокрема за ст. 32 [7]; Законом

України «Про інформацію» та «Про доступ до публічної інформації», що визначають принципи доступу до відкритих джерел [9, 5]; «Про захист персональних даних», який регламентує оброблення інформації про осіб [8]; Кримінальним процесуальний кодекс України, що встановлює вимоги до доказової бази [10].

Разом з тим, варто зауважити, що попри значний технологічний потенціал, практична імплементація OSINT стикається з низкою суттєвих перешкод: від поширення дезінформації та маніпулятивних матеріалів до активної протидії з боку злочинних угруповань, які використовують засоби шифрування й анонімізації.

Підсумовуючи, можна стверджувати, що розвідка за відкритими джерелами трансформувалася у критично важливий елемент сучасної оперативно-розшукової діяльності, який суттєво пришвидшує аналітичні процеси та розширює можливості оперативних та інших службових працівників. Однак для повноцінної інтеграції цього інструменту необхідне не лише впровадження новітніх технологій, таких як штучний інтелект та автоматизовані системи аналізу, але й створення чіткої законодавчої бази. Саме належне правове врегулювання дозволить забезпечити баланс між ефективністю заходів та дотриманням прав людини, а також гарантувати допустимість доказів, отриманих методом OSINT, у подальшому кримінальному провадженні.

Література

1. Bocharov S., Tyshchuk V., Bielai S. Use of OSINT in operational and investigative activities: tools and legal aspects. State security. 2025. T. 1, № 5. С. 25–30. URL: https://doi.org/10.33405/2786-8613/2025/1/5/336692 (дата звернення: 15.12.2025).
2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII : станом на 9 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 15.12.2025).
3. Басалик С. А., Туз О. С., Тищук В. В. Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності.

Український політико-правовий дискурс. 2025. № 9. URL: https://doi.org/10.5281/zenodo.15086041 (дата звернення: 15.12.2025).
4. Кудінов С. С., 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. № 3. С. 126–133. URL: https://doi.org/10.32782/2311-8040/2025-3-14 (дата звернення: 15.12.2025).
5. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 8 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 15.12.2025).
6. Задерейко О. Geoint: можливості геопросторової розвідки. Кіберпростір в умовах війни та глобальних викликів xxi століття: теорія та практика.Матеріали міжнародної науково-практичної конференції. Національний університет «одеська юридична академія». 2023. URL: https://dspace.onua.edu.ua/items/e0713052-8aa4-40b3-b182-e45bff5ebf36 (дата звернення: 15.12.2025).
7. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 15.12.2025).
8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 15.12.2025).
9. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.12.2025).
10. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 1 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 15.12.2025).

Петрущак Катерина Богданівна

курсантка факультету №2 Львівського державного університету внутрішніх справ

Рудий Тарас Володимирович

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ВИКОРИСТАННЯ ПАКЕТУ MATHCAD PRIME 9.0 ДЛЯ РОЗВ'ЯЗАННЯ СИСТЕМИ ЛІНІЙНИХ АЛГЕБРИЧНИХ РІВНЯНЬ

Розв'язання системи лінійних алгебричних рівнянь (СЛАР) є актуальною задачею багатьох галузей науки і техніки. Загальні методи їх розв'язання відомі та детально описані у літературних джерелах.

Метою нашого дослідження є підходи до розв'язання СЛАР у пакеті MathCad Prime 9.0. Чому саме MathCad Prime 9.0? Наш вибір зумовлений тим, що MathCad Prime 9.0 є однією з найновіших версій програмного забезпечення, яка містить сучасні інструменти для математичних обчислень і Львівський державний університет внутрішніх справ має 50 ліцензій, які функціонують під IP-адресою університету. Здобувачі мають необмежений доступ до ресурсу у лабораторіях кафедри інформаційних технологій. Ліцензійна чистота програмного забезпечення у процесі підготовки здобувачів освітнього ступеня «бакалавр» галузі знань 12 «Інформаційні технології» спеціальності 126 «Інформаційні системи і технології» має дуже велике значення.

До того ж у літературі нема опису роботи з пакетом навіть на рівні інтерфейсу, який радикально відрізняється від версій 14 та 15 пакетів MathCad.

Отже, нам довелося використати англомовний електронний варіант посібника MathCad Prime від PTC [1]. Автори використали термін, який зустрівся нам вперше. Це *Engineering Notebook* (Інженерний Блокнот). Як трактувати цей термін і який зміст розробники у нього вкладали

було незрозумілим. Проте, у процесі практичної роботи дещо з'ясувалося.

Отже, у нашому розумінні, *Engineering Notebook* – це робочий простір, який об'єднує ядра для числових та символьних обчислень, графічний та текстовий процесор, систему інтегрування з іншими програмними продуктами, підтримку OLE-технологій. Таке поєднання цих інструментальних засобів у межах єдиного функціоналу створює потужний програмний механізм для розв'язання інженерних задач та формування звітів і документації.

Поданий підхід підтверджує відданість розробників MathCad початковому принципу орієнтування на розв'язання завдань властиво *прикладної*, а не *теоретичної* математики, коли необхідно отримати результат без глибокого розуміння математичної суті задачі.

Тепер повернемося до нашої задачі. Методи розв'язання СЛАР дуже доступно і зрозуміло викладені у [2]. Проте, ми розв'яжемо специфічну задачу, коли СЛАР має декілька правих частин. Теоретично така задача нічим не відрізняється від класичної, з однією правою частиною. У нашому випадку права частина буде формуватися матрицею векторів вільних членів (векторів правих частин).

На основі загального формулювання формується матриця коефіцієнтів *A* та матриця векторів правих частин *B*. Це ми виконали у області *Math* вкладки *Matrices/Tables Engineering Notebook*. Є певна специфіка обчислення оберненої матриці. У вкладці *Matrices/Tables* нема стандартного оператора обчислення оберненої матриці, тому використовуємо оператор x^y розділу *Algebra* вкладки *Math*. Відразу записуємо оператор виведення і візуалізуємо матрицю A^{-1}.

Отримавши матрицю A^{-1} можемо обчислити матрицю векторів невідомих, як звиклого матричного виразу. По виведенні результату обчислення матричного виразу виконуємо оцінювання результату на рівні числа. Іншими словами, переходимо до початкового формулювання задачі і обчислюємо матричний вираз *A*X*. Отриманий результат співпадає зі значеннями елементів матриці векторів правих частин.

На рис. 1. Подано класичне формулювання задачі розв'язання СЛАР і запропоноване нами.

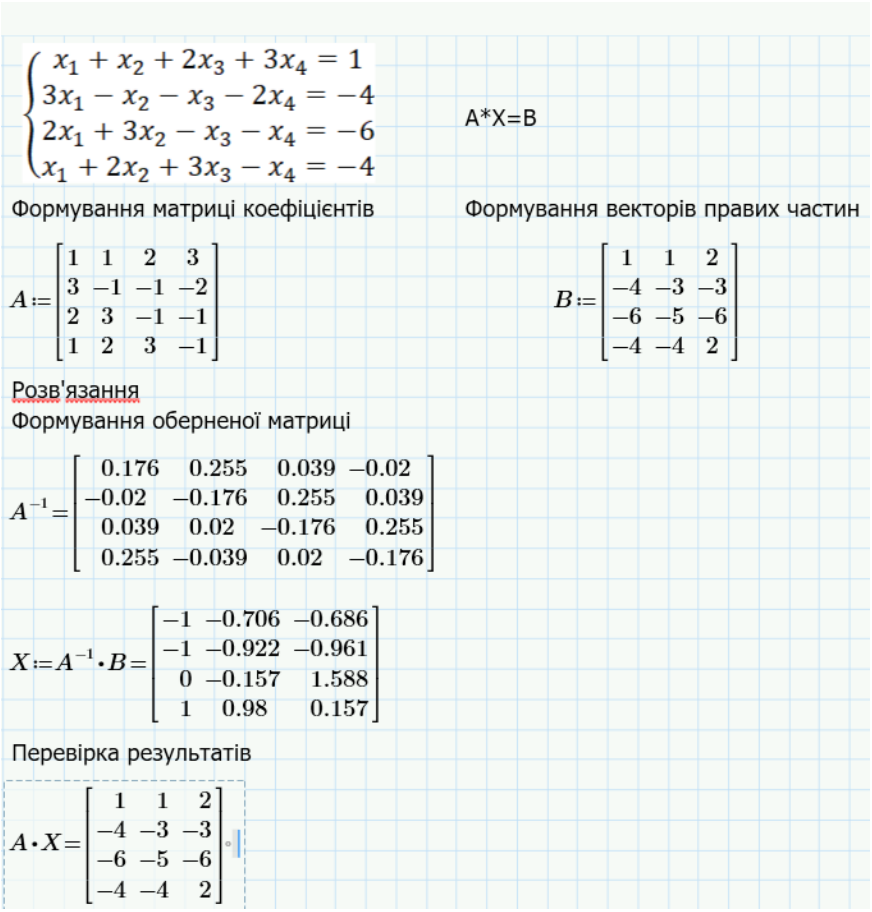

Рис. 1. Процес розв'язання задачі у MathCad-документі Engineering Notebook пакету MathCad Prime 9.0

Неможливо обійти увагою таку спеціальну структуру у *Engineering Notebook* пакету MathCad Prime 9.0 як *Solve Block*. Якщо ви поважно налаштовані використовувати MathCad Prime у інженерних розрахунках, тоді без *Solve Block* не обійдетеся.

Також MathCad Prime має вмонтовану функцію *lsolve*, яка призначена для розв'язання СЛАР у класичному формулюванні. Параметрами функції *lsolve* є матриця коефіцієнтів та вектор правих частин. Використання функції подано на рис. 3.

Solve Block активується у вкладці *Math*. Необхідно заповнити три розділи, це початкові наближення, обмеження та розв'язання. Процес розв'язання СЛАР з використанням *Solve Block* подано на рис. 2.

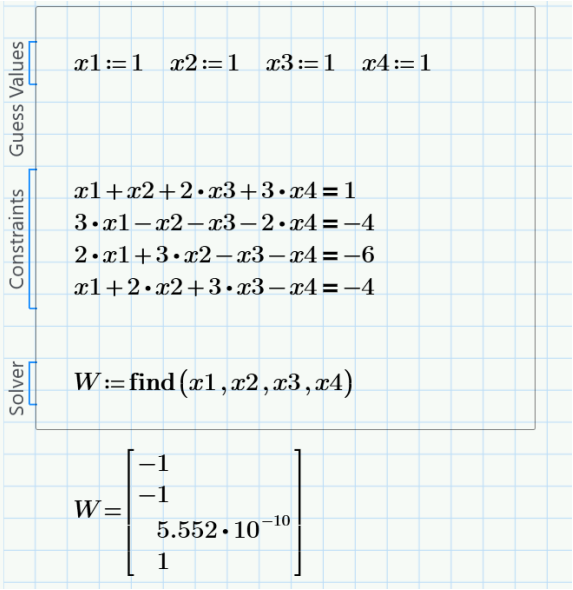

Рис. 2. Процес розв'язання СЛАР з використанням Solve Block

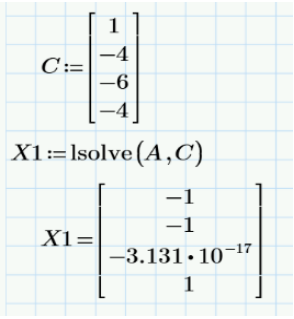

Рис. 3. Процес розв'язання СЛАР з використанням функції lsolve

Як висновок можемо стверджувати, що пакет MathCad не є безумовною альтернативою мовам програмування, а тільки оперативний інструмент для розв'язання інженернених задач, де результат отримується просто, без особливих витрат часу і глибокого розуміння математичного змісту. Результати розв'язання СЛАР запропонованими методами є однаковими.

Понад те, без глибокого розуміння реалізування класичних алгоритмів, алгоритмів і структур даних ми не могли б так легко опанувати роботу з пекетом MathCad.

Література

1. https://support.ptc.com/help/engineering_notebook/r11.0/en/index.html#page/PTC_Mathcad_Help/Tutorials/gs_tutorial/about_the_getting_started_tutorial.html#
2. Огірко О. І., Галайко Н. В. Вища математика. Частина 1: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2025. 370 с.

Побережник Максім Валентинович

студент Львівського державного університету безпеки життєдіяльності

Ткачук Ростислав Львович

професор кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, доктор технічних наук, професор

Ящук Валентина Ігорівна

доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат економічних наук, доцент

ІНФОРМАЦІЙНА ВІЙНА ЯК ІНСТРУМЕНТ ГІБРИДНОЇ АГРЕСІЇ: ВИКЛИКИ ТА МЕХАНІЗМИ ПРОТИДІЇ

На межі XX–XXI століть світ увійшов в інформаційну епоху, у якій інформація набула статусу стратегічного ресурсу та інструмента геополітичного впливу, інтегрованого в системи оборони й національної безпеки. У сучасних міжнародних відносинах інформаційна війна розглядається як ключовий елемент гібридних конфліктів, що поєднують військові, інформаційні, психологічні та кібернетичні операції, спрямовані на дестабілізацію суспільства та дискредитацію державних інституцій [1].

Стрімкий розвиток цифрових технологій і глобальна доступність Інтернету трансформували кіберпростір у критично важливу сферу протиборства. Кібератаки на об'єкти критичної інфраструктури, втручання у політичні процеси та масове поширення дезінформації стали системними інструментами впливу в міжнародних конфліктах [2]. Інформаційні та кібернетичні операції реалізуються комплексно, поєднуючи технічні атаки з інформаційно-психологічним впливом на суспільну свідомість [3].

Особливої актуальності ці загрози набули для України з 2014 року, коли інформаційно-кібернетичні впливи стали складовою стратегії держави-агресора. Аналітичні дослідження фіксують системний характер кампаній, спрямованих на підрив довіри до органів влади, поляризацію

суспільства та дестабілізацію внутрішньополітичної ситуації [4]. Практика України підтверджує загальносвітову тенденцію використання інформації та кібернетичних технологій як інструментів стратегічного впливу [5].

Сфера інформаційної та кібербезпеки в сучасних умовах характеризується високим рівнем загроз, що мають комплексний і системний характер та спрямовані як на технічні, так і на соціальні компоненти інформаційного простору. До основних проявів таких загроз належать кібератаки на об'єкти критичної інфраструктури, зокрема енергетичні, транспортні, фінансові та комунікаційні системи, кібершпигунство, спрямоване на незаконне отримання конфіденційної, службової або стратегічно важливої інформації, а також саботаж інформаційних ресурсів шляхом їх блокування, модифікації або знищення. Окрему небезпеку становлять інформаційно-психологічні впливи та маніпуляція суспільною думкою із використанням цифрових платформ і соціальних мереж, що можуть дестабілізувати суспільно-політичну ситуацію та підривати довіру до державних інституцій [6].

Метою дослідження є комплексний аналіз феномену інформаційної війни, сучасних викликів у сфері кібербезпеки та обґрунтування практично орієнтованих заходів протидії. В умовах гібридної війни Україна сформувала багаторівневу систему кіберзахисту, ключову роль у якій відіграє Національний координаційний центр кібербезпеки при РНБО України. Досвід ЄС та Ізраїлю підтверджує ефективність поєднання державної координації, інноваційних технологій і міжсекторальної взаємодії у забезпеченні кіберстійкості.

Методи протидії кіберзагрозам

Системний захист інформаційного простору передбачає комплексний підхід, що включає технічні, організаційні та соціально-психологічні заходи. Основними напрямами є:

1. Впровадження багатофакторної автентифікації та сучасних систем шифрування для забезпечення безпеки доступу до критичних інформаційних ресурсів.

2. Навчання працівників основам кібергігієни та цифрової обережності, включаючи протидію фішинговим атакам та соціальній інженерії.
3. Створення резервних копій та відновлювальних систем для критично важливих даних, що дозволяє мінімізувати наслідки кібератак.
4. Розвиток технологій моніторингу та виявлення аномалій у мережах, що дозволяє своєчасно реагувати на нові типи атак.
5. Активна інформаційна політика та медіаграмотність населення, яка спрямована на нейтралізацію фейкових новин та пропаганди, формування культури критичного сприйняття інформації.
6. Міжнародне співробітництво та обмін досвідом у сфері кібербезпеки для узгодження стандартів і протоколів реагування на інциденти [7-9].

Практичне впровадження зазначених заходів може здійснюватися як на державному, так і на корпоративному рівнях, а також у системі освіти та громадського сектору, що дозволяє підвищити кіберстійкість усіх компонентів інформаційного простору.

Інформаційна війна та кібербезпека є двома взаємопов'язаними складовими сучасного безпекового середовища. Перемогу у сучасних конфліктах визначає не лише військова міць, а й здатність держави та суспільства ефективно захищати інформаційний простір. Україна вже накопичила значний досвід протидії кіберзагрозам, але перед країною стоїть завдання подальшого розвитку:

– розробка систем раннього виявлення кіберзагроз на основі технологій штучного інтелекту;

– вдосконалення законодавчого регулювання кіберпростору та імплементація сучасних стандартів інформаційної безпеки;

– формування культури кібербезпеки серед громадян та державних службовців, що передбачає навчання та підвищення медіаграмотності;

– розширення міжнародного співробітництва для забезпечення обміну знаннями, координації протидії глобальним кіберзагрозам.

Застосування зазначених стратегій сприятиме зміцненню національної безпеки шляхом підвищення захищеності критичної інформаційної інфраструктури та державних інформаційних ресурсів. Формування ефективної системи кіберстійкості забезпечить здатність своєчасно запобігати кіберзагрозам, мінімізувати наслідки інцидентів і оперативно відновлювати функціонування інформаційних систем, що підвищить стабільність державних інституцій, довіру до цифрових технологій та стійкий розвиток країни в умовах зростання інформаційних викликів.

Література

1. Галіпчак В. М. Інформаційна війна як складова сучасних гібридних конфліктів / В. М. Галіпчак // Політологічні студії. – 2024. – Вип. 15. – С. 45–58. – Режим доступу: https://journals.pnu.if.ua/index.php/politology/article/view/50
2. Матвієнко С., Коноплич І. Кібербезпека та інформаційна протидія в умовах гібридних конфліктів / С. Матвієнко, І. Коноплич // Дослідження з питань безпеки. – 2023. – Вип. 12. – С. 23–39. – Режим доступу: https://dspace.pdau.edu.ua/items/ec77c0cf-b24b-4edb-8e56-22b58f19d835
3. Габрильчук О., Шевчук М., Литвиненко П. Кіберзагрози у сучасних гібридних конфліктах: методи виявлення та протидії / О. Габрильчук, М. Шевчук, П. Литвиненко // Науковий вісник Львівського національного університету імені Івана Франка. Серія «Безпека життєдіяльності». – 2025. – Вип. 7(1). – С. 112–130. – Режим доступу: https://science.lpnu.ua/uk/csn/vsi-vypusky/vypusk-7-nomer-1-2025/doslidzhennya-kiberatak-z-vykorystannyam-mashynnogo-navchannya
4. Левченко І., Охрімчук А. Інформаційна безпека України в умовах зовнішніх гібридних загроз / І. Левченко, А. Охрімчук // Журнал міжнародних студій. – 2022. – Вип. 9. – С. 77–92. – Режим доступу: https://jrnl.nau.edu.ua/index.php/ZI/article/view/17377/24697
5. Vasyshchev D., Denysenko M. Cybersecurity and Information Warfare in Hybrid Conflicts / D. Vasyshchev, M. Denysenko // Scientific Bulletin

of the National Academy of Management. – 2023. – Vol. 18, Issue 3. – P. 45–63. – Режим доступу: https://sts.nangu.edu.ua/article/view/288258
6. Мазур О. Інформаційні загрози та кібернетична безпека: науковий аналіз і практичні аспекти / О. Мазур // Журнал прикладних наук. – 2024. – Вип. 10. – С. 98–115. – Режим доступу: https://journal-app.uzhnu.edu.ua/article/view/317255
7. Ткачук Р., Ткаченко А. Кібербезпека: комплекс заходів щодо захисту критичної інфраструктури в умовах сучасних загроз // Цивільний захист в умовах війни : зб. тез доп. І Міжнар. наук.-практ. конф. (м. Львів, 17–18 квіт. 2025 р.). Львів : ЛДУ БЖД, 2025. С. 128–291.
8. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали ІІІ Міжнар. наук.-практ. конф. (м. Хмельницький, 21 листоп. 2024 р.). Хмельницький : НАДПСУ, 2024. С. 1136–1138.
9. Балацька В. С., Ткачук Р. Л., Маслова Н. О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України // Кібербезпека: освіта, наука, техніка : електрон. фах. наук. вид. 2025. № 2 (30). С. 316–332. DOI: 10.28925/2663-4023.2025.30.975.

Погар Максим Юрійович,

курсант ННІ №4 Харківського національного університету внутрішніх справ

Лучик Світлана Дмитрівна,

професор кафедри інформаційних систем та технологій ННІ №4 Харківського національного університету внутрішніх справ, доктор економічних наук, професор

МОДЕЛЮВАННЯ РИЗИКІВ ВИТОКУ ДАНИХ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасному цифровому середовищі більшість підприємств і державних установ використовують розподілені інформаційні системи, які об'єднують численні вузли, бази даних, користувацькі застосунки та хмарні сервіси. Така архітектура забезпечує високу швидкодію, масштабованість і доступність інформації, проте одночасно створює значні ризики витоку конфіденційних даних. Проблема ускладнюється тим, що контроль над інформаційними потоками у розподілених середовищах є фрагментованим, а обмін даними відбувається через різні канали з неоднаковим рівнем безпеки. Тому актуальним напрямом досліджень є моделювання ризиків витоку даних, яке дає змогу кількісно оцінювати ймовірність інцидентів і прогнозувати їх наслідки.

Під розподіленими інформаційними системами розуміють комплексні системи, що складаються з кількох взаємопов'язаних комп'ютерів та пристроїв (вузлів), які працюють разом над загальним завданням з обробки та зберігання інформації, розташованих у різних місцях, але логічно об'єднані мережею для забезпечення спільних інформаційних потреб користувачів, пропонуючи високу доступність, масштабованість та стійкість до відмов. Прикладами розподілених інформаційних систем є: Інтернет-магазини (Amazon, eBay): сервери, бази даних та системи замовлень рознесені по світу; хмарні сервіси (Google Drive, Dropbox): дані зберігаються на кластерах серверів; банківські системи: мережа банкоматів і відділень, що оновлюють спільну базу даних; системи бронювання (авіа, готелі): єдина база доступна агентам по всьому світу.

Такі системи є основою сучасної цифрової інфраструктури, забезпечуючи ефективне управління інформацією в масштабах підприємств та всього світу.

Моделювання ризиків передбачає формалізацію основних джерел загроз. До них належать:

– технічні чинники (вразливості програмного забезпечення, помилки конфігурації, відсутність шифрування під час передавання даних);
– організаційні (недостатній контроль доступу, людський фактор, неналежне управління правами користувачів);
– мережеві (небезпека під час маршрутизації, використання публічних каналів, відсутність сегментації).

Кожен з цих чинників формує власну складову загального ризику, що в сукупності визначає рівень небезпеки для системи [1].

Для опису архітектури розподіленої системи доцільно застосовувати графову модель, вершинами якої є такі компоненти як сервери, бази даних, користувацькі пристрої, шлюзи, а ребрами виступають канали передачі даних. Кожен елемент характеризується імовірністю інциденту та потенційними втратами від нього. Це дозволяє побудувати інтегральний показник ризику для всієї системи, який враховує як частоту подій, так їхній можливий вплив. На основі такого аналізу можна виділити «критичні вузли» інфраструктури, тобто ті, що становлять найбільшу загрозу в разі порушення безпеки [2].

У процесі дослідження ризиків доцільно використовувати імітаційні моделі. Зокрема, метод Монте-Карло дозволяє моделювати велику кількість випадкових сценаріїв витоку — від зламу облікового запису до втрати даних через помилку персоналу. Це дає змогу оцінити динаміку ризику у часі та спрогнозувати найуразливіші періоди чи ділянки системи. Додатково можна застосовувати мережі Байєса для встановлення залежностей між подіями. Наприклад, успішна фішинг-атака підвищує ймовірність компрометації облікових даних, що, своєю чергою, збільшує ризик несанкціонованого доступу до бази даних.

Практична реалізація моделі ризику може бути використана для формування карти ризиків у розподіленій інфраструктурі. Така карта допомагає визначити пріоритети у сфері кіберзахисту. Зокрема, де потрібне посилення контролю доступу, сегментація мережі чи додаткове шифрування каналів. Крім того, результати моделювання можуть стати основою для побудови систем моніторингу безпеки в реальному часі, які відстежують підозрілі дії та попереджають витоки ще на ранніх етапах.

Особливу увагу слід приділяти людському фактору, адже значна частина інцидентів спричинена саме помилками користувачів або недотриманням політик безпеки. Модель ризику повинна враховувати поведінкові параметри: рівень кіберграмотності персоналу, частоту проходження навчань, кількість попередніх інцидентів у підрозділі. Це дозволить підвищити точність прогнозів та ефективність заходів профілактики.

Таким чином, моделювання ризиків витоку даних у розподілених інформаційних системах є важливим інструментом забезпечення кіберстійкості організації. Побудована модель дозволяє не лише оцінити поточний рівень небезпеки, а й визначити шляхи її зниження, оптимізувати політику безпеки та підвищити довіру до цифрової інфраструктури.

Література

1. Матов О.Я., Василенко В.С. Модель загроз у розподілених мережах. Реєстрація, зберігання і оброб. даних. 2008. Т. 10, № 1. С. 91-102.
2. Лєнков С., Джулій В., Муляр І., Лєнков Є., Кольцов Р. (2025). Оцінки ефективності системи захисту конфіденційної інформації розподілених інформаційних систем. Кібербезпека: освіта, наука, техніка: електронне фахове наукове видання, 1(29), 628–644. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/916

Поляк Святослав Петрович
доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівсь.-кого державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ІНФОРМАЦІЙНО-АНАЛІТИЧНА РЕВОЛЮЦІЯ: НЕЙРОМЕРЕЖІ ПРОТИ АНАЛІТИКІВ

Існування суспільства в конкретному часовому хронометражу продукує такі інструменти, які б змогли забезпечити вирішення завдань, що постають саме на цьому етапі еволюції спільноти та правоохоронної діяльності як супутника правової цивілізації.

Нова суспільна реальність та фактично завершений четвертий рівень промислової революції (Industry 4.0), яка активно інтегрує сучасні інформаційні технології, штучний інтелект, автоматизацію та інтернет речей (IoT) у виробничі процеси й повсякденне життя, вимушено спонукають використовувати сучасні інформаційні технології та комп'ютерне інтелектуальне моделювання і у сфері протидії протиправним діянням, оскільки чимало таких діянь вчиняється за допомогою тих же технологій.

Тут хочеться навести короткий дискурс основних особливостей та складових Четвертої промислової революції, до яких ми ще будемо детально звертатися в ході нашого дослідження, зокрема таких як:

1. Цифровізація: Повсюдне впровадження цифрових технологій, які інтегрують фізичні та віртуальні світи.
2. Штучний інтелект (AI): Використання машинного навчання, обробки даних і нейронних мереж для автоматизації складних завдань.
3. Інтернет речей (IoT): Зв'язок між пристроями, які взаємодіють у реальному часі.
4. Великі дані (Big Data): Аналітика великих обсягів інформації для прийняття ефективних рішень.
5. Хмарні обчислення: Доступ до обчислювальних ресурсів через інтернет.

6. Кіберфізичні системи: Інтеграція фізичних об'єктів із програмним забезпеченням через мережі.
7. Робототехніка та автоматизація: Використання автономних систем у промисловості, логістиці, державному управлінні та інших сферах.

Отже, адміністрування правоохоронною системою за таких умов також повинно здійснюватися на основі своєчасної зміни парадигми.

Зміна парадигми означає засвоєння нової моделі мислення, яка починає використовуватися як основна [1, с. 59].

Що стосується зміни концептуальних підходів до інформаційно-аналітичного забезпечення правоохоронної діяльності в Україні, то спостерігається певна стагнація як у правовому регулювання, так і в практичних підходах до реалізації нової парадигми, що витікає з цифрової революції та розвитку нейромережі як нової реальності. Так, на даний час в Україні діє Концепція Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, схвалена розпорядженням Кабінету Міністрів України ще від 13 грудня 2007 р. № 754-р. [2].

Ця Концепція визначає основні напрями розвитку інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою зі злочинністю та охороною громадського порядку.

Однак, з огляду на стрімкий розвиток інформаційних технологій та зміну безпекової ситуації в країні, виникає потреба в оновленні та адаптації цієї Концепції до сучасних реалій.

Еволюція суспільства звело сучасні правоохоронні органи до масового використання Big Data, AI, GIS-технологій, соціальних мереж для аналізу та прогнозу загроз замість попередніх моделей інформаційно-аналітичного забезпечення правоохоронної діяльності (далі – ІАЗПД), де інформація в основному накопичувалася для статистики, і будучи опрацьованою аналітиками, використовувалася для визначення кримінологічних показників злочинності без активного використання їх для зменшення її рівня чи активного прогнозування. Таким чином, опанування зазначених інструментів активізувало прогнозну аналітику.

У посібнику «Кримінальна розвідка» виданому на основі досліджень Управління Організації Об'єднаних Націй з питань наркотиків і злочинності надано визначення поняття інформація, під якою розуміється сировина, що надходить з відкритих або закритих джерел: документи, звіти, свідчення, цифрові сліди тощо. Проте сама по собі вона не має практичної цінності для оперативних рішень, поки не буде оцінена, перевірена та інтерпретована. Відтак пояснюється різниця між сирими даними (information) та розвідувальними даними (intelligence). Інтелектуальний продукт (розвідка) – це результат обробки інформації з доданим аналітичним сенсом. Вона має бути перевіреною, актуальною, доречною та вчасно доведеною до користувача. Цей перетворений продукт лежить в основі будь-якого стратегічного або оперативного рішення в правоохоронній практиці. Все це породжує відповідну формулу: Інформація + оцінка = розвідка (анг. Information + Evaluation = Intelligence) [3, с. 9-10].

У науковій та прикладній літературі доведено, що ШІ-системи здатні автоматично обробляти великі масиви кримінальних даних, виявляти закономірності та підтримувати аналітичну роботу правоохоронців. Прикладом такої інтегрованої системи є Visual Analytics for Sense-making in Criminal Intelligence Analysis (VALCRI) – аналітична система, яка агрегує дані з різних джерел, автоматично здійснює пошук інформації та візуалізує її для аналітиків, що суттєво скорочує час на обробку даних та підвищує точність висновків, порівняно з традиційними методами. Це ілюструє потенціал ШІ-технологій для інформаційно-аналітичного забезпечення правоохоронної діяльності [4].

Дослідження вказують, що автоматизація з використанням ШІ може не лише підвищувати ефективність розпізнавання закономірностей і прогнозів злочинності, але й піднімає питання прозорості, етичності та відповідальності. Так, сучасні наукові праці з галузі штучного інтелекту для правоохоронних аналітичних систем обговорюють не лише потенціал автоматизації обробки даних і підтримки прийняття рішень, а й необхідність участі людини-аналітика в оцінці та верифікації результатів автоматизованих механізмів, що сприяє точності та етичності застосування технологій у правоохоронній діяльності [5].

Таким чином локальні AI менеджери та автоматизація за допомогою AI менеджерів в інформаційно-аналітичній роботі правоохоронної діяльності набувають нового значення та пріоритету, нівелюючи багато суб'єктивних факторів й корупційних ризиків. Наступний розвиток ІАЗПД та адаптація його сучасних світових концепцій до реалій національного законодавства гарантує ефективний і структурований поділ ресурсів апарату правового переслідування, що суттєво вплине на тенденції протиправної поведінки в Україні.

Література

1. Мурзановська, А. В. (2023). Парадигми: сутність, поняття та значення в методології кримінально-процесуальної науки. Наукові праці, 58 с.
2. Про схвалення Концепції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю: розпорядження Кабінету Міністрів України від 19 вересня 2007 р. № 754-р // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/754-2007-%D1%80. (дата звернення: 27.01.2025).
3. United Nations Office on Drugs and Crime. (2011). Criminal Intelligence: Manual for Analysts. Vienna: UNODC. URL:https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf
4. European Commission. (2018). Visual Analytics for Sense-making in Criminal Intelligence analysis (VALCRI) Final Report. CORDIS. Retrieved URL: https://cordis.europa.eu/project/id/608142/reporting
5. Nowack, V., Alrajeh, D., Muñoz, C. G., Thomas, K., Hobson, W., Hamilton-Giachritsis, C., … Woodhams, J. (2025). Towards user-centred design of AI-assisted decision-making in law enforcement. arXiv. Retrieved URL: https://arxiv.org/abs/2504.17393

Понзель Степан Сергійович

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Йосифович Данило Ігорович

професор кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, кандидат юридичних наук, професор

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ У ВИКРИТТІ НАРКОЛАБОРАТОРІЙ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Інформаційно-аналітичне забезпечення у діяльності оперативних підрозділів кримінальної поліції давно перестало бути другорядним інструментом і перетворилося на стрижневу передумову результативності у викритті нарколабораторій. Варто зазначити, що в сучасних умовах коли незаконний обіг наркотиків зміщується у сферу технологічної анонімності і коли виробництво синтетичних речовин дедалі частіше відбувається у закритих приміщеннях із використанням обладнання доступного кожному охочому саме інформація стає ключем до розуміння логістики функціонування злочинних груп їхніх комунікаційних каналів та таємних місць виготовлення психоактивних речовин. Успішне викриття нарколабораторій можливе лише тоді коли оперативні працівники мають у своєму розпорядженні повні достовірні та своєчасні відомості які дають змогу передбачити поведінку злочинців і мінімізувати ризики для особового складу і суспільства. Тому потрібно проаналізувати особливості інформаційно-аналітичного забезпечення у викритті нарколабораторій оперативними підрозділами кримінальної поліції.

Варто зазначити, що сучасні нарколабораторії відрізняються високим рівнем мобільності і фрагментованості. Злочинні групи використовують орендовані приміщення змінюють локації маскують обладнання під побутові прилади організовують роботу невеликими партіями щоб

уникати одномоментного накопичення речовин та реагентів. За таких умов класичні оперативні заходи не дають змоги в повній мірі забезпечити результативність тому зростає цінність усієї системи інформаційно-аналітичної підтримки. Вона охоплює збір різнорідних даних їх структурування зіставлення аналіз і подальшу трансформацію в аналітичні висновки які спрямовують діяльність оперативних підрозділів [1, с. 33].

В свою чергу, надзвичайно важливим джерелом відомостей стають відкриті дані та цифровий простір. Злочинці залишають сліди у вигляді транзакційних даних логістичних маршрутів придбання хімічних реагентів поштових відправлень замовлень обладнання та електронних комунікацій. Інформаційно-аналітичні підрозділи повинні вміти працювати з великими масивами інформації застосовувати методи глибинного аналізу використовувати алгоритми пошуку закономірностей та аналітику соціальних мереж. Саме цифрові інструменти дозволяють простежити маршрути доставки прекурсорів визначити коло осіб що перебувають у ризиковій групі та виявити неочевидні зв'язки між підозрюваними.

Крім того, як показує практика, важливою складовою діяльності оперативних підрозділів є інтеграція різних видів інформації у єдину систему оперативно-розшукового реагування. Дані від оперативних джерел матеріали негласних заходів результати спостереження сигнали від громадян аналітичні висновки експертів а також інформація з міжнародних джерел мають об'єднуватися у цілісну картину. Чим точніше сформована ця картина тим швидше можна встановити місце розташування нарколабораторії визначити масштаби її діяльності та запобігти поширенню синтетичних наркотиків у суспільстві [2, с. 99].

Успіх інформаційно-аналітичного забезпечення залежить також від кваліфікації аналітиків які повинні не просто збирати відомості а й інтерпретувати їх прогнозувати розвиток подій виявляти слабкі місця в діяльності злочинної групи та пропонувати оперативні рішення. Ефективний аналіз передбачає системність скрупульозність та здатність мислити наперед. Підрозділи кримінальної поліції мають працювати із застосуванням сучасного програмного забезпечення для аналізу зв'язків картування кримінальних подій і візуалізації даних що значно прискорює процес ухвалення управлінських рішень.

Викриття нарколабораторій потребує комплексного підходу який охоплює не лише оперативно-розшукові заходи а й постійне вдосконалення інформаційного забезпечення. Важливо налаштовувати співпрацю з митними органами прикордонною службою міжнародними правоохоронними структурами адміністраторами цифрових платформ логістичними операторами та приватним сектором. Така взаємодія забезпечує доступ до додаткових ресурсів і каналів отримання інформації що підвищує ефективність роботи оперативних підрозділів.

В свою чергу, не менш значущим є питання правового регулювання інформаційно-аналітичної діяльності. Вона має здійснюватися у межах закону з дотриманням прав і свобод громадян а кожне зібране відомство повинно мати чітке правове підґрунтя. Гармонізація технологічних можливостей і правових норм є умовою легітимності діяльності кримінальної поліції та збереження довіри громадськості.

В умовах розвитку ринку синтетичних наркотиків та розширення ролі цифрових середовищ інформаційно-аналітичне забезпечення стає основою успішної протидії наркозлочинності. Саме аналітика формує основу для ухвалення зважених оперативних рішень які дозволяють швидко реагувати на зміну тактики злочинців та перешкоджати створенню нових нарколабораторій [3, с. 174-175].

Таким чином, можемо зробити узагальнення, що інформаційно-аналітичне забезпечення у викритті нарколабораторій є не просто допоміжною складовою а фундаментальним інструментом успішної діяльності оперативних підрозділів кримінальної поліції. Воно забезпечує оперативність реагування точність дій і комплексність підходу до боротьби з організованими наркогрупами. Уміння збирати аналізувати та інтерпретувати інформацію надає правоохоронцям можливість не лише реагувати на вже існуючі загрози а й виявляти підготовчі етапи створення нарколабораторій тим самим запобігаючи шкоді суспільству. Сучасні реалії вимагають від кримінальної поліції постійної модернізації технологічних інструментів удосконалення аналітичних методик і зміцнення взаємодії з іншими структурами. Лише скоординована системна та науково обґрунтована інформаційно-аналітична діяльність здатна створити

надійний бар'єр для злочинців і забезпечити ефективну протидію незаконному виробництву наркотичних засобів.

Література

1. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів: Львів. держ. ун-т внутр. справ, 2021. 288 с
2. Ступник Я.В., Плиска В.В., Гецко В.В. Інформаційно-аналітичне забезпечення протидії наркозлочинності. Visegrad Journal on Human Rights. 2021. № 2. P. 96-103.
3. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: ЛьвДУВС, 2017. 244 с.

Проць Іванна Миколаївна,

доцент кафедри адміністративно-правових дисциплін Навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Росяк Софія Тарасівна

здобувач вищої освіти Навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ

ЛЮДИНОЦЕНТРИЧНИЙ ПІДХІД ЯК ОБОВ'ЯЗКОВА ЮРИДИЧНА ПЕРЕДУМОВА У ЗАСТОСУВАННІ СИСТЕМ ОЗБРОЄННЯ ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (далі – ШІ) дедалі активніше інтегрується у військові системи, що створює загрозу втрати людського контролю над рішеннями, які безпосередньо впливають на право на життя. Згідно ст. 22 IV Конвенції про закони і звичаї війни на суходолі та додатку до неї: Положення про закони і звичаї війни на суходолі: «Воюючі сторони не користуються необмеженим правом у виборі засобів завдання шкоди

супротивнику» [1]. Військові розробки, здатні автономно ідентифікувати цілі, приймати рішення про ураження та здійснювати запуск озброєння без участі людини, ставлять під сумнів відповідність таких систем основоположним принципам міжнародного гуманітарного права. Центральною вимогою сучасної доктрини є збереження людиноцентричного підходу, що передбачає обов'язкову участь людини у ключових рішеннях щодо застосування летальної сили. Юридична сутність цього підходу полягає у необхідності забезпечення людського контролю над зброєю, який би гарантував відповідність її дій нормам міжнародного гуманітарного права.

Стаття 36 Протоколу І встановлює обов'язок держави перевіряти нові види зброї на відповідність міжнародному праву: «При вивченні, розробці, придбанні чи прийнятті на озброєння нових видів зброї, засобів або методів ведення війни Висока Договірна Сторона повинна визначити, чи підпадає їх застосування, за деяких або за всіх обставин, під заборони, що містяться в цьому Протоколі або в яких-небудь інших нормах міжнародного права, застосовуваних до Високої Договірної Сторони» [2]. Автономні системи озброєння мають підвищений рівень ризику втрати контролю, тому їх аналіз повинен враховувати можливість системної помилки, кібератак, дефектів алгоритмів та помилкових параметрів навчання. Кутовий О.В., Бурма С.К. зазначили про проблематику впровадження автономних систем озброєння: «Їхнє застосування супроводжується істотними юридичними, етичними та технологічними ризиками – насамперед через часткову або повну втрату людського контролю над застосуванням сили, непрозорість алгоритмів прийняття рішень, проблеми атрибуції відповідальності, а також ризик невибіркових або непропорційних атак» [3, с. 192]. Застосування зброї можливе лише за умови, що її ефекти можуть бути оцінені і контрольовані людиною. Це є підставою для висновку, що автономні системи без людського контролю суперечать духу та букві МГП.

Норми Женевських конвенцій 1949 року та Додаткового протоколу І 1977 року закріплюють персональний характер військової відповідальності. Принцип розрізнення, закріплений у статтях 48 («Для забезпечення

поваги й захисту цивільного населення та цивільних об'єктів сторони, що перебувають у конфлікті, повинні завжди розрізняти цивільне населення й комбатантів, а також цивільні й воєнні об'єкти та відповідно спрямовувати свої дії тільки проти воєнних об'єктів»), 51 («Напади невибіркового характеру заборонено») і 52 («У разі сумніву в тому, чи не використовується об'єкт, який звичайно призначений для цивільних цілей, наприклад, місце відправлення культу, житловий будинок чи інші житлові будови або школа, для ефективної підтримки воєнних дій, передбачається, що такий об'єкт використовується в цивільних цілях») Протоколу І, зобов'язує комбатантів розмежовувати цивільних і військові об'єкти [2]. Автономні системи, що працюють на основі ШІ, не здатні забезпечити гарантоване розрізнення у складних бойових умовах, особливо під час міських боїв та змішаних конфліктів, де цивільні і комбатанти перебувають у тісній близькості. Це створює ризик невідворотних порушень МГП у разі делегування функції вибору цілі алгоритму, який не здатний оцінювати ситуацію у повному обсязі. Принцип пропорційності передбачає оцінку співвідношення очікуваної військової переваги та можливих втрат серед цивільного населення. Автономна система не здатна оцінювати гуманітарні наслідки у ширшому контексті, оскільки її рішення обмежуються обробкою наявних даних без можливості моральної оцінки ризиків. Тому передання алгоритму права на запуск зброї означає порушення вимоги пропорційності, оскільки відсутня гарантія, що система врахує всі релевантні фактори.

У межах ООН упродовж останнього десятиліття ведуться дискусії щодо регулювання автономних систем озброєння, де ключовою концепцією є meaningful human control. Ця концепція передбачає реальну, а не формальну участь людини у ланцюгу прийняття рішень про застосування летальної сили, включно з аналізом даних, схваленням атаки та можливістю її припинення [4]. У висновках Групи урядових експертів щодо смертельно небезпечних автономних систем 2021–2023 років наголошується, що жодна система не може ухвалювати рішення про ураження без належного людського контролю [5]. Ряд держав виступають проти обмежень, зокрема США і Росія, що підтверджується новинами про відсутність підтримки глобальної заборони автономної

зброї. Це створює ризик глобальних перегонів автономного озброєння, у межах яких питання гуманітарної відповідальності відходить на другий план.

З точки зору теорії права збройних конфліктів застосування автономної летальної зброї без людського контролю суперечить природі міжнародного гуманітарного права, яке виходить із презумпції раціональності та моральної оцінки дій людиною. У теорії підкреслюється, що МГП не лише регулює засоби та методи війни, а й встановлює етичні межі насильства. Автономний алгоритм не здатний до морального судження, а тому він не може бути суб'єктом виконання гуманітарних обов'язків. Людина має унікальну властивість оцінювати поведінку противника, символічні дії цивільних осіб, зміну поведінки в режимі реального часу і гуманітарний контекст ситуації. Жоден алгоритм не може відтворити цей комплекс оцінок у повному обсязі.

Загроза втрати людського контролю набуває особливої актуальності для України, оскільки РФ активно розробляє та застосовує системи з елементами автономності у безпілотниках і керуванні атакувальними платформами. Це створює реальний ризик того, що противник буде використовувати алгоритми для ухвалення рішень про атаки у спосіб, що суперечить МГП. У таких умовах Україна має уникати практики, що може поставити під сумнів її відповідність міжнародному праву, та дотримуватися принципу людського контролю незалежно від поведінки противника. Україна повинна формувати власні стандарти відповідності міжнародному гуманітарному праву, включаючи створення процедури проведення статті 36, визначення обов'язкового рівня участі оператора, затвердження технічних вимог до систем з елементами штучного інтелекту та запровадження механізмів юридичного та парламентського нагляду за їх використанням.

Література

1. IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі від 18.10.1907. URL: https://zakon.rada.gov.ua/laws/show/995_222#Text

2. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text
3. Кутовий О.В., Бурма С.К. Автономні системи озброєнь і штучний інтелект як виклик міжнародному гуманітарному праву та правам людини. Науковий вісник Ужгородського національного університету. Серія: Право. Том 5. № 90. 2025. С. 185-194.
4. Roff, Heather, Moyes, Richard. «Meaningful Human Control, Artificial Intelligence and Autonomous Weapons Systems.» Briefing Paper for Delegates for the CCW GGE Meeting on LAWS (April, 2016).
5. United Nations Office for Disarmament Affairs. Convention on Certain Conventional Weapons: Group of Governmental Experts on Lethal Autonomous Weapons Systems, 2025. URL: https://meetings.unoda.org/ccw/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2025

Рижков Едуард Володимирович

професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

СТАН ТА ПЕРСПЕКТИВИ КОМПЛЕКСНОГО ВИКОРИСТАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ (ФРЕЙМВОРКІВ) ТА МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСІ OSINT ПРАВООХОРОННИХ ОРГАНІВ

В умовах стрімкої цифровізації суспільства та безпрецедентних викликів, пов'язаних із військовою агресією проти України, традиційні методи оперативно-розшукової та слідчої діяльності потребують кардинальної модернізації. Злочинність активно використовує новітні технології, залишаючи глибокий «цифровий слід» практично на кожному кроці.

У відповідь на це, розвідка на основі відкритих джерел (OSINT — Open Source Intelligence) набуває критичного значення як систематизована діяльність зі збору, аналізу та інтерпретації публічно доступної інформації.

Особлива актуальність OSINT зумовлена необхідністю розслідування значної кількості воєнних злочинів в умовах, коли фізичний доступ до місць злочину чи доказів часто відсутній. Розслідування такого масиву специфічних правопорушень створює надмірне навантаження на діючі органи досудового розслідування та оперативні підрозділи правоохоронних органів.

Вирішення цієї проблеми можливе через комплексне використання штучного інтелекту (ШІ), що відповідно до Концепції розвитку ШІ в Україні є організованою сукупністю інформаційних технологій, яка дозволяє виконувати складні комплексні завдання шляхом використання алгоритмів обробки інформації, створення власних баз знань та моделей прийняття рішень [1]. ШІ виступає як революційний інструмент, здатний обробляти великі обсяги даних, аналізувати складні інформаційні структури та знаходити приховані зв'язки, що значно підвищує ефективність розслідувань [2, с. 14].

Сучасний стан та функціональний потенціал автоматизованих OSINT-фреймворків свідчить про їх ефективність як інструментів при здійсненні ОРД. Традиційні методи OSINT мають суттєві обмеження, пов'язані зі значним обсягом інформації, її динамічністю та складністю ручної верифікації [3, с. 358].

Це зумовлює необхідність переходу до автоматизації, яка оптимізує використання ресурсів та підвищує точність [4, с. 240].

Разом з тим автоматизовані OSINT-фреймворки, такі як SpiderFoot, належать до класу комплексних рішень, які забезпечують автоматизований збір та первинний аналіз даних. SpiderFoot — це інструмент з відкритим вихідним кодом (Open Source), написаний мовою Python, який забезпечує автоматизацію OSINT-розвідки.

Функціональність SpiderFoot базується на його модульній архітектурі (понад 200 модулів), які взаємодіють між собою за моделлю «Publisher/Subscriber». Це дозволяє модулям «підживлювати» один одного, забезпечуючи максимальну екстракцію та кореляцію даних.

На прикладі SpiderFoot більшість фреймворків включають в себе такі ключові можливості:

1. Збір ідентифікаторів особистості (екстракція електронних адрес, номерів телефонів, імен користувачів (Username Enumeration)).
2. Аналіз мережевих слідів (сканування IP-адрес, доменних імен, DNS-запитів, гео-локація IP та перевірка на вразливості).
3. Проведення фінансової розвідка (екстракція адрес Bitcoin та Ethereum для відстеження кримінальних фінансових потоків).
4. Моніторинг Dark Web (інтеграція з TOR дозволяє анонімно та безпечно проводити пошук у Dark Web).
5. Візуалізація (система генерує інтерактивний граф (Graph View), що дозволяє миттєво побачити структуру злочинної групи або інфраструктуру шахрайського ресурсу, перетворюючи розрізнені дані у зв'язки).

Найбільший інтерес становить прикладне застосування автоматизованих систем у правоохоронній діяльності. В цьому контексті автоматизовані фреймворки критично важливі для вирішення складних оперативних завдань. Вони здатні реалізовувати наступні функції. Здійснювати деанонімізацію. Наприклад, перевірка нікнейму «DarkBaron99» через модуль sfp_accounts може призвести до знаходження старих e-mail адрес, які, у свою чергу, відкривають шлях до реального ПІБ та номера телефону через бази даних витоків. Проводити аналіз інфраструктури розроблювальних осіб. Використання реверсивного пошуку за IP-адресою (Reverse IP Lookup) дозволяє виявити всі інші доменні імена, що хостяться на тому ж сервері, об'єднуючи, наприклад, фішингові сайти в одне провадження. Виявляти приховані зв’язки між учасниками кримінальних схем, ідентифікувати постраждалих та прогнозувати поведінку зловмисників.

З позиції пошуку максимальної ефективності використання сучасних ІТ-інструментів важливою є потенційна інтеграція штучного інтелекту (ШІ) та OSINT-аналітики.

Інтеграція ШІ в OSINT-системи суттєво скорочує час на первинне збирання інформації та підвищує її релевантність, забезпечуючи стратегічну перевагу у розслідуваннях та розкритті злочинів. Так ШІ здатний ефективно фільтрувати великі обсяги інформації (Big Data), виявляти зв'язки за непрямими ознаками та формувати аналітичні досьє. Автоматизовані системи, як SpiderFoot, у свою чергу дозволяють експортувати зібрані дані в графові формати, зокрема GEXF (Graph Exchange XML Format), що є ідеальною технічною передумовою для подальшого застосування ШІ-моделей для графового аналізу та виявлення прихованих мережевих зв'язків [5].

Для максимальної ефективності OSINT-розслідувань, на нашу думку, перспективним є інтеграція наступних ключових категорій моделей ШІ:

Обробка природної мови (Natural Language Processing, NLP). NLP є критичною для роботи з величезними обсягами неструктурованих текстових даних (соціальні медіа, форуми, чат-логи). Застосування NLP дозволяє: класифікувати контент та автоматично ідентифікувати мову ворожнечі, погрози, або шахрайські схеми; виявляти наміри, аналізувати свідчення, коментарі та дописи для виявлення таких намірів, емоційної тональності та джерел фейкової інформації; автоматизовано створювати звіти, формувати стислі аналітичні досьє з мільйонів повідомлень.

Комп'ютерний зір та біометрія (Computer Vision, CV). CV технології використовуються для аналізу візуальних даних, що критично важливо для фіксації воєнних злочинів. В рамках цієїтехнології проводиться: ідентифікація та розпізнавання обєктів, покращення та геолокація зображень.

Генеративний ШІ (Generative AI) (наприклад, Large Language Models, LLMs) може бути використаний для прискорення адміністративних завдань, як-от написання звітів та узагальнення інформації, реалізації управлінських функцій та прийняття рішень.

На ряду із перевагами впровадження автоматизованих OSINT-фреймворків та ШІ стикається зі значними технічними та правовими викликами.

Так, аксиоматичним є те, що ефективність ШІ залежить від якості, повноти та неупередженості даних. При цьому складність та непрозорість алгоритмів ШІ, особливо глибокого навчання, ускладнює пояснення рішень, що є критичним для забезпечення підзвітності та допустимості доказів у суді. Саме з цих позицій виникає необхідність розробки «свого поліцейського ШІ». Але головний на сьогодні, на нашу думку, стримуючий фактор для повноцінного використання високотехнологічних OSINT/ШІ методів в Україні — це правова прогалина. Зібрана в процесі ОРД з відкритих джерел інформація має трансформуватися у доказ, якому суд може довіряти. Відсутність прозорості методології, використаної автоматизованим фреймворком для кореляції даних, може стати підставою для відхилення результатів OSINT як ненадійних. До того ж сама технологія OSINT в Україні станом на кінець 2025 року залишається нормативно не врегульованою.

Для забезпечення принципу правової визначеності ми підтримуємо відповідні зміни до ст. 264 КПК України, а саме — легалізувати здобуття інформації з електронних систем з використанням OSINT, що забезпечить правову основу для автоматизованого збору цифрових слідів (IP, email, криптоадреси) та ст. 273 КПК України — унормувати можливість створення віртуальних засобів (особи) для зняття інформації з електронних систем, що легалізує діяльність легендованих акаунтів, необхідних для ефективного Username OSINT та моніторингу Dark Web. Також через ст. 8 Закону України «Про оперативно-розшукову діяльність» доречно унормувати практику використання OSINT для одержання даних, які мають значення для оперативно-розшукової діяльності [6].

Для забезпечення допустимості доказів, особливо у контексті міжнародного правосуддя, необхідно дотримуватися міжнародних стандартів, таких як Протокол Берклі (Berkeley Protocol on Digital Open Source Investigations) [7].

Таким чином, синергія OSINT + ШІ є перспективною та безальтернативною. Комплексне поєднання автоматизованих систем (наприклад, SpiderFoot як інструменту збору та структуризації) та аналітичних моделей ШІ (NLP, комп'ютерний зір, графовий аналіз) дозволяє якісно змінити можливості правоохоронних органів щодо обробки великих обсягів інформації, автоматизації рутинних завдань та виявлення прихованих зв'язків, особливо при розслідуванні воєнних злочинів та кіберзлочинів.

Негайне (з урахуванням воєнного стану) прийняття законодавчих змін, особливо у КПК України, є критичним для забезпечення допустимості електронних доказів, здобутих за допомогою автоматизованих систем, та легалізації віртуальних оперативних дій.

Стратегічний розвиток також полягає у розробці вітчизняних моделей ШІ виключно для потреб правоохоронних органів та формалізації методики «OSINT+», яка інтегрує дані з відкритих джерел із інформацією з відомчих баз даних обмеженого доступу (наприклад, ІКС Інформаційний портал НПУ) для підвищення верифікації та операційної ефективності [8, с. 193].

Необхідно створити централізовану інфраструктуру (на базі рішень, подібних до SpiderFoot HX, що пропонує хмарне управління та багатокористувацьку співпрацю) та забезпечити масове підвищення кваліфікації кадрів (AI Literacy) у сфері OSINT/AI, включаючи глибоке розуміння процесуальних вимог до цифрових доказів.

Інтеграція ШІ в OSINT, яка з часом буде підкріплена належним правовим регулюванням, є, на наше переконання, невід'ємною частиною цифрової трансформації криміналістики, оперативно-розшукової діяльності та інформаційних технологій, що забезпечить українській правоохоронній системі стратегічну перевагу в боротьбі зі злочинністю.

Література

1. Концепція розвитку штучного інтелекту в Україні : схвалена розпорядженням Кабінету Міністрів України від 2 гру дня 2020 р. № 1556 - р. URL : https://zakon.rada.gov.ua/laws/show/155 6-2020-%D1%80#n8.

2. Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. Теорія та практика судової експертизи і криміналістики. Вип. 4 (29). 2023. С.12-46.
3. Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки і обороноздатності України. Юридичний науковий електронний журнал. № 6. 2024. С. 356 – 361.
4. Шевчук В. Використання технологій штучного інтелекту в OSINT як напрям підвищення ефективності розслідування воєнних злочинів. URL: https://dspace.nlu.edu.ua/bitstream/123456789/20611/1/Shevchuk_239-243.pdf
5. SpiderFoot automates OSINT for threat intelligence and mapping your attack surface. – GitHub. URL: https://github.com/smicallef/spiderfoot
6. Кудінов С.С., Шехавцов Р.М. Правове регулювання використання OSINT та його результатів під час встановлення обставин кримінальних правопорушень. URL: http://journals.lvduvs.lviv.ua/index.php/law/article/view/1013
7. Протокол Берклі з ведення розслідувань з використанням відкритих цифпрвих даних. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf
8. Рижков Е.В. Методика «OSINT+»: синергія відкритих та відомчих інформаційних ресурсів у діяльності оперативних підрозділів Національної поліції України / Е.В. Рижков / Роль OSINT-досліджень у підвищенні рівня набіональної безпеки України : матер. кр. столу (м. Львів, 07 травня 2025 р.). / упорядник: І. О. Ревак. Львів: Львівськ. держ. ун-т внутр. справ, 2025. – С. 192-199

Романко Уляна Романівна

здобувач вищої освіти освітнього ступеня «бакалавр» спеціальності 126 Інформаційні системи та технології Львівського державного університету внутрішніх справ

Огірко Ольга Ігорівна

професор кафедри інформаційних технологій Львівського державного університету внутрішніх справ кандидат технічних наук, доцент

ІНСТРУМЕНТАРІЙ ТА МЕТОДОЛОГІЯ OSINT-АНАЛІЗУ В ЦИФРОВОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Відкрита розвідка (OSINT) посідає важливе місце у системі інформаційно-аналітичного забезпечення діяльності органів сектору безпеки і оборони в умовах цифровізації та інформаційної надмірності. Сучасне інформаційне середовище потребує застосування спеціалізованих пошукових інструментів, аналітичних методів і міждисциплінарних підходів до обробки відкритих даних. У цьому контексті актуальним є дослідження інструментарію та методологічних засад OSINT-аналізу з метою підвищення ефективності отримання та інтерпретації інформації.

Пошукові системи загального призначення (Google, Bing, DuckDuckGo, Baidu) є базовим інструментом OSINT-аналізу, ефективність якого забезпечується використанням спеціалізованих операторів пошуку (dorks), зокрема site:, filetype:, intitle:, intext:, inurl: та логічних операторів, що підвищують точність результатів [1].

Гранулярність пошукових запитів забезпечується через комбінування базових операторів з параметричними модифікаторами – daterange: (для обмеження хронологічних рамок), loc: (для географічної локалізації), related: (для виявлення семантично пов'язаних ресурсів), та wildcard-символами (для пошуку варіацій ключових слів). Особливо цінним підходом є конструювання складних пошукових запитів, які комбінують декілька операторів для виявлення інформації, яка зазвичай залишається прихованою від стандартних пошукових алгоритмів [2].

Алгоритмічна специфіка різних пошукових систем створює ситуацію інформаційної асиметрії, коли використання одного пошукового енджину не забезпечує повного охоплення релевантної інформації, що обумовлює необхідність диверсифікації пошукових джерел. Глибинна взаємодія з інтерфейсами пошукових систем через спеціалізовані запити та фільтри дозволяє долати обмеження стандартних пошукових алгоритмів та отримувати доступ до інформаційних пластів, які зазвичай залишаються невидимими для звичайних користувачів [3].

У табл. 1 подано узагальнену класифікацію основних джерел та інструментів OSINT-аналізу з урахуванням їх функціонального призначення та аналітичних можливостей. Представлена систематизація демонструє міждисциплінарний характер OSINT, що поєднує пошукові, соціально-мережеві, технічні та академічні джерела інформації. Комплексне використання зазначених інструментів дозволяє підвищити повноту, достовірність і аналітичну цінність результатів розслідувань.

Таблиця 1

Класифікація основних джерел та інструментів OSINT-аналізу

Категорія джерел	**Інструменти / сервіси**	**Аналітичні можливості**
Пошукові системи загального призначення	Google, Bing, DuckDuckGo	Пошук вебконтенту, застосування операторів (dorks), виявлення прихованої інформації
Академічні пошукові системи	Google Scholar, Semantic Scholar, ResearchGate	Доступ до наукових публікацій, оцінка авторитетності джерел, бібліометричний аналіз
Архівні вебсервіси	Wayback Machine, archive.today	Ретроспективний аналіз змін вебконтенту, відновлення видаленої інформації

Соціальні мережі та месенджери	Telegram, Instagram	Аналіз соціальних зв'язків, контенту, метаданих, темпоральних патернів активності
Технічні бази даних	WHOIS, RIPE NCC, BGP	Атрибуція доменів і IP-адрес, аналіз мережевої інфраструктури
Спеціалізовані OSINT-платформи	Shodan, Censys, ZoomEye	Виявлення підключених пристроїв, аналіз вразливостей, технічна розвідка
Інструменти аналізу витоків	VirusTotal, HaveIBeenPwned	Перевірка компрометації доменів, облікових записів та цифрових об'єктів

Пошукові системи наукових публікацій – Google Scholar, Semantic Scholar, Microsoft Academic, ResearchGate – надають доступ до масивів фахової літератури, дослідницьких звітів, дисертацій та конференційних матеріалів, що містять високоякісну верифіковану інформацію. Бібліометричні показники наукових публікацій – індекси цитування, імпакт-фактори журналів, h-індекси авторів – можуть використовуватися як додаткові критерії оцінки авторитетності та впливовості джерел. Спеціалізовані академічні пошукові системи дозволяють здійснювати пошук за авторами, установами, ключовими словами, роками публікації, що створює можливості для виявлення експертів у певних галузях та відстеження розвитку наукових напрямів [4].

Архівні сервіси – Internet Archive (Wayback Machine), archive.today, Archive-It – надають унікальну можливість ретроспективного аналізу вебконтенту, фіксуючи історичні стани вебсторінок, що особливо цінно при розслідуванні видаленої або модифікованої інформації[5].

Особливе місце у структурі OSINT-джерел займають спеціалізовані технічні бази даних – WHOIS (інформація про реєстрацію доменів), RIPE NCC (розподіл IP-адрес в Європі), BGP-дані (маршрутизація в інтернеті), які дозволяють встановлювати технічну атрибуцію цифрових об'єктів[6].

Соціальні медіа трансформувалися у безпрецедентно масштабне джерело структурованих та неструктурованих даних для OSINT-розслідувань, формуючи багатовимірний цифровий портрет індивідів, організацій та соціальних груп. Методологія аналізу соціальних мереж у контексті OSINT диференціюється залежно від специфіки кожної платформи, проте ґрунтується на спільних принципах вивчення цифрових артефактів, інтеракцій, темпоральних патернів активності та мережевих взаємозв'язків [7].

Теоретико-методологічним підґрунтям для аналізу соціальних мереж у OSINT виступає синтез соціологічних концепцій мережевого аналізу, теорії графів, інформаційно-комунікаційних моделей та цифрової антропології. Діджиталізація соціальних взаємодій призвела до формування феномену «цифрового двійника» – віртуальної проекції особи або організації в інформаційному просторі, яка акумулює цифрові сліди активності та формує комплексний інформаційний портрет [8].

Telegram цінне джерело для OSINT завдяки публічним каналам, групам та функції «Люди поблизу», яка за певних умов дозволяє ідентифікувати користувачів за геолокацією. Аналітичний потенціал Telegram посилюється через значну кількість політичних, економічних, військових інсайдерських каналів, які часто стають первинними джерелами ексклюзивної інформації [9].

Instagram фокусується на візуальному контенті, який містить багатий набір метаданих – від геотегів, часових міток до прихованих EXIF-даних фотографій (якщо вони не були автоматично видалені при завантаженні). Аналіз хештегів, згадок, коментарів та локацій в Instagram дозволяє встановлювати соціальні зв'язки, реконструювати хронологію переміщень та виявляти сфери інтересів об'єктів розслідування [10].

Особливу цінність для OSINT-розслідувань становить аналіз соціального графа – вивчення структури зв'язків між акаунтами для виявлення прихованих спільнот, встановлення ключових вузлів впливу та ідентифікації кластерів взаємодії. Соціально-мережевий аналіз дозволяє виявляти координовані мережі ботів, тролів та інших неавтентичних

акаунтів через аномальні патерни взаємодії, синхронізацію активності та спільні лінгвістичні характеристики [11].

Фундаментальним джерелом геолокаційних даних у цифровому середовищі виступають EXIF-метадані фотографій, які в нередагованому стані містять GPS-координати місця зйомки, часову мітку, інформацію про пристрій та інші технічні параметри. Специфікація EXIF (Exchangeable Image File Format) передбачає включення широкого спектру метаданих – від базової інформації про камеру (виробник, модель) до детальних технічних параметрів зйомки (фокусна відстань, витримка, діафрагма, ISO) та геопросторових даних (координати, висота, напрямок) [12].

Аналіз візуального контенту навіть за відсутності EXIF-даних дає змогу встановлювати геолокацію об'єктів шляхом ідентифікації архітектурних, ландшафтних та інших геопросторових маркерів із використанням порівняльного аналізу картографічних і супутникових даних [13].

Атрибуція IoT-пристроїв через дослідження їхньої мережевої активності та унікальних ідентифікаторів є перспективним напрямом OSINT, що реалізується за допомогою спеціалізованих пошукових систем Shodan, Censys і ZoomEye та дозволяє виявляти вразливості й потенційні вектори кібератак [14].OSINT-аналіз ґрунтується на комплексному використанні пошукових систем, наукових баз даних, соціальних мереж, архівних сервісів і технічних реєстрів відкритої інформації. Інтеграція методів пошуку, соціально-мережевого аналізу, геолокації та технічної атрибуції дозволяє формувати цілісний інформаційний портрет об'єктів дослідження. Застосування сучасних OSINT-підходів підвищує якість аналітичних продуктів та сприяє прийняттю обґрунтованих управлінських рішень у сфері безпеки.

Література

1. Constitution of Ukraine - Chapter II. Rights, Freedoms and Obligations of A Man And A Citizen. URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-ii

2. Користін О.Є., Денисенко Б.А. Зміст та інтерпретація терміна «intelligence» в контексті моделі Intelligence-led policing (ILP). Південноукраїнський правничий часопис. № 1. 2023. С. 72–79. DOI https://doi.org/10.32850/sulj.2023.1.13.
3. Bazzell M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. [S. l.]: Independently published, 2019.
4. Criminal Codex Of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
5. How To Use Osint For The Benefit Of Ukraine. URL: https://itarena.ua/how-to-use-osint-for-the-benefit-of-ukraine/
6. The Rise of OSINT: Few Rules, Many Opportunities. URL: https://www.afcea.org/signal-media/intelligence/rise-osint-few-rules-many-opportunities
7. Ісмайлов К., Пєфтієв Д. Розділ 16. Цифрові технології та аналітичні засоби аналізу воєнних злочинів в Україні. 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: «ВАЙТ», 2024. 504 с. С. 253–267.
8. Dincelli E., Van Slyke C., Yayla A. Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. Communications of the Association for Information Systems. 2023. Vol. 53, № 1. P. 1052–1071. DOI: 10.17705/1cais.05345.
9. Tools information struggle: OSINT, IPSO and opposition misinformation. URL: https://infolight.in.ua/wp-content/uploads/2023/02/brochure-2.pdf
10. What is OSINT (Open Source Intelligence)? URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/
11. Sidorenko V. V. The Schuchart-Deming Cycle (Pdca) for the Organization of Continuing Professional Development of Specialists. VI International Scientific and Practical Conference «CONTINUOUS

EDUCATION OF THE NEW CENTURY: ACHIEVEMENTS AND PROSPECTS». 2020.
12. Varzhanskyi I. Reflexive Control as a Risk Factor for Using OSINT: Insights from the Russia–Ukraine Conflict. International Journal of Intelligence and CounterIntelligence. 2023. P. 1–31. DOI: 10.1080/08850607.2023.2228489.
13. Facebook was fined five billion dollars in the US. URL: http://surl.li/rqqjp
14. OSINT, digital footprint and how to reduce it? URL: https://euprostir.org.ua/practices/133410

Романко Уляна Романівна

курсант факультету №2 (з підготовки фахівців для підрозділів превентивної діяльності та правоохоронних інформаційних систем) Львівського державного університету внутрішніх справ

Мовчан Анатолій Васильович

професор кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ ТА ДНК-ЕКСПЕРТИЗИ В СИСТЕМІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ПРИ РОЗШУКУ БЕЗВІСТИ ЗНИКЛИХ ОСІБ

Результативність роботи правоохоронних органів у сфері боротьби зі злочинністю значною мірою визначається рівнем якості, своєчасності та повноти інформаційно-аналітичного забезпечення, яке є необхідною умовою для прийняття обґрунтованих управлінських рішень і ефективної реалізації покладених на них завдань.

Одним із різновидів правової інформації, що використовується в ОРД, є оперативно-розшукова інформація. Одне з перших і упродовж

тривалого часу домінуючих у теорії ОРД визначень поняття оперативно-розшукової інформації було запропоновано Д. Гребельським, який сформулював його як сукупність даних про осіб, причетних до підготовки і вчинення злочинів, факти злочинних виявів, стан оперативно-розшукових сил і засобів, а також про умови, в яких відбувається діяльність ОВС щодо боротьби зі злочинністю [1].

Відомо, що певна частина громадян, які зникли за невідомих обставин, стає жертвами злочинів у результаті вчинення стосовно них кримінальних правопорушень, зокрема вбивства, викрадення, незаконного позбавлення волі. Не менш важливим є розшук таких осіб в аспекті вирішення звернень громадян щодо встановлення місця знаходження рідних чи близьких людей, з котрими за різних причин утрачені родинні зв'язки; відновлення соціального статусу, цивільних та інших гарантованих державою прав осіб, які за віком або через травму чи захворювання втратили пам'ять, дезорієнтовані тощо [2].

Методологічну основу розшукової діяльності створює ідентифікація особи. На досудовому слідстві також найчастіше використовується метод криміналістичної ідентифікації (ототожнення) живих осіб і трупів. Серед розмаїття його форм виділяють ототожнення за слідами пальців рук, ніг, ДНК-зразками, зовнішністю [2].

Останнім часом значного поширення в діяльності правоохоронних органів набули інформаційно-пошукові системи біометричної ідентифікації особистості по зображенню обличчя за оперативними даними від камер, розміщених у громадських місцях, за словесним описом, або портретом, складеним за допомогою фоторобота [2].

Сучасні системи криміналістичного обліку, наприклад, такі як автоматизована дактилоскопічна інформаційна система (зокрема, АДІС «Папілон») та Інтегрована інформаційно-пошукова система органів внутрішніх справ України, які містять у своєму складі модулі, що забезпечують внесення інформації про зовнішність людини як у формі словесного портрета, так і фотографії [2].

У науковій літературі з точки зору поширеності біометричних методик виділяють «три великі біометрики»: ідентифікація за відбитками пальців, за геометрією обличчя та за райдужною оболонкою ока [2].

Сьогодні системи ідентифікації за відбитками пальців охоплюють більше половини ринку біометричних технологій, системи на основі технології розпізнавання за геометрією обличчя – 13-18%, а системи на основі ідентифікації за райдужною оболонкою ока – 6-9% [2].

Дактилоскопічний метод базується на унікальності та незмінності протягом життя відбитків пальців людини, що доведено криміналістичною наукою та підтверджено експертною практикою. На відбитку пальця знаходяться мінуції – унікальні для кожного узору точки зміни структури папілярних ліній – їх закінчення, роздвоєння, розрив, тощо. Система визначає для кожної мінуції її координати і орієнтацію папілярних ліній у цій точці [2].

Біометричний метод ідентифікації за формою обличчя (автоматичний face-контроль) полягає в тому, що за допомогою відеокамери будується 2D або 3D образ обличчя, при цьому виявляються контури брів, очей, носа, губ, підборіддя, вух та ін. Потім між ними обчислюється відстань і будується множина варіантів у залежності від повороту обличчя, нахилу, зміни міміки [2].

Біометричний метод ідентифікації за термограмою обличчя базується на неповторності розподілу на обличчі кровоносних судин, які виділяють тепло. Для сканування необхідна термочутлива камера інфрачервоного діапазону [2].

Біометричний метод ідентифікації за сітківкою ока базується на унікальності малюнку судин очного дна. При скануванні всередину ока направляється пучок світла (іноді інфрачервоного), а обличчя повинно бути розташоване з високою точністю відносно сканер [2].

За словами Артура Добросердова, надання біологічного зразка від родича зниклої особи – абсолютно безболісна процедура. Для цього необхідно звернутися в поліцію, і слідчий за кілька хвилин організує відбір [3].

Система для відбору ДНК і тривалого його зберігання – це пластиковий прилад розміром не більше, ніж пульт від телевізора. У рідних зниклої безвісти особи відбирається зразок буквального епітелію (мазок з внутрішньої частини щоки), який потім передається слідчим в лабораторію, призначається відповідна експертиза та береться ДНК-профіль [3].

Якщо одна з версій слідства, що зникла особа загинула, при знаходженні тіла (останків) також візьмуть біологічний зразок і виведуть ДНК-профіль. Центральний облік генетичних ознак людини дасть попередній висновок, що є співпадіння. Після цього буде проведена додаткова порівняльна експертиза. Зрештою експерт зможе зробити остаточний висновок, чи належить тіло загиблого до родичів особи, яка здала біологічний зразок [3].

Наразі на території України зразки ДНК можуть відбиратись тільки у кровних родичів: батьків чи дітей зниклої людини. Зазвичай відбирають зразки крові, слини та епітелій з ротової порожнини. У померлих зразки відбираються судово-медичними експертами, які передають їх для опрацювання в Державний науково-дослідний експертно-криміналістичний центр МВС України. Вже там виділяється ДНК-профіль. ДНК-картка направляється до єдиної бази централізованого обліку генетичних ознак людини при Державному науково-дослідному експертно-криміналістичному центрі МВС України, де її поміщають під унікальним ідентифікатором. Ідентифікатор присвоюють і під час реєстрації невстановлених осіб [4].

Після цього встановлюються генетичні ознаки родичів загиблих, зниклих та невпізнаних осіб. У кожному управлінні поліції вже створені робочі групи, які приймають заяви [4].

Після цього ДНК-профіль родича також відправляється до обліку генетичних ознак людини, де в автоматичному режимі проводиться порівняння ДНК-профілів потерпілого та родичів. У разі виявлення збігів про це інформується орган, який призначив експертизу та проводить досудове розслідування. Далі відбувається інформування родичів загиблої особи [4].

Біометричні та генетичні методи дозволяють працювати навіть у випадках, коли відсутні будь-які інші ідентифікаційні дані або коли особа тривалий час вважається зниклою. ДНК-експертиза, зокрема, відіграє роль у встановленні родинних зв'язків та ідентифікації невпізнаних тіл.

Подальший розвиток і впровадження таких технологій потребує чіткого нормативно-правового регулювання, захисту персональних даних та постійного вдосконалення інформаційних систем. За умови комплексного підходу, належної підготовки фахівців і дотримання прав людини біометричні технології та ДНК-експертизи можуть максимально ефективно виконувати своє призначення в системі оперативно-розшукової діяльності.

Література

1. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А. В. Мовчан. – Львів: ЛьвДУВС, 2017, с. 23-24.
2. Електронний ресурс URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/318/1/%D0%BC%D0%BE%D0%B2%D1%87%D0%B0%D0%BD.pdf (дата звернення: 13.12.2025)
3. Кримінальне право та кримінологія. Біометричні методи ідентифікації безвісно зниклих осіб: Р. С. Козьяков, 2015, с. 312-314
4. Ел. ресурс URL: http://jnas.nbuv.gov.ua/j-pdf/Chkup_2015_3_74.pdf (дата звернення: 13.12.2025)
5. МВС України. Як виводиться ДНК-профіль для пошуку осіб, зниклих безвісти за особливих обставин – пояснення Артура Добросердова Електронний ресурс URL: https://mvs.gov.ua/news/iak-vivoditsia-dnk-profil-dlia-posuku-osib-zniklix-bezvisti-za-osoblivix-obstavin-poiasnennia-artura-dobroserdova (дата звернення: 13.12.2025)
6. МОЗ України. Як проходить ДНК-експертиза для пошуку загиблих та зниклих.
7. Електронний ресурс URL: https://moz.gov.ua/uk/jak-prohodit-dnk-ekspertiza-dlja-poshuku-zagiblih-ta- zniklih#! (дата звернення: 13.12.2025)

Рукіна Діана Олексіївна

здобувач вищої освіти Інституту післядипломної освіти та заочного навчання Дніпровського державного університету внутрішніх справ

Синиціна Юлія Петрівна

т.в.о. завідувача кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА ЯК ФАКТОР МОДЕРНІЗАЦІЇ ПРАВОВОЇ СИСТЕМИ

Процес цифровізації будь-яких суспільних відносин є не тільки об'єктивним наслідком еволюції людського буття, але й важливим інструментом для адаптації до сучасних викликів. Основною умовою реалізації зазначеного напрямку є готовність держав інтегрувати інформаційно-комунікаційні технології у всі сфери життя, включаючи правову систему. За таких умов неминучою є побудова нової моделі правового регулювання, яка буде спрямована на забезпечення стійкості громадського суспільства до можливих загроз як внутрішнього, так і зовнішнього характеру, прозорості діяльності органів влади, зміцненню довіри між суспільством та державою, а також розширенню можливостей для участі громадян у державних справах.

Органи сектору безпеки та оборони активно впроваджують цифрові рішення для обробки оперативної інформації, аналітики загроз, ідентифікації кіберризиків та взаємодії між структурами. Водночас інформаційні потоки стають дедалі більшими, а їх обробка вимагає використання сучасних IT-платформ, систем Big Data, автоматизованих аналітичних комплексів та інструментів OSINT. Відзначається поступовий перехід від паперових носіїв до цифрових реєстрів, інтегрованих баз даних та електронного документообігу.

Попри прогрес, система все ще стикається з низкою проблем: фрагментарністю та неузгодженістю державних реєстрів; недостатнім

рівнем кіберзахисту критичної інфраструктури; нестачею кваліфікованих кадрів у сфері цифрової аналітики; технічним відставанням окремих підрозділів; нормативною неврегульованістю окремих аспектів використання новітніх технологій. Значною загрозою залишається вплив кібератак, інформаційно-психологічних операцій та маніпулятивних технологій. Як зазначає Хаустова М.Г. основною метою цифровізації є трансформація вже існуючих сфер життєдіяльності у нові більш ефективні та сучасні завдяки здатності технологій позитивно впливати на ефективність, результативність, вартість та якість економічної, громадської та особистої діяльності. Відповідно її подальший розвиток і застосування будуть можливі лише за умови включені до стратегій і програм розвитку на національному, регіональному та галузевому рівнях всіх наявних напрацювань, починаючи від ідей, а закінчуючи конкретними діями [1, с. 754]. На нашу думку, цифровізація це не лише технічний інструмент, а системний чинник, здатний змінювати основоположні засади функціонування правової системи. Сюди належить: вплив на характер правового регулювання, трансформація механізмів взаємодії між державою та суспільством, а також формування нових моделей забезпечення прав і свобод людини та громадянина. Як наслідок, потрібно звернути увагу на наявні тенденції гармонізації правової дійсності нашої держави з сучасними реаліями.

Процеси цифровізації не лише реформують механізми державного управління, а й докорінно змінюють підходи до правозастосування. Сучасна правова система адаптується до нових цифрових реалій: електронне правосуддя, цифрові докази, електронні реєстри, онлайн-послуги (Дія), впровадження е-підпису та Smart Contracts. Підвищення прозорості, швидкості доступу до інформації, автоматизація процедури фіксації та аналізу порушень формують нову якість юридичної діяльності та сприяють зниженню бюрократії. Принагідно зауважити, що Україна активно намагається впроваджувати такі ініціативи шляхом використання електронного урядування, цифрових судів, блокчейну для державних реєстрів та штучного інтелекту у юридичній діяльності, що своєю чергою повинно гарантувати взаємодію між громадянами та органами влади, підвищуючи прозорість, підзвітність і доступність державних послуг.

Проте на практиці ми зіштовхуємось з низкою суттєвих недоліків, які уповільнюють впровадження використання цифрових технологій у правовій площині [2, с. 149].

Цифрова трансформація посилює можливості для збору, обробки і використання інформації у сфері національної безпеки. Використання систем штучного інтелекту, машинного навчання, автоматизації обробки великих масивів даних забезпечує: швидке виявлення загроз та аномалій; побудову прогнозних моделей; підвищення точності прийняття управлінських рішень; поліпшення міжвідомчої взаємодії та обміну даними.

Окремо зростає роль інформаційної безпеки, кіберзахисту, цифрової криміналістики та аналітики, без яких розслідування сучасних правопорушень майже неможливе. Так, доцільно звернути увагу на думку Жорницької А.І. яка переконана, що невирішеними є наступні питання: подолання цифрової нерівності між регіонами, підвищення цифрової грамотності населення, забезпечення кібербезпеки, розробка єдиної стратегії цифровізації громадянського суспільства та створення фінансових механізмів підтримки цифрових ініціатив [3, с. 656]. Однак більш розгорнутий перелік проблем, які потребують розв'язання викладено у межах Концепції розвитку штучного інтелекту в Україні від 02.12.2020 р. № 1556-р (далі – Концепція) [4].

У межах Концепції пропонується виділити окремий пункт, який стосується складності перевірки відповідності роботи систем штучного інтелекту (далі – ШІ) законодавству та існуючих етичним принципам. Це ускладнює забезпечення прозорості, відповідальності та соціальної безпеки при впровадженні технологій ШІ [4]. Вагомі внески у дослідженні правових питань щодо застосування штучного інтелекту внесені О.А. Барановим, В.М. Брижко, К.С. Мельником, В.Г. Пилипчуком та іншими. Питанням ролі і місця штучного інтелекту в сфері кримінально-правових відносин приділено увагу в роботах В.А. Мисливого, М.В. Карчевського та Н.А. Савінової. Втім, за кожним стриманим кроком наукового пошуку відкриваються ще більші горизонти безмежного пізнання дійсності [5]. При цьому нормативно-правова база України з досліджуваного питання,

охоплюють окремі напрямки цифровізації, інноваційної діяльності та захисту персональних даних для розвитку технологій ШІ. Так, Закони України «Про захист персональних даних», »Про електронну ідентифікацію та електронні довірчі послуги», «Про наукову і науково-технічну діяльність» тощо, формують правову основу для інтеграції технологій ШІ у різні сфери суспільного життя. Разом з тим, з огляду на необхідність відповідності нашої держави стандартам ЄС, НАТО та інших європейських інституцій, виникає потреба у вдосконаленні визначень і підходів до регулювання практичного використання зазначених технологій, що дозволить забезпечити їхню ефективність та відповідність міжнародним нормам у національному контексті. Вбачається, що першочерговим завданням для України є розробка Закону України «Про використання технологій штучного інтелекту», який буде відповідати сучасним міжнародним стандартам та практикам регулювання у цій сфері. Зокрема, важливим орієнтиром є досвід ЄС, адже 01.08.2024 року набув чинності Artificial Intelligence Act (Акт про штучний інтелект), який встановлює правові межі та правила використання технологій штучного інтелекту, визначає класифікацію ризиків, обов'язки розробників і користувачів та гарантує дотримання етичних та безпекових норм його використання [6]. Логічним наслідком такої законодавчої ініціативи буде забезпечення уніфікованих критеріїв етики та безпечного користування ШІ, інтеграція національної практики з міжнародними нормами та створення стабільного правового середовища для розвитку ШІ у різних сферах суспільного життя.

Майбутнє інформаційно-аналітичного забезпечення сектору безпеки та оборони визначатимуть такі напрями:

– створення централізованих інтегрованих платформ обміну інформацією між держорганами;

– широке застосування штучного інтелекту, автоматизованого OSINT та систем прогнозування;

– впровадження стандартів кіберстійкості та цифрової безпеки;

– підготовка нової генерації фахівців цифрової аналітики й кібербезпеки;

– адаптація законодавства до швидких технологічних змін (регулювання ШІ, цифрових доказів, кіберзлочинів);

– розвиток електронного правосуддя та автоматизованих реєстрів.

З урахуванням вищезазначеного, можна зауважити, що одним із чинників розвитку правової системи є цифровізації. У контексті досвіду нашої держави вбачається наявність певних труднощів щодо реалізації цього процесу, зокрема починаючи від цифрової невірності, закінчуючи можливими кіберзагрозами. Враховуючи це, оновлення нормативно-правової бази та ухвалення спеціального закону, що відповідатиме європейським стандартам у досліджуваній сфері є гарантом ефективного та безпечного використання технологій ШІ.

Література

1. Хаустова М.Г. Вигоди, ризики та проблеми цифровізації суспільства: загально-теоретичний аспект. Аналітично-порівняльне правознавство. 2023. № 5. С. 753-759.
2. Маньгора В. В., Михальчук Ю. О. Використання цифрових технологій у праві: перспективи та виклики. Інформація і право. 2023. №4(47). С. 147−158.
3. Жорницька А. І. Цифровізація громадянського суспільства: перспективи та виклики для регіонів України. Державне будівництво. 2024. № 2 (36). С. 656–664.
4. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02 груд. 2020 р. № 1556. URL: https://www.kmu.gov.ua/npas/pro-shvalennyakoncepciyi-rozvitku-shtuchnogo-intelektu-vukrayini-s21220 (дата звернення: 19.11.2025).
5. Синиціна Ю.П. Штучний інтелект як інструмент інформаційної безпеки державних і комерційних установах Moderní aspekty vědy: XXVI. Díl mezinárodní kolektivní monografie /Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Instituts.r.o., 2022. str. 588 – 599.

6. AI Act enters into force. Directorate-General for Communication. URL: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en. (дата звернення: 19.11.2025).

Рущишин Роман Романович

курсант факультету №2 Львівського державного університету внутрішніх справ

Пиляк Ігор Михайлович

курсант факультету №2 Львівського державного університету внутрішніх справ

Рудий Тарас Володимирович

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

РЕАЛІЗАЦІЯ МЕТОДУ ГАУСА ДЛЯ РОЗВ'ЯЗАННЯ СИСТЕМ ЛІНІЙНИХ АЛГЕБРИЧНИХ РІВНЯНЬ З КІЛЬКОМА ПРАВИМИ ЧАСТИНАМИ МОВОЮ ПРОГРАМУВАННЯ С++

Система лінійних алгебраїчних рівнянь (СЛАР) є однією з фундаментальних математичних моделей, що описують широкий спектр задач у фізиці, інженерії, економіці, комп'ютерних науках та інших галузях. Загальний вигляд СЛАР можна подати як AX=B, де A – квадратна матриця коефіцієнтів, X – вектор або матриця невідомих, а B – вектор правих частин. Якщо правих частин кілька, тоді кожен стовпець матриці B відповідає окремій системі з тією ж матрицею коефіцієнтів. Такі задачі часто виникають при застосуванні числових методів, коли потрібно розв'язати одну й ту ж СЛАР для різних наборів початкових даних (інваріантних розрахунків).

Метод Гауса є класичним і найбільш універсальним способом розв'язання СЛАР. Його ідея полягає в тому, щоб за допомогою елементарних операцій над рядками перетворити матрицю A до

потрібного нам вигляду [1]. Це досягається шляхом послідовного виключення невідомих: на кожному кроці вибирається опорний елемент на діагоналі, рядок нормується, а всі елементи під ним стають нулями. Після завершення цього процесу система набуває вигляду, зручного для зворотного ходу, коли невідомі обчислюються починаючи з останнього рівняння. У випадку кількох правих частин усі ті самі операції застосовуються до кожного стовпця матриці B, що дозволяє отримати одразу матрицю розв'язків.

У програмному реалізуванні методу Гауса ключову роль відіграють вкладені цикли. Зовнішній цикл проходить за діагональними елементами матриці, визначаючи поточний опорний рядок. Усередині нього виконуються цикли нормування рядка та цикли, які присвоюють значення нуль елементам під головною діагоналлю. На етапі зворотного ходу інший цикл рухається від останнього рядка до першого, а вкладений цикл присвоює значення нуль елементам над головною діагоналлю. Така структура циклів повністю підпадає під логіку методу Гауса: кожен рівень вкладеності відповідає певному рівню обробки матриці - рядок, стовпець або праві частини.

Метод Гауса є прямим методом, тобто він гарантує отримання точного розв'язку (за умови невиродженості матриці) за скінченну кількість кроків. Його перевага полягає в універсальності та можливості застосування до довільної квадратної системи. У випадку множинних правих частин він особливо ефективний, оскільки найскладніша частина – прямий хід – виконується лише один раз. Саме тому цей метод широко використовується в числових алгоритмах, реалізованих мовами програмування, зокрема C++.

```
#include <iostream>
#include <vector>
#include <string>
using namespace std;

template <typename T> class Matrytsia
{
private:
```

```
    vector<vector<T>> dani;
    int ryadky;
    int stovptsi;
public:
    Matrytsia(const          vector<vector<T>>&
vhidni_dani) : dani(vhidni_dani) {
        ryadky = vhidni_dani.size();
        stovptsi    =    (ryadky    >    0)    ?
vhidni_dani[0].size() : 0;
    }
    Matrytsia(int  r,  int  s)  :  ryadky(r),
stovptsi(s) {
        dani.resize(r, vector<T>(s));
    }
    void druk(const string& nazva) const {
        cout << nazva << «:\n»;
        for (int i = 0; i < ryadky; i++) {
            for (int j = 0; j < stovptsi; j++)
{
                cout << dani[i][j] << «\t»;
            }
            cout << endl;
        }
        cout << endl;
    }
    Matrytsia<T>              mnozhennia(const
Matrytsia<T>& insha) const {
        if (stovptsi != insha.ryadky) {
            throw       runtime_error(«Rozmiry
matryts ne pidkhodyat dlya mnozhennia!»);
        }
        Matrytsia<T>          rezultat(ryadky,
insha.stovptsi);
        for (int i = 0; i < ryadky; i++) {
            for (int j = 0; j < insha.stovptsi;
j++) {
                rezultat.dani[i][j] = 0;
                for (int k = 0; k < stovptsi;
k++) {
```

```
                    rezultat.dani[i][j]     +=
dani[i][k] * insha.dani[k][j];
                }
            }
        }
        return rezultat;
    }
    static                          Matrytsia<T>
metodGaussa(Matrytsia<T> A, Matrytsia<T> B) {
        int n = A.ryadky;
        int m = B.stovptsi;
        // Pryamyi khid
        for (int k = 0; k < n; k++) {
            T opornyi = A.dani[k][k];
            for (int j = k; j < n; j++)
                A.dani[k][j] /= opornyi;
            for (int j = 0; j < m; j++)
                B.dani[k][j] /= opornyi;
            for (int i = k + 1; i < n; i++) {
                T koef = A.dani[i][k];
                for (int j = k; j < n; j++)
                    A.dani[i][j]  -=  koef  *
A.dani[k][j];
                for (int j = 0; j < m; j++)
                    B.dani[i][j]  -=  koef  *
B.dani[k][j];
            }
        }
        // Zvorotnyi khid
        for (int k = n - 1; k >= 0; k--) {
            for (int i = k - 1; i >= 0; i--) {
                T koef = A.dani[i][k];
                for (int j = 0; j < m; j++)
                    B.dani[i][j]  -=  koef  *
B.dani[k][j];
                A.dani[i][k] = 0;
            }
        }
        return B;
    }
```

```
};
int main() {
    vector<vector<double>> vektorA = {
        {1, 1, 2, 3},
        {3, -1, -1, -2},
        {2, 3, -1, -1},
        {1, 2, 3, -1}
    };
    vector<vector<double>> vektorB = {
        {1, 2, 3, 4},
        {-4, 1, -2, 2},
        {-6, 3, 1, -1},
        {-4, -1, 2, 3}
    };
    Matrytsia<double> A(vektorA);
    Matrytsia<double> B(vektorB);
    A.druk(«A»);
    B.druk(«B»);
    Matrytsia<double>           X           =
Matrytsia<double>::metodGaussa(A, B);
    X.druk(«X»);
    Matrytsia<double> AX = A.mnozhennia(X);
    AX.druk(«A * X (perevirka)»);
    return 0;
}
```

Результат виконання програмного коду:

A:

1 1 2 3

3 -1 -1 -2

2 3 -1 -1

1 2 3 -1

B:

1 2 3 4

-4 1 -2 2

-6 3 1 -1

-4 -1 2 3

X:

-1 0.745098 0.0196078 1.11765

-1 0.509804 0.627451 -0.568627

0 -0.686275 0.411765 1.13725

1 0.705882 0.509804 0.392157

A * X (perevirka):

1 2 3 4

-4 1 -2 2

-6 3 1 -1

-4 -1 2 3

Висновок.

Розроблений проєкт програмного коду надає такі можливості:

– забезпечує розв'язання СЛАР з кількома правими частинами;

– використовує стандартні контейнери STL (vector), що робить його універсальним та гнучким;

– має модульну структуру, що спрощує розуміння та модифікування;

– дозволяє відслідковувати проміжні результати.

Література

1. Огірко О. І., Галайко Н. В. Вища математика: навчальний посібник. – Львів: Львівський державний університет внутрішніх справ, 2025. 370 с. Онлайн-ресурс. – URL: https://dspace.lvduvs.edu.ua/handle/1234567890/8789

Савінчук Олександр Олегович

курсант спеціальності 262 «Правоохоронна діяльність» факультету № 2 (з підготовки фахівців для підрозділів превентивної діяльності та правоохоронних інформаційних систем) Львівського державного університету внутрішніх справ

Мовчан Анатолій Васильович

професор кафедри оперативно-розшукової діяльності навчально-наукового інституту з підготовки фахівців для підрозділів кримінальної поліції Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ ОБОРОННОЇ СФЕРИ

У сучасних умовах зростання глобальних і регіональних безпекових загроз оборонна сфера дедалі більше потребує оперативного, точного та обґрунтованого аналітичного забезпечення. Обсяги інформації, що надходять із різноманітних джерел – розвідувальних систем, супутникових спостережень, кіберпростору, відкритих джерел та бойових підрозділів, – значно перевищують можливості їх ефективної обробки традиційними методами. У цьому контексті штучний інтелект виступає ключовим інструментом трансформації аналітичних процесів в оборонній сфері. Завдяки здатності швидко обробляти великі масиви даних, виявляти приховані закономірності, прогнозувати розвиток подій і підтримувати процес ухвалення рішень, технології ШІ істотно підвищують рівень ситуаційної обізнаності та ефективність управління оборонними ресурсами.

Штучний інтелект відіграє ключову роль у сучасному аналітичному забезпеченні оборонної сфери, оскільки суттєво розширює можливості збору, обробки та інтерпретації великих обсягів інформації, необхідної для прийняття обґрунтованих управлінських рішень у сфері національної безпеки та оборони. В умовах зростання кількості загроз і ускладнення воєнно-політичної обстановки традиційні методи аналізу даних виявляються недостатньо ефективними, що зумовлює потребу у впровадженні інтелектуальних технологій.

Аналітичні системи на основі штучного інтелекту забезпечують обробку значних масивів різнорідної інформації, зокрема текстових, графічних, аудіо- та відеоданих, які надходять із розвідувальних джерел, систем спостереження, кіберпростору та відкритих інформаційних ресурсів. Завдяки застосуванню методів машинного навчання, інтелектуального аналізу даних, нейронних мереж, технологій розпізнавання образів і обробки природної мови підвищується точність оцінки безпекової ситуації, оперативність виявлення загроз і якість прогнозування можливого розвитку подій.

Використання штучного інтелекту в аналітичному забезпеченні оборонної сфери сприяє підвищенню ефективності діяльності суб'єктів сектору безпеки і оборони, зокрема Збройних Сил України, правоохоронних і розвідувальних органів, а також органів стратегічного управління. Інтелектуальні аналітичні платформи дозволяють здійснювати моделювання кризових сценаріїв, прогнозувати наслідки надзвичайних ситуацій, оптимізувати використання ресурсів і координувати дії між різними інституціями [1, с. 6–8].

Особливе значення штучний інтелект має для забезпечення готовності до реагування на надзвичайні та кризові ситуації. Інтеграція інтелектуальних алгоритмів у системи аналізу критичної інфраструктури підвищує рівень раннього виявлення потенційних загроз, ефективність оповіщення та якість управлінських рішень у режимі реального часу. Це дає змогу мінімізувати ризики та запобігати негативним наслідкам для національної безпеки [2, с. 146].

Водночас застосування штучного інтелекту в аналітичному забезпеченні оборонної сфери супроводжується низкою викликів, серед яких ключовими є питання кібербезпеки, надійності алгоритмів, етичних обмежень і правової відповідальності за рішення, ухвалені з використанням ШІ. У зв'язку з цим актуалізується необхідність розроблення чітких нормативно-правових механізмів контролю та регулювання використання інтелектуальних систем у військовій діяльності [3].

У науковому й експертному середовищі активно обговорюється питання формування універсальних міжнародних стандартів застосування

штучного інтелекту у військових цілях. Серед пріоритетних напрямів такого регулювання називають обмеження або заборону розробки повністю автономних бойових систем, здатних самостійно ухвалювати рішення щодо застосування летальної сили без участі людини, встановлення вимог до прозорості та підконтрольності алгоритмів, а також запровадження заходів із недопущення поширення цих технологій серед державних і недержавних акторів, які можуть використовувати їх з агресивною або терористичною метою.

Окрему групу проблем становлять питання кібербезпеки в умовах активного використання штучного інтелекту у військових системах. Залежність сучасних засобів управління, розвідки та озброєння від алгоритмів ШІ формує нові вразливості, які можуть бути використані противником. Кібератаки, спрямовані на компрометацію або маніпуляцію системами штучного інтелекту, здатні спричинити надзвичайно небезпечні наслідки, особливо у разі втручання в управління озброєнням чи стратегічно важливими об'єктами. У зв'язку з цим першочергового значення набуває розвиток адаптивних захисних технологій, зокрема алгоритмів самонавчання, здатних оперативно реагувати на нові типи загроз [4].

Водночас слід враховувати потенціал подвійного використання технологій штучного інтелекту. Рішення, розроблені для потреб оборонної сфери, можуть бути ефективно адаптовані для цивільних галузей, зокрема охорони здоров'я, транспорту, енергетики чи систем реагування на надзвичайні ситуації. Так, аналітичні алгоритми обробки великих даних, які застосовуються у розвідувальній діяльності, можуть бути використані для прогнозування епідемій або запобігання природним катастрофам. Такий підхід сприяє формуванню позитивного суспільного сприйняття оборонних інновацій та стимулює інвестиції у наукові дослідження.

У перспективі очікується поглиблена інтеграція штучного інтелекту з іншими передовими технологіями, зокрема квантовими обчисленнями, блокчейн-рішеннями та біотехнологіями. Подібна технологічна синергія може докорінно змінити способи ведення бойових дій, підвищивши їх

точність, керованість і прогнозованість. Водночас це вимагатиме перегляду традиційних підходів до військової стратегії, етичних засад та норм міжнародного права.

Отже, штучний інтелект відіграє дедалі важливішу роль в аналітичному забезпеченні оборонної сфери, забезпечуючи новий рівень швидкості, точності та комплексності аналізу інформації. Його застосування сприяє підвищенню ефективності стратегічного та оперативного планування, своєчасному виявленню загроз, оптимізації використання ресурсів і підтримці процесів ухвалення управлінських рішень. Водночас впровадження технологій ШІ супроводжується низкою викликів, зокрема питаннями кібербезпеки, надійності алгоритмів, етичної та правової відповідальності за результати їх використання. Тому подальший розвиток і використання штучного інтелекту в оборонній сфері потребує комплексного підходу, що поєднує технологічні інновації з чітким нормативно-правовим регулюванням і людським контролем. Лише за таких умов ШІ може стати ефективним і безпечним інструментом посилення обороноздатності держави.

Література

1. Правоохоронні та спеціалізовані інституції сектору безпеки і оборони України: навчально-методичний посібник / за заг. ред. О. Ю. Бусол. Київ: Юрінком Інтер, 2024. 492 с.
2. Трофименко О. Г., Яремчук М. В. Штучний інтелект у військовій сфері. Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика: матер. міжнар. наук.-практ. конф. (Одеса, 24 листопада 2023 р.). Одеса: НУ «ОЮА», 2023. С. 144–148. DOI: https://doi.org/10.32837/11300.27179.
3. Про оборону України: Закон України від 06.12.1991 р. №1932-XII. URL: https://ips.ligazakon.net/document/view/t193200?an=1&ed=2023_03_21
4. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text

Савчук Костянтин Вікторович
аспірант кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка»

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ ВЕБ АТАКАМ

Веб-додатки сьогодні лежать в основі більшості цифрових сервісів, якими користуються близько 5.5 мільярдів людей для новин, електронної комерції та освіти. Однак саме вони залишаються головними цілями для атак, таких як SQL-ін'єкції (SQLi), міжсайтовий скриптинг (XSS), підробка запитів (CSRF) та DDoS.

Традиційна практика веб-безпеки, що базувалася на захисті периметра та сигнатурних правилах для статичних сайтів, застаріла. Сучасні архітектури, орієнтовані на API та хмарні технології, вимагають переходу до системного зіставлення типів трафіку з протоколами. Актуальною є **семіотична багаторівнева модель** захисту:

- **Семантичний рівень:** шифрування та автентифікація.
- **Синтаксичний рівень:** забезпечення цілісності даних.
- **Прагматичний рівень:** захист від соціальних маніпуляцій.

Аналіз трафіку та поведінки користувачів. Розуміння природи трафіку є ключовим для побудови захисту. Дослідження 2024 року «Механізми захисту трафіку в кіберпросторі» наводить детальну статистику активності, яка підкреслює масштаб обробки даних.

Таблиця 1. Структура інтернет-трафіку та активності Ці дані демонструють величезні обсяги інформації, які необхідно фільтрувати в реальному часі.

Базова лінія захисту та OWASP Top-10. В основі стратегії захисту лежить **OWASP Top-10 (2021)**, який класифікує ризики на основі реальних даних. Атаки часто є комбінованими: наприклад, слабкий токен сесії надає початковий доступ, а IDOR (небезпечні прямі посилання на об'єкти) дозволяє розширити права до повного захоплення облікового запису.

Таблиця 1

Аналіз інтернет-трафіку за категоріями та типами активності

Тип трафіку	Категорія	Обсяг трафіку (%)	Кількість користувачів (млрд)	Середній час сесії (хвилини)	Загальний трафік (ТБ/день)
Веб-серфінг	Новинні сайти	15	2.5	8	500
	Електронна комерція	20	1.8	12	650
	Освітні ресурси	10	1.2	15	300
Соціальні мережі	Facebook	30	2.9	20	900
	Instagram	15	2.1	25	600
	TikTok	15	1.8	45	550
	LinkedIn	5	0.9	10	200
Відеострімінг	YouTube	30	2.8	40	1500
	Netflix	25	1.5	120	1200
	Amazon Prime	10	0.8	90	800
Онлайн-ігри	Комп'ютерні ігри	20	1.2	60	1000
	Мобільні ігри	15	2.5	30	700
	Консольні ігри	10	0.7	120	800

Для протидії цим загрозам використовуються **детерміновані базові засоби контролю**, які ШІ не замінює, а доповнює:

– **Протидія ін'єкціям та XSS:** Використання параметризованих запитів, сувора валідація вхідних даних та політики безпеки контенту (CSP).

– **Захист сесій та CSRF:** Впровадження SameSite cookies, короткоживучих токенів та багатофакторної автентифікації (MFA) для ризикованих дій.

– **Інфраструктурна безпека:** WAF для нормалізації запитів та віртуального патчингу, а також TLS/HSTS для наскрізного шифрування.

Роль Штучного Інтелекту: Від правил до поведінкового аналізу. Масштабування загроз вимагає автоматизації. Галузеві звіти (Qualys, Fortinet) визначають роль ШІ як інструменту для аналізу великих масивів сигналів (Big Data) з метою раннього виявлення аномалій. ШІ дозволяє перейти від реагування на інциденти до їх прогнозування.

Технологічні підходи у застосуванні AI/ML:

1. **Вбудовування HTTP (Embeddings) та NLP:** Метод **HTTP2vec** розглядає HTTP-запити як текстову послідовність (мову). Моделі навчаються створювати векторні представлення (embeddings), що фіксують структуру та вміст запитів. Це дозволяє виявляти аномалії, такі як SQL-ін'єкції, аналізуючи відхилення від «нормальної граматики» запитів.
2. **Графові нейронні мережі (GNN):** Традиційний аналіз окремих запитів часто пропускає складні атаки. GNN моделюють зв'язки між сутностями (Користувач ↔ Пристрій ↔ Сесія ↔ IP). Це дозволяє виявляти скоординовані атаки та шляхи шахрайства, які непомітні при лінійному аналізі логів.
3. **Онлайн-виявлення аномалій (Kitsune):** Використання ансамблів невеликих автокодерів дозволяє виконувати аналіз трафіку безпосередньо на шлюзах або IoT-пристроях з низьким енергоспоживанням, забезпечуючи швидку реакцію.

Емпіричні докази ефективності (Case Studies). Інтеграція ШІ в системи SIEM/SOAR демонструє конкретні операційні переваги. Згідно з даними реальних впроваджень, поєднання базових контролів із моніторингом ШІ забезпечує:

– Зменшення кількості хибних спрацювань (False Positives) на **~60%**.
– Пришвидшення розслідування інцидентів на **~40%**.
– Зниження ризиків захоплення облікових записів (АТО).

Таблиця 2 показує результати впровадження ШІ.

Таблиця 2

Випадки застосування штучного інтелекту в кібербезпеці та результати робити ШІ

Використання ШІ	Реальний приклад	Галузь / Сектор	Вплив / Результат
Виявлення загроз та моніторинг аномалій	Darktrace & Aviva	Фінанси / Управління статками	73 правдивопозитивних сповіщень про дії проти 11 раніше; проаналізовано 23 млн подій
Виявлення та запобігання шкідливому ПЗ	CordenPharma & Darktrace	Фармацевтика	Заблоковано криптомайнер; запобігли ексфільтрації >1 ГБ даних
Протидія захопленню облікових записів (АТО) та захист ідентичності	Memcyco & Global Bank	Банківська сфера	18 500 випадків АТО/рік зменшено на 65%
Виявлення інсайдерських загроз	Securonix & Golomt Bank	Фінансові послуги	На 60% менше хибних спрацювань; розслідування швидше на 40%; кількість сповіщень зменшено з 1 500 до <200/день

Безпека IoT та OT	Smart City Deployment	Міська інфраструктура	Точність виявлення аномалій ~96–97%; децентралізоване виявлення; реакція <30 с
Реагування на інциденти та автоматизація SOC	DXC Technology	Технології / Керовані послуги	Зменшення сповіщень на 60%; реакція швидше на 50%
Зменшення перевантаження сповіщеннями	IBM QRadar & Gulf-Based Bank	Банківська сфера	Менше сповіщень і хибних спрацювань; підвищена ефективність SOC
Розвідка загроз та превентивний захист	IBM Watson AI	Технології	Проактивне виявлення загроз; раннє попередження про шкідливе ПЗ та внутрішні ризики
Захист електронної пошти та запобігання фішингу	Google Gmail	Технології / Комунікації	Щодня блокуються мільйони фішингових листів за допомогою ML-моделей
Модерація контенту та виявлення загроз у соцмережах	Facebook NLP Monitoring	Соціальні мережі	Виявлення шкідливого контенту в реальному часі; кращий аналіз трендів
Виявлення фінансового шахрайства	Visa AI	Платежі	Заблоковано 80 млн шахрайських транзакцій

Виявлення та захист фінансових даних	Capital One & AWS Macie	Банківська сфера	Класифікація чутливих даних; автоматична реакція на аномалії

Висновки. Аналіз показує, що ШІ не є панацеєю, яка замінює традиційні засоби захисту, а виступає потужним підсилювачем («Force Multiplier»). Рекомендована стратегія є гібридною:

1. Підтримувати сувору базову гігієну (валідація, шифрування, WAF).
2. Інтегрувати високоякісні сигнали ШІ через SIEM/SOAR для обробки великих обсягів даних.
3. Інвестувати в MLOps та інтерпретованість моделей, щоб аналітики розуміли причини спрацювання правил безпеки.

Подальші дослідження мають зосередитися на створенні специфічних для вебу наборів даних та методів навчання, що зберігають конфіденційність, для скорочення розриву між теорією та практикою.

Література

1. OWASP Top 10. URL: https://owasp.org/Top10/
2. Qualys. AI Security Monitoring. URL: https://blog.qualys.com/product-tech/2025/04/18/ai-security-monitoring
3. Fortinet. Artificial Intelligence in Cybersecurity. URL: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity
4. AIMultiple. AI Cybersecurity Use Cases. URL: https://research.aimultiple.com/ai-cybersecurity-use-cases/
5. Fontugne R. et al. HTTP2vec: Embedding of HTTP Requests for Detection of Anomalous Traffic. arXiv preprint arXiv:2108.01763. URL: https://arxiv.org/abs/2108.01763

Сербенюк Симон
науковий співробітник Харківського національного університет внутрішніх справ

ПРАВО НА ЯКІСНУ ОСВІТУ ЯК СПЕЦИФІКА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ЗВО, ЩО ГОТУЮТЬ ВІЙСЬКОВИХ І ПОЛІЦЕЙСЬКИХ, В УМОВАХ ВОЄННОГО СТАНУ

Особливої уваги в контексті воєнного стану заслуговує огляд специфіки міжнародної співпраці ЗВО, що готують військових і поліцейських.

О. Горбунова, розглядаючи міжнародну співпрацю щодо підготовки кадрів для сектору безпеки і оборони, виокремлює міжнародне співробітництво з провідними військовими академіями в рамках програм стажування й обміну, а також з міжнародними освітніми установами щодо проведення спільних тренувань, семінарів та обміну досвідом. Зокрема, доцільність відповідних програм співробітництва окреслюється доступом до «передових методик навчання, включаючи симуляційні тренування, використання сучасного озброєння та техніки, а також практичні заняття за участю іноземних інструкторів». [1, с. 166]

В контексті підготовки правоохоронців / персоналу сфери безпеки В. Дубина і В. Світличний наголошують на співпраці з міжнародними організаціями, з-поміж яких за ступенем важливості виокремлюють Організацію Об'єднаних Націй (ООН), Європейський Союз (ЄС) та Організацію з безпеки і співробітництва в Європі (ОБСЄ). Так, ОБСЄ відіграє важливу роль у реформуванні вітчизняного сектору безпеки завдяки освітнім ініціативам, що спрямовані на вдосконалення у відповідності до потреб сучасного суспільства навичок майбутніх та/або чинних поліцейських, прикордонників щодо забезпечення правопорядку, професійної поведінки в контексті дотримання сучасних стандартів щодо етичного ставлення до громадян, гендерної рівності та дотримання прав

людини. ЄС за допомогою місії EUAM Ukraine (Місія ЄС з підтримки реформ цивільного сектору безпеки) задіяний в оновленні вітчизняної системи підготовки кадрів сфери правопорядку. Зокрема, в рамках навчальних модулів, розроблених спільно з українськими інституціями, приділяється увага протидії корупції, аналітиці ризиків, стратегічному плануванню, цифровій криміналістиці, а також розвитку лідерських якостей та формуванню нової управлінської культури тощо. [2, с. 200]. Співпраця з ЄС створює можливість проходити стажування у навчальних закладах і правоохоронних структурах Європи [2, с. 200], а співпраця з міжнародними організаціями в цілому є важливим фактором у впровадженні сучасних технологій в освітній процес (симуляційні тренінги, інтерактивні освітні платформи тощо, які дозволяють здійснювати навчання у максимальній наближеності до реальних професійних умов) [2, с. 201].

У свою чергу, Є. Зозуля та К. Видрич виділили приклади найбільш продуктивних практик міжнародної співпраці щодо підготовки кадрів сектору безпеки і оборони, зокрема [3, с. 226-227]: спільні програми (подвійних дипломів) Національного університету оборони України (НУОУ) та військових академій Великої Британії, Польщі, США тощо; курси НАТО з питань стратегічних комунікацій, кризового управління, кібервійни; міжнародні школи безпеки (зокрема в рамках співпраці ЗВО, НАТО та ЄС), які створюються з метою підготовки лідерів сфери безпеки та оборони; програма «Defense Education Enhancement Program» (DEEP) як освітня ініціатива НАТО щодо реформування військової освіти в країнах-партнерах (Грузія, Молдова, Україна); діяльність Європейського коледжу безпеки та оборони (ESDC) щодо проведення тренінгів для цивільних та/або військових експертів щодо гібридних загроз, кризового менеджменту і стратегічного планування; ініціативи ОБСЄ щодо навчальних курсів з кібербезпеки, протидії тероризму, контролю над озброєннями тощо; співпраця вітчизняних й іноземних військових університетів та академій у рамках спільних досліджень в галузях міжнародної безпеки, військової стратегії та технологій; стажування викладачів вітчизняних військових ЗВО у Балтійському оборонному коледжі, Військовій академії США тощо. [3, с. 226- 227]

У свою чергу, В. Іванов акцентує увагу на співпрацю з НАТО, зокрема: Україна у рамках Індивідуального плану партнерства з НАТО отримала підтримку щодо реформ в системі військової освіти; в рамках співпраці з експертами НАТО і провідними військовими академіями Заходу в межах Програми DEEP (Defence Education Enhancement Programme) у вітчизняних ЗВО сектору безпеки було упроваджено нові навчальні програми та здійснено обмін досвідом між викладачами та здобувачами освіти; тощо. [4, с. 230-231]

Останні тези доповнює М. Лапчик, який в контексті раціоналізації трансформації вітчизняної військової освіти, наголошує на співпраці з ООН, ЄС, ОБСЄ, а особливо – з НАТО та окремій двосторонній з країнами-членами Альянсу. Окремо зауважено на програмах професійної військової освіти (PME), обміні досвідом між інструкторами та спільних навчаннях й оцінках [5, с. 359]. Крім того, поряд з програмою НАТО DEEP виокремлено Програму професійного розвитку (Professional Development Programme), в рамках яких «українські військові виші отримують методичну, наукову та кадрову підтримку для оновлення змісту навчання» [5, с. 360]. Крім того, М. Лапчик виділяє такі ключові аспекти співпраці ЗВО з НАТО, як: уніфікація відповідно до стандартів НАТО STANAG вітчизняних стандартів і навчальних програм; оновлення матеріально-технічної та дидактичної інфраструктури ЗВО, зокрема – модернізація лабораторій, тренувальних центрів, симуляторів та розвиток дидактичної бази дистанційного навчання; багатонаціональні навчання здобувачів освіти, офіцерів та інструкторів («Maple Arch», «Rapid Trident», «Sea Breeze» тощо); «інтеграція у спільну систему оперативного планування та прийняття рішень відповідно до процедур НАТО (OPLAN, CONOPS, SOP)». [5, с. 360]

Д. Кравчук та Б. Семенишина-Фіголь, розглядаючи підготовку фахівців для підрозділів Національної поліції, виокремлюють Асоціацію європейських коледжів як одну із найвпливовіших практико орієнтованих організацій міжнародної співпраці ЗВО МВС. Як громадська організація, до складу якої входить 53 ЗВО різних країн (точніше, країн-членів ЄС і сусідніх країн), Асоціація на громадських засадах переважно займається

проведенням онлайн тренінгів та конференцій із залученням фахівців-практиків правоохоронних органів різних держав та/або міжнародних організацій, а також поглиблює зв'язки між ЗВО з підготовки правоохоронців, сприяє поширенню найкращих практик і проводить дослідження щодо підготовки поліцейських кадрів тощо. [6, с. 336]

О. Яровий та Р. Валєєв, розглядаючи співпрацю в контексті підготовки поліцейських зауважили на посиленні співпраці з «провідними міжнародними освітніми та безпековими інституціями», роблячи акцент на приведення освітніх програм до європейських стандартів, участі правоохоронців у міжнародних тренінгах, навчаннях і програмах обміну й стажування, створенні платформ систематичного міжнародного обміну професійними практиками. [7, с. 685]

Таким чином, міжнародна співпраця ЗВО, які готують військових і поліцейських, в умовах воєнного стану характеризується не лише спрямованістю на посилення безпеки й оборони, а й приведенням до міжнародних стандартів підготовки фахівців сектору безпеки, оборони та правопорядку, що є безумовною складовою забезпечення права здобувачів освіти відповідних спеціальностей на якісну освіту.

Література

1. Горбунова О. Міжнародна співпраця у підготовці кадрів для сектору безпеки і оборони: обмін досвідом та адаптація до викликів збройної агресії проти України. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. С. 164-167.
2. Дубина В., Світличний В. Роль міжнародних організацій (ОБСЄ, ЄС, ООН) у формуванні моделі підготовки безпекового персоналу. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. С. 199-202.

3. Зозуля Є., Видрич К. Напрями та форми міжнародної співпраці у сфері підготовки кадрів для сектору безпеки і оборони. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. С. 225-229.
4. Іванов В. Міжнародна співпраця та обмін досвідом у сфері підготовки кадрів для сектору безпеки і оборони України. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. С. 229-232.
5. Лапчик М. Роль міжнародних партнерів у підвищенні стандартів військової освіти. впровадження стандартів НАТО у національні програми підготовки. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. С. 359-361.
6. Кравчук Д., Семенишина-Фіголь Б. Міжнародна практика підготовки фахівців для підрозділів Національної поліції: взаємодія органів МВС з міжнародними громадськими організаціями у підготовці фахівців для підрозділів Національної поліції. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. 335-337.
7. Яровий О., Валєєв Р. Міжнародна співпраця та обмін досвідом у сфері підготовки поліцейських кадрів. Актуальні питання підготовки фахівців для сектору безпеки і оборони в умовах війни : матеріали II Міжнародної науково-практичної конференції (м. Кропивницький, 17 квітня 2025 року). Кропивницький : ДонДУВС, 2025. 690 с. С. 684-686.

Смик Денис Дмитрович

аспірант, кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів Україна

Бурак Назарій Євгенович

кандидат технічних наук, доцент, начальник кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів Україна

ЦИФРОВІ ПЛАТФОРМИ ЗБОРУ ТА АНАЛІЗУ ДАНИХ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Цифрові платформи даних – це інтегровані програмно-апаратні рішення, що забезпечують збирання, зберігання і аналіз інформації з різних джерел (сенсорних мереж, БПЛА, супутників, телекомунікацій, відкритих джерел тощо). У сучасній війні та умовах гібридних загроз своєчасна цифрова обробка даних є критичною для підтримки ситуаційної обізнаності і прийняття рішень.

Ключові функції цифрової платформи збору та аналізу даних у секторі безпеки і оборони узагальнено на рис. 1. Цифрові платформи збору та аналізу даних у секторі безпеки і оборони насамперед забезпечують багатоджерельний збір інформації, її централізовану агрегацію та візуалізацію в режимі, наближеному до реального часу. Йдеться про інтеграцію потоків даних від розвідувальних безпілотних літальних апаратів, супутникових систем спостереження, радіолокаційних станцій, тепловізійних комплексів, систем зв'язку, кіберпростору, а також відкритих джерел (OSINT) [1]. Завдяки такій консолідації формується єдиний інформаційний простір, у межах якого можливе не лише пасивне накопичення даних, а й активне керування ними – фільтрація, категоризація, встановлення пріоритетів та маршрутизація до відповідних користувачів залежно від їхніх повноважень та оперативних завдань.

Рис.1. Основні функції цифрової платформи збору та аналізу даних у секторі безпеки і оборони

Ключовою функцією таких платформ є створення цілісної картини поля бою та забезпечення ситуативної обізнаності (situational awareness) на тактичному, оперативному й стратегічному рівнях управління. Інструменти геоінформаційного аналізу дозволяють відображати на електронних картах розташування власних і ворожих сил, лінії фронту, зони ураження, логістичні маршрути, об'єкти критичної інфраструктури та інші ключові елементи операційного середовища. На основі цього формується спільне інформаційне поле для командирів різних рівнів, що дає змогу уникати інформаційних «розривів», підвищувати узгодженість дій підрозділів та зменшувати ризики «дружнього вогню». Візуалізаційні модулі дозволяють налаштовувати відображення даних під потреби конкретного користувача – від детальної тактичної карти для підрозділу на передовій до агрегованих дашбордів для вищого військово-політичного керівництва.

Важливою складовою сучасних цифрових платформ є впровадження інструментів аналітики та штучного інтелекту. Алгоритми комп'ютерного зору, машинного навчання й обробки великих даних дають змогу автоматично розпізнавати об'єкти на аерофото- та відеоматеріалах (бронетехніка, артилерійські системи, засоби радіоелектронної боротьби тощо), виявляти аномалії в поведінці противника (нетипове скупчення техніки, зміна характеру руху колон, поява нових вогневих позицій), а також автоматично корелювати цю інформацію з даними радарів, тепловізорів, радіоперехоплень й іншими сенсорними потоками. Завдяки цьому різко скорочується час циклу «виявлення – оцінка – рішення – ураження», а роль аналітика зміщується від ручної обробки масивів даних до контролю якості роботи алгоритмів, інтерпретації результатів та формування комплексних висновків для керівництва.

Українська система ситуаційної обізнаності DELTA є прикладом того, як подібні функції реалізуються в умовах повномасштабної війни. Вона забезпечує збір даних від військових підрозділів, партнерських структур, технічних засобів спостереження та цивільних цифрових рішень, створюючи єдину операційну картину для Збройних Сил України та інших складових сектору безпеки [2]. Однією з принципових переваг DELTA є збереження історичних даних: інформація про події, розташування сил, результати боїв та інші параметри не видаляється, що дає змогу здійснювати ретроспективний аналіз, відслідковувати динаміку змін на конкретних ділянках фронту, відпрацьовувати моделі поведінки противника та оцінювати ефективність власних дій. Також, система підтримує мобільний застосунок для роботи в умовах обмеженого чи відсутнього зв'язку, захищене файлове сховище для обміну оперативними документами, шифрований чат для координації підрозділів та інтегровані інструменти оперативного планування, що поєднують аналітику з безпосереднім управлінням.

Сучасні цифрові платформи збору та аналізу даних у секторі безпеки і оборони поєднують функції сенсорної інтеграції, аналітичної обробки, візуалізації, комунікації та підтримки прийняття рішень. Завдяки цьому вони трансформують інформаційний цикл: замість фрагментарного й розрізненого збору даних формується комплексне, безперервне

управління знаннями в умовах високої невизначеності та динаміки бойової обстановки. Така інтеграція забезпечує перехід від реактивної до проактивної моделі управління — командири не лише реагують на вже проявлені загрози, а й отримують інструменти для їх раннього виявлення, прогнозування розвитку подій та своєчасного коригування дій сил безпеки і оборони.

У цьому контексті цифрові платформи постають не просто технічним інструментом, а ключовим елементом трансформації системи управління в секторі безпеки і оборони. Вони дають змогу поєднати розрізнені інформаційні потоки різних відомств і зменшити інформаційну асиметрію між тактичним, оперативним і стратегічним рівнями, формуючи культуру прийняття рішень, орієнтовану на доказовість, швидкість та сценарне прогнозування. Водночас результативність таких рішень прямо залежить від якості даних, рівня кіберзахищеності, інтероперабельності систем і готовності персоналу працювати в цифровому середовищі. Тому розвиток платформ має супроводжуватися вдосконаленням нормативно-правового регулювання, стандартизацією форматів даних, інвестиціями в захист інформації та системним підвищенням цифрових компетентностей військовослужбовців і працівників сектору безпеки, що в сукупності створює передумови для побудови цілісної цифрової екосистеми оборони.

У підсумку, цифрові платформи збору та аналізу даних виступають важливим інструментом підвищення ефективності діяльності органів сектору безпеки і оборони України в умовах сучасних воєнних та гібридних загроз. Вони забезпечують більш швидке і точне виявлення загроз, скорочують час на опрацювання інформації та підготовку управлінських рішень, підвищують узгодженість дій різних структур. Завдяки можливостям глибокої аналітики та прогнозування ці платформи сприяють переходу до проактивної моделі реагування, коли загрози і ризики ідентифікуються ще до їх повної матеріалізації. Для України, яка здійснює масштабну оборонну й інституційну трансформацію, системний розвиток таких рішень означає не лише технологічне посилення, а й зміцнення стійкості держави до довготривалих безпекових викликів. Отже, впровадження й масштабування цифрових платформ має розглядатися як

один із пріоритетних напрямів модернізації сектору безпеки і оборони, інтегрований із загальною стратегією цифрової трансформації державного управління.

Література

1. Ukraine's Defence Tech Ecosystem: Real-Time Coordination and AI Targeting in Action. Digital State UA, 2025. URL: https://digitalstate.gov.ua/news/tech/2-sekundy-i-tsil-vyiavleno-iak-pratsiuye-tsyfrova-ekosystema-zsu (дата звернення: 10.12.2025)
2. Delta: система ситуаційної обізнаності сил оборони України. Delta Wiki. Міністерство оборони України. Центр інновацій та розвитку оборонних технологій. URL: https://delta.mil.gov.ua/open-wiki/ (дата звернення: 10.12.2025).

Стельмахович Аліна

здобувач вищої освіти ННІ УПБ Львівського державного університету внутрішніх справ

Магеровська Тетяна Валеріївна

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ BIG DATA-АНАЛІТИКИ У ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ

Практичне впровадження Big Data-аналітики у діяльність правоохоронних органів у сфері протидії торгівлі людьми є складним багатоаспектним процесом, що не обмежується модернізацією програмно-технічних засобів або впровадженням нових інформаційних платформ. Йдеться про глибинну зміну самої логіки аналітичної роботи, трансформацію підходів до збору, обробки та інтерпретації інформації, а також перегляд ролі аналітики у системі ухвалення управлінських і проце-

суальних рішень. У традиційній правоохоронній практиці аналіз здебільшого зосереджувався на фіксації окремих фактів, подій і епізодів злочинної діяльності, тоді як сучасні виклики потребують системного бачення соціальних, економічних і поведінкових процесів, у межах яких формується та відтворюється торгівля людьми.

Особливість цього виду злочинної діяльності полягає в її високому рівні латентності та здатності маскуватися під формально легальні або напівлегальні соціально-економічні практики. На ранніх стадіях торгівля людьми рідко проявляється у вигляді очевидних кримінальних правопорушень, а найчастіше пов'язується з трудовою міграцією, неформальною зайнятістю, діяльністю посередницьких структур або використанням цифрових платформ для вербування. Це істотно ускладнює її виявлення за допомогою традиційних кримінально-процесуальних інструментів, які орієнтовані на реагування на вже вчинені правопорушення. У цьому контексті Big Data-аналітика відкриває принципово нові можливості для виявлення непрямих ознак злочинної діяльності шляхом зіставлення великих масивів різнорідної інформації, що походить із різних джерел і відображає різні аспекти соціального життя.

Архітектура інформаційно-аналітичних систем, призначених для протидії торгівлі людьми, має забезпечувати не лише накопичення значних обсягів даних, а й умови для їх багаторазової інтерпретації залежно від конкретних аналітичних завдань. На практиці це означає необхідність використання гнучких моделей зберігання інформації, здатних працювати з даними різної структури, походження та ступеня надійності. Такий підхід є принципово важливим для правоохоронної сфери, оскільки результати аналітичної роботи можуть підлягати процесуальній перевірці, а отже мають ґрунтуватися на відтворюваних, прозорих і документованих процедурах обробки інформації. Саме можливість простежити шлях формування аналітичного висновку від первинних даних до узагальненого результату є необхідною умовою легітимності використання Big Data в правоохоронній діяльності.

Ключову роль у практичній реалізації аналітичних систем відіграє інтеграція з національними інформаційними ресурсами. Ефективна

протидія торгівлі людьми неможлива без поєднання даних правоохоронних органів з інформацією інших державних інституцій, які фіксують соціально значущі процеси у сферах міграції, зайнятості, соціального захисту та судочинства. Саме на стику різних реєстрів і баз даних виникають можливості для виявлення нетипових ситуацій, які окремо можуть не мати кримінального характеру, але в сукупності свідчать про підвищений ризик експлуатації людини. Водночас на практиці інтеграція таких ресурсів часто ускладнюється як технічними, так і організаційними чинниками, зокрема відсутністю єдиних стандартів даних, обмеженнями доступу та інституційною замкненістю окремих відомств.

Застосування Big Data-підходів дозволяє частково подолати зазначені обмеження за рахунок використання методів зіставлення даних, виявлення дублікатів і суперечностей, а також автоматизованого аналізу аномалій. Важливо підкреслити, що такі аналітичні процедури не замінюють міжвідомчу взаємодію, а, навпаки, сприяють її поглибленню, створюючи спільне інформаційне поле для ухвалення рішень. У цьому сенсі Big Data-аналітика виступає не лише технологічним інструментом, а й каталізатором інституційних змін у системі державного управління, стимулюючи перехід від ізольованого функціонування відомств до координації їхніх зусиль на основі спільного аналізу даних.

Окремого значення набуває міжнародний вимір аналітичної діяльності, оскільки торгівля людьми в сучасних умовах рідко обмежується територією однієї держави. Злочинні мережі активно використовують різницю в національних правових режимах, рівнях контролю та соціально-економічних умовах, що дозволяє їм мінімізувати ризики викриття. Інтеграція з міжнародними інформаційними платформами та участь у транснаціональних аналітичних ініціативах дає змогу правоохоронним органам виходити за межі національного контексту та аналізувати злочинні процеси у ширшому географічному та часовому вимірі. Водночас така інтеграція потребує чіткого правового врегулювання, високого рівня інформаційної безпеки та дотримання міжнародних стандартів захисту персональних даних, що є особливо актуальним у випадках обміну чутливою інформацією.

Практичне використання Big Data-аналітики у правоохоронній діяльності неминуче загострює питання безпеки та конфіденційності. Обробка великих масивів інформації про осіб, зокрема тих, які можуть перебувати у вразливому становищі, створює ризики зловживань, витоків даних і порушення прав людини. Саме тому захист персональних даних має розглядатися не як окремий технічний модуль, а як наскрізний принцип функціонування аналітичної системи. Це передбачає не лише обмеження доступу до інформації та фіксацію дій користувачів, а й чітке розмежування аналітичної та процесуальної функцій, що унеможливлює автоматичне перенесення аналітичних висновків у площину правозастосування без належної перевірки.

Важливим практичним аспектом є проблема інтерпретації результатів Big Data-аналізу. Алгоритмічні моделі здатні формувати складні висновки та прогнозні оцінки, однак без належного пояснення вони можуть бути неправильно сприйняті або використані як безумовна підстава для прийняття рішень. У правоохоронній сфері це є особливо небезпечним, оскільки може призвести до необґрунтованого втручання у права людини або до формування упереджених практик. Тому аналітичні системи мають бути зорієнтовані на підтримку прийняття рішень, а не на їх автоматизацію, зберігаючи ключову роль за підготовленими фахівцями, які несуть персональну відповідальність за результати своєї діяльності.

Кадрове забезпечення залишається одним із найбільш уразливих елементів практичного впровадження Big Data-аналітики. Формування аналітичних підрозділів потребує фахівців, здатних працювати на перетині інформаційних технологій, права та оперативної діяльності. На практиці дефіцит таких кадрів часто призводить до того, що складні аналітичні інструменти використовуються поверхово або не використовуються взагалі, що знецінює інвестиції у технічну інфраструктуру. Це зумовлює необхідність системного підходу до підготовки персоналу, орієнтованого на реальні завдання правоохоронної практики, а не лише на формальне засвоєння технічних навичок.

Безперервне навчання та підвищення кваліфікації аналітичного персоналу є обов'язковою умовою сталого функціонування Big Data-систем. Швидкий розвиток цифрових технологій, поява нових джерел даних і зміна тактик злочинних мереж вимагають постійного оновлення знань і навичок. Водночас навчальні програми мають включати не лише технічні аспекти роботи з даними, а й питання правової відповідальності, етики та захисту прав людини, що є критично важливим у контексті протидії торгівлі людьми та недопущення повторної віктимізації постраждалих осіб.

Таким чином, практичні аспекти впровадження Big Data-аналітики у діяльність правоохоронних органів у сфері протидії торгівлі людьми слід розглядати як комплексну трансформацію, що охоплює інформаційну архітектуру, міжвідомчу та міжнародну інтеграцію, безпекові механізми та кадрове забезпечення. Лише узгоджений розвиток усіх цих компонентів дозволяє перетворити Big Data-аналітику з формального елементу цифровізації на реальний інструмент проактивної, ефективної та правово виваженої протидії торгівлі людьми в сучасних умовах.

Література

1. Василенко В. Ю., Буряк А. М. Безпека даних в епоху цифрової трансформації: проблеми та виклики. Інформація та соціум. 2024. №1. С. 103 – 106.
2. Шопіна І. М. Інформаційна безпека цифрової трансформації. Науковий вісник Львівського державного університету внутрішніх справ (серія юридична). 2023. №1. С. 28 – 35.
3. Mantelero A., Esposito M. S. An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems // arXiv. – 2024.

Талайло Роман Ігорович

студент Львівського державного університету безпеки життєдіяльності

Ткачук Ростислав Львович

професор кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, доктор технічних наук, професор

Маслова Наталія Олександрівна

доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, андидат технічних наук, доцент

ПРОБЛЕМИ ТА РІШЕННЯ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В НАЦІОНАЛЬНУ СИСТЕМУ БЕЗПЕКИ

Розвиток технологій штучного інтелекту (ШІ) відкриває нові можливості для підвищення ефективності управління, оперативного реагування та прогнозування загроз у сфері національної безпеки України. У сучасних умовах гібридних конфліктів інформація стає критичним ресурсом, а аналіз великих масивів даних дозволяє виявляти приховані закономірності та формувати прогностичні сценарії, недоступні традиційним методам [1, 2].

Одним із ключових напрямів є створення інтегрованих систем раннього попередження загроз, що об'єднують дані розвідки, супутникового моніторингу, кіберпростору, соціальних мереж і сенсорних систем. Такі рішення дозволяють своєчасно ідентифікувати підготовку диверсій, терористичних актів або кібератак, забезпечуючи проактивне ухвалення управлінських рішень [3].

ШІ ефективний також у стратегічному плануванні та моделюванні військових ризиків, прогнозуванні напрямків ударів і визначенні вразливих ділянок оборони, що підвищує ефективність управління військами та знижує ризики для особового складу [4].

Важливою є роль ШІ у сфері інформаційної та кібербезпеки. Нейронні мережі дозволяють виявляти дезінформаційні кампанії, аналізувати ботоферми, прогнозувати вплив інформаційно-психологічних операцій, а також передбачати кібератаки на основі поведінкового аналізу та виявлення аномалій у мережах. Практичне впровадження таких систем підвищує стійкість держави до гібридних загроз та захищає інформаційний суверенітет [5, 6].

Міжнародний досвід (США, Велика Британія, Ізраїль) демонструє ефективність інтеграції ШІ у системи аналізу загроз, кіберзахисту та оперативного управління, що поєднує технологічні інновації з підготовкою кваліфікованих кадрів і нормативною регламентацією [7].

Незважаючи на значний потенціал штучного інтелекту для підвищення ефективності системи національної безпеки, його широке впровадження в Україні супроводжується низкою системних проблем, що мають як технологічну, так і організаційно-правову природу. Вказані чинники не лише знижують ефективність інтелектуальних систем, але й можуть створювати додаткові ризики для безпеки держави.

Однією з ключових проблем є відсутність інтегрованої екосистеми державних даних для навчання та функціонування моделей ШІ. Існуючі ресурси різних відомств формувалися автономно з несумісними стандартами, форматами та протоколами доступу, що ускладнює агрегацію та знижує якість навчальних вибірок. Більшість баз даних має низький рівень кіберзахисту, створюючи ризики несанкціонованого доступу або підміни даних, що безпосередньо впливає на точність моделей ШІ. Без централізованих, захищених та стандартизованих дата-сховищ використання ШІ залишається фрагментарним та обмеженим [8].

Окремою проблемою є маніпуляція навчальними даними, навмисна або ненавмисна. Моделі ШІ чутливі до якості та репрезентативності вибірок; потрапляння викривлених або неповних даних може призвести до хибних висновків і прогнозів. У сфері національної безпеки це може спричинити недооцінку реальних загроз, формування помилкових сигналів тривоги та упередженість рішень щодо регіонів, груп або типів активності. Крім того, існує загроза цілеспрямованих атак на моделі (data

poisoning), що використовується у гібридній війні як прихований інструмент стратегічного впливу. Відсутність процедур валідації та аудиту значно підвищує ризики алгоритмічних помилок у критичних системах [9, 10].

Ще одним обмежувальним фактором є дефіцит кадрів, здатних працювати на перетині ШІ, кібербезпеки, воєнної аналітики та державного управління. Більшість фахівців зосереджені або на технічних аспектах обробки даних, або на класичних безпекових дослідженнях, що ускладнює інтеграцію ШІ у практичне ухвалення рішень. Критично важливим є поєднання технічних навичок із розумінням військово-політичних процесів, логіки оперативного управління та наслідків автоматизованих рішень для суспільства. Відсутність системної підготовки міждисциплінарних фахівців знижує практичну цінність ШІ і обмежує його впровадження до експериментального рівня.

Суттєвим викликом залишається невизначеність правового статусу систем штучного інтелекту, особливо у частині автономного ухвалення рішень. В українському законодавстві відсутні чіткі норми, які б регламентували відповідальність за наслідки дій ШІ-систем, порядок їх сертифікації, допустимі межі автономності та механізми людського контролю.

Етичний аспект також набуває особливої ваги, оскільки рішення, прийняті на основі алгоритмів, можуть безпосередньо впливати на життя людей, доступ до ресурсів або застосування сили. Відсутність етичних стандартів використання ШІ у сфері безпеки створює ризик зниження довіри суспільства до державних інституцій і технологій загалом.

Правова невизначеність стримує масштабне впровадження ШІ та ускладнює його інтеграцію у систему державного управління.

Практичні рекомендації щодо впровадження ШІ у сфері національної безпеки України:

1. Створення єдиної захищеної державної платформи даних для навчання та використання моделей ШІ у секторі безпеки і оборони.

2. Розробка національних стандартів застосування ШІ з урахуванням вимог інформаційної безпеки, етики та відповідальності.
3. Інтеграція ШІ у системи стратегічного та оперативного управління ЗСУ, СБУ, ДСНС та інших сил безпеки.
4. Підготовка фахівців нового покоління, які поєднують компетенції у сфері ІТ, аналітики та національної безпеки.
5. Розширення міжнародного співробітництва у сфері спільних досліджень, обміну даними та кращими практиками застосування ШІ.

Таким чином, проблеми впровадження штучного інтелекту в Україні мають комплексний характер і потребують системного підходу до їх розв'язання. За відсутності інтегрованих і захищених даних, належного кадрового забезпечення та нормативно-етичного регулювання застосування ШІ у сфері національної безпеки може не лише не забезпечити очікуваного ефекту, а й сформувати додаткові ризики. У зв'язку з цим подальші наукові дослідження та управлінські рішення мають бути спрямовані на створення цілісної, контрольованої та безпечної державної екосистеми штучного інтелекту, що дозволить підвищити рівень кібер- й інформаційної стійкості та забезпечити якісно новий рівень національної безпеки в умовах сучасних і майбутніх викликів.

Література

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Hoboken : Pearson, 2021. 1136 p.
2. Floridi L. The Ethics of Artificial Intelligence. Oxford : Oxford University Press, 2023. 312 p.
3. Вдовенко О., Шевчук М., Литвиненко П. Штучний інтелект у системах національної безпеки // Інформаційна безпека України. 2022. № 3. С. 45–53.
4. Галіпчак В. М. Інтелектуальні системи прогнозування загроз у гібридних конфліктах // Національна безпека: теорія і практика. 2024. № 1. С. 17–26.
5. Pierri F. et al. Information manipulation and AI-based detection // Nature Human Behaviour. 2022. Vol. 6. P. 123–135.

6. Мазур О. В. Штучний інтелект у забезпеченні кіберстійкості критичної інфраструктури // Кібербезпека: освіта, наука, техніка. 2024. № 1. С. 98–107.
7. Vasyshchev D., Denysenko M. Artificial intelligence in national security systems // Security and Defence Quarterly. 2023. Vol. 41. P. 55–67.
8. Пановик У. П., Ткачук Р. Л. Кібербезпека через призму системного аналізу. Комп'ютерні технології друкарства : зб. наук. пр. Львів : УАД, 2023. № 1 (49). С. 197–208. URL: https://doi.org/10.32403/2411-9210-2023-1-49-197-208
9. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.
10. Балацька В. С., Ткачук Р. Л., Маслова Н. О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України. Кібербезпека: освіта, наука, техніка. Спеціальний випуск : електронне фахове наукове видання Київ, 2025. № 2 (30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

Тимощук Христина Василівна

курсант ННІПФПКП Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

СУЧАСНІ ТЕХНОЛОГІЇ У БОРОТЬБІ З ТОРГІВЛЕЮ ЛЮДЬМИ: РОЛЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ В ДІЯЛЬНОСТІ ОРГАНІВ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

Торгівля людьми є одним із найнебезпечніших транснаціональних злочинів сучасності, що посягає на фундаментальні права і свободи людини та підриває основи національної і міжнародної безпеки. В умовах глобалізації, цифровізації та активного використання інформаційних технологій злочинні мережі значно ускладнили свої механізми вербування, переміщення та експлуатації жертв. Саме тому протидія цьому явищу вимагає від держави не лише класичних правоохоронних заходів, а й системного впровадження сучасних технологій, здатних забезпечити своєчасне виявлення загроз, аналітичне осмислення великих масивів даних та ефективну координацію дій органів безпеки і оборони. Україна, перебуваючи в умовах збройної агресії та масштабних міграційних процесів, особливо гостро відчуває потребу в інноваційних інструментах боротьби з торгівлею людьми, оскільки війна, соціальна вразливість населення та вимушене переміщення створюють сприятливий ґрунт для злочинної діяльності. Тому потрібно проаналізувати особливості використання сучасних інформаційних технологій в протидії торгівлі людьми.

Перш за все потрібно зазначити, що сучасні технології поступово змінюють саму філософію безпекової діяльності держави. Якщо раніше основний акцент робився на реактивні заходи після вчинення злочину, то нині пріоритетом стає превенція, прогнозування та раннє виявлення

ризиків. Інформаційно-аналітичні системи у цьому контексті виступають не просто технічним інструментом, а комплексним середовищем для прийняття управлінських і оперативних рішень. Вони дозволяють акумулювати інформацію з різних джерел, поєднувати дані правоохоронних органів, прикордонної служби, соціальних інституцій, міжнародних партнерів і громадських організацій, формуючи цілісну картину процесів, пов'язаних із торгівлею людьми [1, с. 189-190].

Особливе значення інформаційно-аналітичні системи мають у сфері виявлення та аналізу ризикових груп. За допомогою цифрових інструментів стає можливим відстеження соціально-економічних показників, міграційних потоків, активності в соціальних мережах та онлайн-платформах з працевлаштування. Саме в цифровому просторі сьогодні часто відбувається вербування жертв, маскування злочинної діяльності під легальні пропозиції роботи або допомоги. Аналітичні алгоритми, що застосовуються органами безпеки і оборони України, здатні виявляти аномальні шаблони поведінки, повторювані сценарії оголошень, мережеві зв'язки між акаунтами та ресурсами, що можуть свідчити про організовану злочинну діяльність. Таким чином технології дозволяють перейти від фрагментарних розслідувань до системного аналізу кримінальних мереж [2, с. 70].

Важливою складовою сучасної протидії торгівлі людьми є використання великих даних та штучного інтелекту. Масиви інформації, які накопичуються державними органами, самі по собі не гарантують ефективності без належної аналітичної обробки. При цьому, саме інформаційно-аналітичні системи забезпечують перетворення даних на знання, що мають практичну цінність. Застосування машинного навчання дає змогу прогнозувати можливі маршрути незаконного переміщення людей, визначати потенційні точки концентрації ризиків, оцінювати ймовірність повторної віктимізації осіб, які вже перебували в зоні небезпеки. Для органів безпеки і оборони це означає підвищення точності оперативних рішень і раціональніше використання ресурсів [3, с. 465].

Не менш важливою є роль інформаційно-аналітичних систем у міжвідомчій взаємодії. Торгівля людьми є комплексним явищем, що виходить за межі компетенції одного органу. Ефективна протидія можлива лише за умови узгоджених дій Служби безпеки України, Національної поліції, Державної прикордонної служби, органів прокуратури, соціальних служб та військових структур. Цифрові платформи забезпечують швидкий обмін інформацією, уніфікацію підходів до обліку та аналізу даних, зменшення бюрократичних бар'єрів. У результаті формується єдиний безпековий простір, у якому рішення приймаються на основі повної та актуальної інформації [4, с. 158].

В умовах війни значення інформаційно-аналітичних систем зростає ще більше. Масові переміщення населення, евакуація, перебування людей на тимчасово окупованих територіях або за кордоном створюють нові виклики для органів безпеки і оборони України. Технології дозволяють відстежувати загальні тенденції, координувати дії з міжнародними партнерами, документувати злочини для подальшого притягнення винних до відповідальності. Цифрові інструменти також відіграють важливу роль у захисті самих жертв, забезпечуючи конфіденційність даних, швидкий доступ до допомоги та відновлення порушених прав.

Водночас використання сучасних технологій у боротьбі з торгівлею людьми потребує дотримання балансу між безпекою та правами людини. Інформаційно-аналітичні системи повинні функціонувати в межах закону, з урахуванням принципів захисту персональних даних, недопущення дискримінації та зловживань. Саме правове регулювання, прозорість алгоритмів і підзвітність органів безпеки є необхідними умовами довіри суспільства до цифрових інструментів. Без цієї довіри навіть найсучасніші технології не зможуть повною мірою виконувати свою превентивну та захисну функцію [5, с. 37].

Розвиток інформаційно-аналітичних систем у сфері протидії торгівлі людьми також має стратегічний вимір. Інвестиції у цифрову інфраструктуру, підготовка фахівців, розвиток аналітичної культури в органах безпеки і оборони формують довгострокову спроможність держави реа-

гувати на складні безпекові загрози. Україна, інтегруючись у європейський і світовий безпековий простір, отримує можливість запозичувати кращі практики, обмінюватися даними та спільно протидіяти транснаціональним злочинним мережам [6, с. 60].

Таким чином, сучасні технології у боротьбі з торгівлею людьми перестали бути допоміжним елементом і перетворилися на ключовий інструмент забезпечення національної безпеки. Інформаційно-аналітичні системи дозволяють органам безпеки і оборони України діяти проактивно, передбачати загрози та мінімізувати ризики ще до того, як злочин набуде незворотних наслідків. Їх застосування забезпечує системність, міжвідомчу узгодженість і стратегічне бачення проблеми торгівлі людьми як складного соціального і кримінального явища. В умовах війни та глобальних трансформацій саме цифрові інструменти стають основою для захисту найвразливіших верств населення і документування злочинів для майбутньої відповідальності винних. Водночас ефективність цих систем можлива лише за умови дотримання прав людини, законності та прозорості їх використання. У перспективі подальший розвиток інформаційно-аналітичних систем є необхідною передумовою формування стійкої, сучасної та гуманістично орієнтованої системи безпеки України, здатної протистояти як традиційним, так і новітнім формам злочинності.

Література

1. Кісіль З. Р. Торгівля людьми – соціальна проблема сучасності. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. Львів, 2017. №2. С. 188-193.
2. Андрусишин Р. М., Сидорук І. І., Когут Я. М. Протидія та соціальна профілактика торгівлі людьми в Україні: навчальний посібник. Львів, 2023. 240 с.
3. Лугіна Н. А., Василинчук Ю. О. Торгівля людьми як глобальна проблема транснаціонального характеру. Юридичний науковий електронний журнал. 2020. №2. С. 463-466.
4. Сень Р. Ю. Використання інформаційних технологій у злочинах пов'язаних з торгівлею людьми. Актуальні питання протидії

кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 15 листоп. 2017 р.). МВС України, Харк. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2017. С. 157-159.
5. Гузій В. Виявлення, попередження та розслідування злочинів торгівлі людьми, учинених із застосуванням інформаційних технологій : навч. курс. Київ, 2015. 158 с.
6. Протидія торгівлі людьми в Україні: стратегічні пріоритети, цифрові інструменти та міжвідомча взаємодія : аналітичний звіт. – Київ : Представництво МОМ в Україні, 2023. – 60 с. – URL: https://ukraine.iom.int (дата звернення: 14.12.2025).

Форос Ганна Володимирівна

завідувачка кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Калугін Володимир Юрійович

Професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПРОТИДІЯ ВРАЗЛИВОСТЯМ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Інформаційні системи органів сектору безпеки і оборони (СБО) України становлять фундаментальний компонент національної безпекової інфраструктури, забезпечуючи функціонування критично важливих процесів державного управління у сфері оборони та безпеки. Саме завдяки цим системам здійснюється оперативний обмін даними, підтримується управління військовими, спеціальними та контррозвідувальними операціями, координується міжвідомча взаємодія силових структур, а також реалізуються розвідувальні, аналітичні й кіберзахисні процеси. У глобальному масштабі спостерігається стійка тенденція до зростання

уваги до проблематики інформаційної безпеки, що зумовлено стрімким розвитком цифрових технологій та ескалацією кіберзагроз.

Під інформаційною безпекою розуміється такий стан функціонування інформаційного простору, за якого забезпечується його стабільний розвиток, гарантоване використання інформаційних ресурсів в інтересах особи, суспільства та держави, а також ефективна нейтралізація зовнішніх і внутрішніх загроз. У структурі національної безпеки України інформаційна безпека займає виняткове місце, оскільки інформатизація, цифровізація та масове впровадження телекомунікаційних технологій роблять інформаційні процеси критичними для всіх сфер суспільного життя — від промисловості й оборони до науки, освіти й державного управління. У цих умовах питання забезпечення інформаційної безпеки не лише посилює свою актуальність, але й набуває самостійного стратегічного значення.

Зовнішні та внутрішні загрози інформаційній безпеці мають інтегрований, багатовимірний характер і можуть бути спрямовані на завдання шкоди політичним, економічним, соціальним, військовим, екологічним, науково-технічним та іншим національно значущим сферам. Інформаційна сфера перетворилася на ключовий рушій суспільного розвитку, істотно впливаючи на стан політичної стабільності, економічної стійкості, обороноздатності та функціонування інших складових системи національної безпеки. Відтак рівень захисту інформації прямо визначає ефективність реалізації національних інтересів та результативність діяльності державних інститутів.

Сучасні інформаційні технології, можливості віддаленого доступу до необмежених ресурсів глобальних мереж, експоненційне зростання швидкості обробки даних і повсюдне впровадження телекомунікацій у повсякденне життя формують нові соціально-інформаційні відносини. За умов обмеженості природних, трудових та енергетичних ресурсів саме інформація у розвинених державах стає стратегічним активом, що визначає конкурентоспроможність та рівень національної безпеки. У такому контексті системи захисту інформації виступають базовими елементами механізму забезпечення інформаційної безпеки, без яких

функціонування будь-яких інформаційних процесів стає фактично неможливим. Саме тому дослідження типових вразливостей інформаційних систем набуває критичного значення.

Вразливість інформаційної системи — це структурно-функціональна слабкість технічного чи організаційного характеру, яка може бути використана для порушення конфіденційності, цілісності або доступності даних. Типові вразливості інформаційних систем органів СБО зумовлюються комплексом технічних, організаційних, кадрових та операційних чинників. У контексті триваючої гібридної війни будь-яка з таких вразливостей може бути використана противником для досягнення стратегічно значущих результатів, зокрема паралізації роботи органів управління, дезорганізації системи оборони або компрометації секретної інформації. Їх нейтралізація потребує системного підходу, що передбачає модернізацію інфраструктури, впровадження міжнародних стандартів кіберзахисту, формування ефективної політики управління ризиками, а також підвищення професійної компетентності персоналу. Тільки інтеграція цих заходів у єдину концепцію дозволить сформувати стійку, захищену та функціонально ефективну інформаційну інфраструктуру сектору безпеки і оборони.

У рамках діяльності СБО вразливості можуть формуватися внаслідок: складності та багаторівневості інформаційних систем; використання застарілих, несумісних або гетерогенних технологічних рішень; впливу людського фактора під час експлуатації; недостатнього фінансування процесів модернізації й аудиту; а також інтенсифікації зовнішніх загроз, що включають кібератаки, засоби радіоелектронної боротьби та інтегровані операції противника.

Саме вбачаючи актуальність цієї проблеми, Президентом України наприкінці 2020 року було затверджено «Стратегію національної безпеки України». затверджену 14 вересня 2020 року указом Президента України № 392/2020 [1]

Специфіка сучасного українського державотворення полягає в тому, що серед ключових детермінант загроз її суверенітету, незалежності та демократичного розвитку продовжують домінувати внутрішні

системні дисфункції. До них, зокрема, належать недостатня інституційна спроможність органів державної влади та високий рівень корупційних практик, які істотно знижують результативність ухвалення й реалізації державної політики. Законодавчий процес у багатьох випадках характеризується пріоритетом кількісних показників та політичного самопіару окремих законотворців над якісним опрацюванням нормативних актів, що призводить до втрати їхньої структурної послідовності, практичної застосовності та концептуальної цілісності. Постійне ініціювання реформ без їх комплексної імплементації та доведення до завершальної стадії унеможливлює ефективне управління державними ресурсами, оптимальний їх розподіл і фактично створює бар'єри для розбудови дієвої системи публічного адміністрування.

На тлі зростання інтенсивності сучасних викликів та ескалації загроз національній безпеці продовжує спостерігатися істотна диспропорція між станом сектору безпеки і оборони України та масштабом завдань, визначених у сфері захисту національних інтересів. Це свідчить про необхідність глибокої модернізації підходів до стратегічного планування, ресурсного забезпечення та інституційної взаємодії в межах системи СБО.

Узагальнюючи викладене, можна дійти висновку, що чинні законодавчі документи, попри наявність у них сформульованих пріоритетів розвитку національної безпеки до 2030 року, не забезпечують достатнього рівня практичної деталізації. Для реальної імплементації визначених стратегічних орієнтирів вимагається розроблення цілісного комплексу підзаконних нормативно-правових актів, у яких би містилися чітко структуровані тактичні завдання для кожної з підсистем національної безпеки та визначалися відповідальні суб'єкти їх реалізації.

З позиції автора, необхідним є також перегляд та розширення переліку потенційних загроз, передбачених Стратегією національної безпеки України. Такий перелік має охоплювати весь спектр можливих факторів впливу на життєдіяльність особи, суспільства та держави, а не бути обмеженим лише діяльністю країни-агресора. Комплексний підхід у цьому контексті є передумовою формування повноцінної системи прогнозування та попередження загроз.

Актуальні ризики для національних інтересів та національної безпеки України в інформаційній сфері системно викладені в Доктрині інформаційної безпеки України 2017 року [2]. До них, зокрема, належать: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності держави, деморалізацію особового складу Збройних Сил України та інших військових формувань; провокування екстремістських дій, поширення панічних настроїв, а також дестабілізація суспільно-політичної та соціально-економічної ситуації; розпалювання міжетнічних та міжконфесійних конфліктів. Окремим видом загроз визначено інформаційні операції держави-агресора в інших країнах, спрямовані на формування негативного міжнародного іміджу України. Також актуальною є проблема інформаційної експансії, що реалізується шляхом розгортання контрольованих агресором інформаційних ресурсів і мереж як на території України, так і поза її межами. Додатковий ризик становлять недосконалість системи державної інформаційної політики, фрагментарність законодавчої бази у сфері інформаційних відносин, відсутність цілісного стратегічного наративу та низький рівень медіакультури суспільства. У цьому контексті особливо небезпечним є поширення закликів до радикальних дій, пропаганда ізоляціоністських або автономістських концепцій регіонального співіснування.

Якщо потрібно, можу доповнити текст посиланнями на інші нормативні акт» [2].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Не менш гостро в умовах гібридної війни постає питання кібербезпеки. У сучасному світі кібернетичний простір дедалі частіше слугує для проведення широкого спектра підривних операцій: від викрадення цінної інформації до актів кібертероризму. Насамперед мережі та інформаційні системи містять конфіденційні дані й економічно цінну інформацію, що підвищує стимул для атак. Атаки на інформаційні системи можуть мати серйозні у національному масштабі наслідки, як то перебої у роботі систем комунікацій, витік конфіденційної інформації тощо [3, с. 202].

Необхідність в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору постійно зростає. Актуальним на сьогодні залишається визначення чітких завдань та відповідальних суб'єктів за інформаційну безпеку. Визначаючи цілі, принципи, правові складові, Доктрина має стати основою для розробки проєктів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України; базою для удосконалення норм та юридичних механізмів системи захисту інформації в державі. [4, с. 202].

У зазначеному контексті першочерговими напрямами державної діяльності мають стати комплексні заходи, спрямовані на підвищення стійкості інформаційного середовища сектору безпеки і оборони. До таких заходів належать:

– модернізація та оптимізація наявної системи забезпечення інформаційної безпеки Збройних Сил України, інших військових формувань та уповноважених державних органів, що передбачає розвиток сил і засобів інформаційного протиборства, удосконалення механізмів реагування на інформаційні інциденти та підвищення їхньої оперативної готовності;

– створення та впровадження ефективної системи прогнозування, ідентифікації, моніторингу й оцінювання інформаційних загроз, зокрема таких, що мають ознаки гібридного або кібервпливу, з метою забезпечення випереджального реагування держави;

– комплексна нейтралізація інформаційно-психологічного впливу на населення, у тому числі спрямованого на підрив національних ідентифікаційних маркерів, підміну історичної пам'яті та девальвацію культурних цінностей;

– системне наповнення національного інформаційного простору високоякісним, конкурентоспроможним вітчизняним контентом, який здатний формувати критичне мислення, зміцнювати суспільну та індивідуальну свідомість, сприяти розвитку громадянського суспільства і протидіяти маніпулятивним інформаційним впливам;

– забезпечення ефективної комунікаційної присутності України на тимчасово окупованих територіях, включно з поширенням якісного

національного інформаційного продукту та розробленням цілісної державної політики інформаційної реінтеграції зазначених територій;

– організація сталого механізму психологічної підтримки населення, що проживає на тимчасово окупованих, прифронтових територіях та у населених пунктах, розташованих поблизу лінії розмежування, із залученням фахівців з кризової психології та системою постійного супроводу;

– розвиток загальнонаціональної системи медіаграмотності, інформаційної культури та профілактики правопорушень у сфері інформаційних відносин, включно з формуванням стійкості населення до дезінформації, маніпуляцій, пропагандистських наративів та технологій когнітивного впливу;

– удосконалення правового регулювання у сфері державної політики інформаційної безпеки, зокрема визначення законодавчих механізмів взаємодії державних інституцій із політичними партіями, громадськими організаціями та іншими недержавними акторами з метою узгодженого реагування на інформаційні загрози.

Політика національної безпеки в сучасних умовах повинна бути спрямована, передусім, на захист базових національних цінностей та забезпечення реалізації національних інтересів, а ключовим її завданням має стати не лише реагування на вже наявні загрози, а їхнє стратегічне попередження, формування умов, за яких потенційні ризики мінімізуються ще до моменту їхнього прояву. Високу важливість становить також здатність держави забезпечувати реалізацію власних національних інтересів в умовах динамічних змін геополітичної конфігурації та внутрішньополітичних процесів.

Органи державного управління мають функціонувати не як пасивні суб'єкти, що лише протидіють загрозам, а як активні інституції, спроможні ідентифікувати, передбачати та нейтралізовувати процеси й явища, які перешкоджають досягненню національних цілей у внутрішній та зовнішній політиці, створюючи сприятливі умови для сталого розвитку держави та зміцнення її безпекового потенціалу. [5].

Серед пріоритетів державної політики у сфері інформаційної безпеки можна виділити такі основні напрями:

Захист життєво важливих інформаційних інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз. Враховуючи сучасні загрози національній безпеці України, цей напрям повинен концентруватись на протидії викликам, що пов'язані із застосуванням інформаційних технологій у військово-політичних цілях, у тому числі для здійснення ворожих дій і актів агресії, спрямованих на підрив суверенітету, порушення територіальної цілісності держави.

Література

1. Указ Президента «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»« URL : https://zakon.rada.gov.ua/laws/show/392/2020#Text. 321
2. Доктрина інформаційної безпеки України 2017 р//Електронний ресурс: https://zakon.rada.gov.ua/laws/show/47/2017#Text
3. Гаврильців М.Т Інформаційна безпека держави в системі національної безпеки УкраїниЮридичний науковий електронний журнал № 2/2020 С. 200-203 http://lsej.org.ua/2_2020/54.pdf
4. Дмитренко М. А. Проблемні питання інформаційної безпеки України. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3318/2997.
5. Садовський В; Дацюк А; Марутян Р, Ніцой О. Як визначати пріоритети державної безпекової політики. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28991.pdf.

Шаповалова Влада Сергіївна

студентка магістратури Одеського державного університету внутрішніх справ

ІНСТРУМЕНТИ DATA SCIENCE ДЛЯ АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ КРИМІНАЛЬНИХ ДАНИХ У ПРОЦЕСІ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Сучасні процеси глобалізації, інтеграції та швидкі зміни у сфері безпеки ставлять перед правоохоронними органами нові виклики, вимагаючи від них підвищення ефективності, оперативності та прозорості роботи. Зростання рівня злочинності, поширення організованих і транснаціональних кримінальних угруповань, а також поява нових видів правопорушень, зокрема у галузі кіберзлочинності, підкреслюють необхідність впровадження сучасних управлінських методик. Ці методики мають базуватися на системному використанні інформаційно-аналітичних інструментів та організаційних підходів. Визначення механізму оцінки ефективності діяльності є ключовою умовою для забезпечення належного управління поліцією як на державному, так і на місцевому рівнях. Це обґрунтовує потребу в суттєвому перегляді існуючої системи оцінки роботи Національної поліції [1, с. 140-141].

У контексті цифровізації державного управління аналіз великих обсягів даних (Big Data) стає важливою складовою роботи правоохоронних органів. Сучасні підходи до візуалізації даних, такі як карти злочинності, інтерактивні дашборди, графові моделі й просторово-часові панелі, сприяють покращенню ситуаційної обізнаності, забезпечують більш об'єктивний процес прийняття рішень та підвищують ефективність стратегій превентивної діяльності. Кримінальні дані включають інформацію про типи злочинів, час та місце їх скоєння, характеристики правопорушників і потерпілих, рівень розкриття злочинів тощо. Відповідно до міжнародних досліджень, ефективний аналіз таких даних має базуватися на:

– описовій статистиці (розподіли, частоти, динаміка). Вона допомагає перетворити сирі кримінальні дані на зрозумілу інформацію, придатну для аналітики та управлінських рішень [2, с. 67];

– аналізі часових рядів (моделі ARIMA, SARIMA, експоненційне згладжування). Часові ряди — це дані, впорядковані у часі (денні, тижневі, місячні показники злочинності, кількість викликів поліції, ДТП тощо);

– просторовому аналізі (кластеризація за методом k-means, DBSCAN, аналіз «гарячих точок» за Getis-Ord Gi*), а саме вивченні закономірностей розподілу злочинів у географічному просторі для виявлення територій із підвищеною криміногенністю, аналізу просторових кластерів злочинів, оптимізації розміщення патрулів, планування профілактичних заходів, оцінки ефективності оперативної роботи, підтримки стратегічних рішень (відеонагляд тощо);

– кореляційних та регресійних методах (перевірка залежності між соціально-економічними змінними та рівнем злочинності). Це ключові статистичні інструменти для вивчення взаємозв'язків між соціально-економічними факторами та рівнем злочинності, виявлення причинно-наслідкових тенденцій, прогнозування впливу змін у середовищі на криміногенну ситуацію, обґрунтування державної політики у сфері безпеки;

методах машинного навчання для прогнозування криміногенної активності. Машинне навчання (ML) дає змогу моделювати складні взаємозв'язки у великих масивах даних, що часто недоступні традиційній статистиці. У правоохоронній системі ML використовується для прогнозування рівня злочинності у певних районах, виявлення закономірностей поведінки правопорушників, оцінки ризику повторного злочину (рецидиву), ідентифікації потенційних «гарячих точок», прогнозування навантаження на підрозділи, автоматичного аналізу відео, текстів, кіберзагроз [3, с. 171-172].

Джерелами даних у поліції виступають статистика злочинів, виклики на «102», дані патрульних маршрутів, відео та фото з камер спостереження, соціально-економічні індикатори, геопросторові дані (OpenStreetMap, міські ГІС). Дослідження показують, що інтеграція статистичних і просторових методів дозволяє досягти значно точнішого

моделювання злочинності у порівнянні з традиційними аналітичними підходами.

Візуалізація є ключовим засобом для інтерпретації складних даних та комунікації результатів аналізу між аналітиками, керівниками та оперативними підрозділами. Основними інструментами виступають:

1. Геоінформаційні карти злочинності (Crime Maps) — це візуальні інструменти, які відображають просторове розподілення кримінальних подій на певній території, зазвичай з використанням систем геоінформаційних систем (ГІС). Вони допомагають правоохоронним органам аналізувати, прогнозувати та ефективніше реагувати на злочинність. Hotspot mapping у США (CompStat, NYPD) використовують ГІС для відстеження злочинів у режимі реального часу. Поліція визначає найбільш «проблемні» райони та розподіляє патрулі відповідно. Деякі європейські правоохоронні органи створюють інтерактивні карти для стратегічного планування та оцінки ефективності превентивних програм.

ГІС-технології забезпечують відображення просторових закономірностей, визначення зон підвищеного ризику, оцінку впливу урбаністичної інфраструктури на рівень злочинності. Моделі теплових карт (heat maps) дозволяють швидко ідентифікувати концентрацію правопорушень [2, с. 68-69].

2. Інтерактивні дашборди — це візуальні панелі, які об'єднують різноманітні дані (кримінальні, соціально-економічні, географічні) у зрозумілі графіки, карти, таблиці та KPI, з можливістю інтерактивного аналізу та фільтрації. Прикладами використання є CompStat (США) - інтерактивні панелі з картою «гарячих точок», графіками типів злочинів та статистики по районах. Поліція може відстежувати злочини у реальному часі та планувати патрулі. Predictive Policing Dashboards використовуються алгоритми прогнозування для визначення районів із високим ризиком злочинів.

В Україні Офіс Генпрокурора запустив бета-тест публічного дашборду Єдиного реєстру досудових розслідувань. Дашборд ЄРДР — це

аналітичний модуль, що цифровізує дані прокуратури й судів щодо кримінальних правопорушень, які стосуються бізнесу в Україні. Він містить дані про статистику розслідувань та розгляду в судах справ у зручному для аналізу й сприйняття форматі. Також має фільтри за конкретною статтею або періодом, а також окремо за органами, які розслідують справи [4, с. 204].

Використання таких платформ, як Power BI, Tableau або Qlik, дає можливість створювати динамічні панелі моніторингу з фільтрами за часом, категоріями злочинів, територіями тощо. Це підвищує прозорість діяльності правоохоронних органів.

3. Графові моделі та мережевий аналіз — це потужні інструменти для оцінки ефективності діяльності правоохоронних органів, особливо у сфері боротьби зі злочинністю, організованими угрупованнями та внутрішньою структурою підрозділів. Вони дозволяють аналізувати взаємозв'язки між суб'єктами, потоками інформації та структурою організації.

Графові моделі - це математичне представлення об'єктів у вигляді вершин (nodes) і їх взаємозв'язків у вигляді ребер (edges). Вершини – особи, підозрювані, злочинні угруповання, підрозділи поліції. Ребра – зв'язки між ними (спільні злочини, комунікації, підпорядкування). Прикладами використання є виявлення ключових лідерів злочинних мереж (центральність вузлів); аналіз соціальних мереж підозрюваних для прогнозування їх поведінки; визначення «слабких місць» організаційної структури правоохоронних органів.

Мережевий аналіз – це методика аналізу структур взаємодії, що дозволяє оцінювати ефективність потоків інформації та взаємодії між підрозділами чи особами.

Побудова графів взаємозв'язків між злочинними групами або типами злочинів дозволяє виявити ключові вузли мережі, осередки координації та потенційні точки впливу [3, с. 175].

За результатами дослідження можна зробити наступні висновки. Використання методів аналізу та візуалізації кримінальних даних сприяє

підвищенню точності оцінювання ефективності роботи правоохоронних органів. Це дозволяє об'єктивно визначати тенденції, аномалії та просторові закономірності у процесах, пов'язаних із криміногенною діяльністю. Інструменти Data Science, зокрема статистичні моделі, машинне навчання, геоінформаційні системи та інтерактивні аналітичні панелі, сприяють формуванню доказової бази для управлінських рішень і дозволяють переходити до проактивного, а не реактивного, підходу в діяльності правоохоронних органів. Візуальна аналітика значно підвищує рівень доступності та інтерпретаційності кримінальної інформації для різних груп користувачів — від керівництва до оперативних підрозділів, що сприяє узгодженості дій та підвищенню ефективності реагування. Інтеграція сучасних аналітичних інструментів у практику правоохоронних структур дозволяє оптимізувати процеси планування, прогнозування та контролю, що в перспективі формує основу для побудови прозорої та результативної системи кримінальної політики.

Література

1. Охріменко І. Оцінка ефективності діяльності органів і підрозділів Національної поліції України: погляд на проблему. Підприємництво, господарство і право. 2016. № 11. С. 139-144. – URL: http://nbuv.gov.ua/UJRN/Pgip_2016_11_29 (дата зв-я: 05.12.2025).
2. Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів. Право і Безпека. 2020. № 4. С. 66–72.
3. Федчак І. А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.
4. Карчевський М.В. Протидія злочинності в Україні у форматі Data Science. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2022. № 2. С. 202-227.

Шарко Владислав Васильович

курсант ННІ №4 Харківського національного університету внутрішніх справ

Буняк Анастасія Володимирівна

курсант ННІ №4 Харківського національного університету внутрішніх справ

Лучик Світлана Дмитрівна

професор кафедри інформаційних систем та технологій ННІ №4 Харківського національного університету внутрішніх справ, доктор економічних наук, професор

AI-ОРІЄНТОВАНІ МЕТОДИ ПРОГНОЗУВАННЯ ЕКОНОМІЧНИХ ПРОЦЕСІВ ТА ЇХ ВПЛИВ НА ЯКІСТЬ УПРАВЛІНСЬКИХ РІШЕНЬ

У сучасному світі цифрової трансформації економічні системи стають все більш складними, багатогранними та залежними від швидкості обробки інформації і точності її інтерпретації. Зростання обсягів даних, динамічні зміни на світових ринках, глобальні кризи та посилення конкуренції вимагають нових інструментів для прогнозування економічних процесів. Одним із найефективніших напрямків у розробці аналітичних систем є використання штучного інтелекту (ШІ), який дозволяє створювати високоточні моделі прогнозування на основі величезних обсягів структурованих і неструктурованих даних. Підходи, засновані на ШІ, мають потенціал значно поліпшити якість управлінських рішень у державному та приватному секторах, а також дозволити проактивно реагувати на економічні загрози та можливості.

Штучний інтелект вже відіграє значну роль у прогнозуванні макроекономічних та фінансових показників у застосунках глобальних компаній. За даними McKinsey, понад 70% міжнародних компаній використовують машинне навчання для оцінки ринкових тенденцій, моніторингу споживчого попиту та оптимізації виробничих процесів [1]. Використання

штучного інтелекту, зокрема нейронних мереж і методів глибокого навчання, дозволяє робити більш точні короткострокові та середньострокові прогнози, які враховують сезонність, випадкові коливання та слабко виражені нелінійні залежності. Це особливо важливо в галузях з високою волатильністю, таких як фінанси, енергетика та логістика.

Використання штучного інтелекту в економічному аналізі пропонує переваги, яких практично неможливо досягти за допомогою традиційних економетричних методів. Наприклад, глибокі моделі можуть обробляти тисячі взаємозалежних показників, щоб виявити приховані закономірності, які не піддаються класичному статистичному аналізу [2]. Такі алгоритми успішно використовуються для прогнозування цін на фондовому ринку, аналізу обмінних курсів, виявлення фінансових аномалій, оцінки ризиків дефолту та моделювання сценаріїв зміни споживчого попиту.

Штучний інтелект відіграє особливу роль у макроекономічному прогнозуванні. Урядові установи США, ЄС та Японії активно тестують моделі нейронних мереж для аналізу інфляційних процесів, монетарних циклів та оцінки впливу глобальних потрясінь на національні економіки [3]. Наприклад, Федеральний резервний банк Нью-Йорка використовує моделі машинного навчання для прогнозування ВВП та рівня безробіття, поєднуючи дані з соціальних мереж, супутникових знімків і новинних стрічок. Цей підхід показує значно вищу адаптивність у порівнянні з традиційними моделями, такими як ARIMA або VAR.

Для бізнесу прогностичні можливості штучного інтелекту стають важливим елементом стратегічного планування. Системи ШІ допомагають:

– визначати оптимальні обсяги виробництва та запаси в логістиці; - прогнозувати зміни цін на сировину та енергоносії;

– аналізувати поведінку споживачів і розробляти персоналізовані маркетингові стратегії;

– оцінювати ризики виходу на нові ринки;

– моделювати вплив зовнішніх факторів, таких як обмінні курси, політичні кризи та стихійні лиха, на діяльність компаній.

У фінансовому секторі впровадження штучного інтелекту в процеси прогнозування не лише дозволяє проводити детальну аналітику, але й автоматизувати певні етапи прийняття рішень. Сучасні алгоритми активно використовуються для кредитного скорингу, оцінки платоспроможності клієнтів, аналізу транзакцій на предмет шахрайства та оцінки ризиків інвестиційного портфеля. За даними Європейського банківського управління, банки в ЄС та США змогли зменшити фінансові втрати від шахрайських транзакцій приблизно на 15-25% завдяки впровадженню моделей штучного інтелекту. [4].

Штучний інтелект відіграє важливу роль у формуванні рішень урядів. Системи, що базуються на ШІ, здатні створювати складні економічні сценарії, оцінювати наслідки змін у податковій політиці та прогнозувати вплив міжнародних санкцій і глобальних криз. У країнах з розвиненою цифровою інфраструктурою ШІ активно використовується для моделювання наслідків інфляційних шоків, аналізу динаміки зайнятості та оптимізації бюджетних витрат. Наприклад, уряд Сінгапуру застосовує моделі машинного навчання для прогнозування спаду або зростання економічної активності в різних секторах, що дозволяє своєчасно перерозподіляти ресурси та запобігати економічним дизбалансам [1].

Однією з основних переваг штучного інтелекту в прогнозуванні є його здатність працювати з відкритими джерелами інформації та потоками даних. Як і в підходах OSINT, ШІ може обробляти дані з новин, соціальних мереж, аналітичних платформ, супутникових систем та сенсорних мереж у реальному часі, що дозволяє вчасно виявляти економічні тенденції [2]. Моделі ШІ в поєднанні з алгоритмами аналізу настроїв можуть передбачати реакцію ринку на політичні події, корпоративні новини або глобальні кризи.

Недавні дослідження показують, що впровадження штучного інтелекту в управлінні економічними ризиками значно підвищує точність цього процесу. На корпоративному рівні це виявляється у створенні систем раннього попередження про можливі фінансові загрози, такі як банкрутства контрагентів, зростання цін, дефіцит сировини або проблеми з ліквідністю на ринку. Моделі глибокого навчання можуть

допомогти керівництву приймати проактивні рішення, виявляючи приховані зв'язки між ринковими показниками та внутрішніми даними компанії.

Вплив прогнозування на основі штучного інтелекту на якість управлінських рішень досягається завдяки:

– вищій точності оцінки ризиків завдяки багатовимірному моделюванню;

– швидшій реакції на зміни в економічному середовищі;

– зменшенню ймовірності людської помилки завдяки автоматизації окремих етапів аналізу;

– оптимізації стратегічного планування на основі багатосценарних моделей прогнозування;

– прозорості та об'єктивності рішень завдяки їх залежності від великих наборів даних та статистично значущих залежностей.

Незважаючи на значні переваги, застосування штучного інтелекту для прогнозування економічних процесів створює низку проблем. По-перше, існує питання якості вихідних даних: алгоритми схильні до неповних або спотворених наборів даних, що може призвести до неточних прогнозів [3]. По-друге, існує проблема інтерпретації моделей: багато алгоритмів глибокого навчання є «чорними скриньками», а їхні рішення важко пояснити з точки зору класичної економічної логіки. По-третє, етичне використання штучного інтелекту, забезпечення кібербезпеки та запобігання технологічному зловживанню залишаються важливими питаннями.

Подальший розвиток штучного інтелекту в економічному прогнозуванні пов'язаний з розробкою гібридних моделей, що поєднують економетричні підходи та методи машинного навчання. Очікується, що протягом наступних 5-10 років повсюдно розповсюдяться повністю автономні аналітичні системи, де ШІ зможе самостійно генерувати прогнозні звіти, сценарії економічного розвитку та рекомендувати управлінські рішення.

У майбутньому інтеграція ШІ в економічну політику та корпоративне управління стане фундаментальною для стабільності та

конкурентоспроможності національних економік. Прогнозні технології на основі ШІ формують основу нової парадигми прийняття рішень, яка є науково обґрунтованою, адаптивною та орієнтованою на дані.

Література

1. McKinsey Global Institute. (2024). The state of AI in 2024: Adoption, impact, and barriers. McKinsey & Company. https://www.mckinsey.com
2. OECD. (2023). Artificial Intelligence in Economic Analysis and Forecasting. Organisation for Economic Co-operation and Development. https://www.oecd.org
3. Federal Reserve Bank of New York. Cho, S., Del Negro, M., Diagne, I., … Pacula, B. (2024). The New York Fed DSGE Model Forecast — December 2024. Liberty Street Economics. https://liberty-streeteconomics.newyorkfed.org/2024/12/the-new-york-fed-dsge-model-forecast-december-2024/
4. European Banking Authority. European Banking Authority. (2025). Rising application of AI in EU banking and payments sector. EBA. https://www.eba.europa.eu/sites/default/files/2025-09/146b3558-d026-47bf-a872-f05e93ed30d2/Rising%20application%20of%20AI%20in%20EU%20banking%20and%20payments%20sector.pdf

Шмаков Станіслав

курсант Львівського державного університету внутрішніх справ

Поляк Святослав Петрович

доцент кафедри оперативно-розшукової діяльності ННІПФПКП Львівського державного університету внутрішніх справ, доктор філософії у галузі знань «Право»

ПСИХОЛОГІЧНІ БАР'ЄРИ У ВИКОРИСТАННІ АНАЛІТИЧНИХ ТЕХНОЛОГІЙ ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Цифровізація діяльності Національної поліції України зумовлює зростання ролі аналітичних систем та програмно-технічних комплексів у процесі прийняття управлінських і оперативних рішень. Ефективність упровадження цих технологій значною мірою залежить від психологічної готовності персоналу до їх освоєння та використання. Психологічні бар'єри, зокрема тривожність перед новими цифровими інструментами чи опір змінам, можуть суттєво знижувати результативність аналітичної діяльності та стримувати потенціал технологічних інновацій.

Використання інформаційних технологій відбувається під час збору та аналізу даних, при веденні відеоспостереження, при зберіганні особистих даних, використанні біометричних даних. Саме для забезпечення прозорості при зборі та аналізі даних має бути використано захист даних від несанкціонованого доступу, забезпечено контроль за надійним збереженням даних громадян. Використання інформаційних технологій для збору та аналізу даних повинно бути потужним інструментом для боротьби зі злочинністю та забезпечення безпеки, але лише за умови етичного та відповідального використання [1, с. 63].

Результативність діяльності правоохоронних органів безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення. Відповідно до Положення про Департамент кримінального аналізу Національної поліції України, затвердженого

наказом Національної поліції України від 29.12.2019 № 1354, до основних завдань підрозділів кримінального аналізу належить, зокрема: організація та здійснення інформаційно-аналітичної діяльності для реалізації повноважень поліції; забезпечення формування та підтримка функціонування автоматизованих інформаційних систем, що утворюються в процесі здійснення оперативно-розшукової та аналітичної діяльності [2, с. 147].

Під час упровадження аналітичних технологій у діяльність правоохоронних органів особливої актуальності набувають психологічні бар'єри, які впливають на готовність працівників до використання цифрових інструментів. Серед найбільш поширених перешкод дослідники виокремлюють цифрову тривожність, що виникає внаслідок побоювання допустити помилку при роботі з новим програмним забезпеченням, а також опір змінам, пов'язаний із порушенням усталених професійних звичок. Високий рівень службового навантаження та емоційного виснаження додатково ускладнює процес адаптації працівників до сучасних аналітичних платформ і знижує ефективність їх практичного застосування.

Одним з основних психологічних бар'єрів є опір змінам. Це явище викликане природним бажанням людей зберігати стабільність і уникати невизначеності. Багато працівників можуть відчувати страх перед новими технологіями, оскільки вони не впевнені в своїх здібностях адаптуватися до інновацій. Цей страх може бути підсилений відсутністю інформації про нові технології або їхнє невідоме вплив на робочий процес. Опір змінам часто проявляється у вигляді негативного ставлення, що може призвести до саботажу або затримки в імплементації нових рішень. Іншим важливим фактором є недостатня підготовка. Часто організації не забезпечують належного навчання для своїх працівників, що призводить до відчуття безпорадності. Недостатня підготовка може викликати тривогу та відчуття невпевненості, що, в свою чергу, підсилює опір змінам. Люди, які не відчувають себе впевненими в нових технологіях, швидше за все, не зможуть їх ефективно використовувати, що негативно вплине на загальний успіх впровадження [3, ст. 327].

У результаті це може породжувати замкнене коло, коли низька обізнаність і невпевненість підтримують подальший опір технологічним нововведенням. Ще одним чинником є відсутність системної підтримки з боку керівництва, що знижує мотивацію працівників долати психологічні труднощі. Водночас запровадження регулярного навчання, наставництва та позитивного підкріплення здатне значно зменшити рівень тривожності. Це створює умови, у яких персонал поступово формує довіру до цифрових інструментів і готовність інтегрувати їх у повсякденну професійну діяльність.

Шляхи мінімізації психологічних бар'єрів у використанні аналітичних технологій працівниками Національної поліції України передбачають системний підхід до підвищення професійної компетентності персоналу. Одним із ключових напрямів є впровадження регулярних тренінгів та навчальних програм, які спрямовані на формування навичок роботи з сучасними аналітичними системами та підвищення впевненості у власних діях. Значну роль відіграє психологічна підтримка, зокрема супервізія та наставництво, що дозволяє зменшити страх перед новими технологіями та знизити рівень опору змінам. Важливим інструментом є створення сприятливого організаційного середовища, яке заохочує обмін досвідом та пом'якшує соціальні та емоційні бар'єри. Крім того, впровадження мотиваційних механізмів та визнання досягнень сприяє підвищенню зацікавленості працівників у використанні аналітичних технологій та адаптації до нових професійних вимог.

Сучасна цифровізація діяльності Національної поліції України створює передумови для широкого використання аналітичних технологій у професійній практиці. Водночас психологічні бар'єри, такі як страх перед новими технологіями, опір змінам та недостатня впевненість у власних навичках, залишаються суттєвою перешкодою для ефективного впровадження цифрових інструментів. Високий рівень службового навантаження та обмежена підтримка з боку керівництва лише підсилюють ці труднощі, знижуючи мотивацію та продуктивність працівників. Усунення бар'єрів вимагає системного підходу, що включає навчання, наставництво, психологічну підтримку та мотиваційні заходи. Створення сприятливого організаційного середовища та розвиток компетенцій персоналу

забезпечують формування довіри до технологій і готовності їх ефективно застосовувати. Таким чином, подолання психологічних перешкод є необхідною умовою для підвищення результативності інформаційно-аналітичної діяльності Національної поліції.

Література

1. Рижков, Е. В., Синиціна, Ю. П., Прокопов, С. О., Гребенюк, А. М., & Рибальченко, Л. В. (2024). Інформаційно-аналітичне забезпечення правоохоронної діяльності.
2. Інформаційне забезпечення кримінального аналізу. (n.d.). У Інформаційні технології та логістика в правоохоронних органах: Навчально-методичний посібник (Розд. 14). Київ: VAITE. https://vaite.kiev.ua/doi/ilp/ILP_Ch_14.pdf
3. Переверзева, Г. О. (2024). Психологічні бар'єри на шляху впровадження нових технологій.

Шопіна Ірина Миколаївна

професор кафедри адміністративно-правових дисциплін навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

ПРОФЕСІЙНО ВАЖЛИВІ ЯКОСТІ ФАХІВЦІВ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Здійснення аналітичної діяльності у сучасних умовах функціонування правоохоронної системи України, які характеризуються динамічним розвитком інформаційних технологій, потребує наявності комплексу професійно важливих знань, вмінь та навичок, які формуються під час освітнього процесу та відображені в освітньо-професійних програмах. Водночас використання вказаних знань, вмінь та навичок значною мірою

залежить від ціннісно-мотиваційної, когнітивної та вольової сфер особистості, формування яких носить більш тривалий характер і розпочинається у ранньому дитинстві.

Особливості агресивного комунікативного середовища, притаманного українському інформаційному простору, актуалізують необхідність формування високого рівня інформаційної гігієни у фахівців, що дозволяє фільтрувати деструктивні повідомлення та ефективно протидіяти маніпуляціям свідомістю. Високий рівень емоційної стійкості спеціалістів, які здійснюють аналітичну діяльність, є передумовою для збереження об'єктивності оцінок і раціональності рішень в умовах дефіциту часу, напружених комунікацій, а також дістресів, які виникають внаслідок регулярних нічних повітряних тривог. Заслуговує на увагу думка американського вченого Д. Канемана, який обґрунтовує, що емоційне напруження, страх, тривога та інформаційне перевантаження активують інтуїтивне («швидке») мислення, яке є схильним до когнітивних упереджень і помилок, тоді як аналітична діяльність потребує емоційної стабільності та контролю («повільного» мислення). Вчений обґрунтував, що саме здатність стримувати емоційні реакції є передумовою раціонального аналізу складної та суперечливої інформації [1]. У контексті сучасного інформаційного простору це означає, що емоційна стійкість є ключовою умовою ефективної аналітичної діяльності, оскільки дозволяє мінімізувати вплив маніпулятивних повідомлень, інформаційного шуму та дезінформації на процес прийняття рішень.

У зв'язку зі значним зростанням обсягів фейкових та діпфейкових даних, що цілеспрямовано створюються для дезорієнтації суб'єктів безпекового сектору, ключовою професійно важливою якістю стає критичність мислення, що передбачає глибоку верифікацію першоджерел та інтегративний аналіз отриманих відомостей. Як справедливо зазначають О. Славута і Т. Ященко, якщо аналітики не можуть підтвердити надійність інформації через дезінформацію або відсутність доступу до джерел, це ускладнює можливість прийняття обґрунтованих рішень на основі такої інформації. Водночас варто зважати на людський фактор, оскільки стрес і небезпека в умовах війни можуть впливати на процес раціонального

прийняття рішень, роблячи його менш об'єктивним і збалансованим [2, с.103]. Слід також звернути увагу на результати досліджень, які підтверджують, що критичне мислення у сучасному військовому дискурсі розглядається нарівні з професіоналізмом та стратегічним мисленням, як одна з ключових характеристик компетентного офіцера, спроможного діяти в умовах складної, багатофакторної та швидкоплинної ситуації. У зв'язку з формування критичного мислення у майбутніх командирів набуває характеру пріоритетного завдання військової освіти та професійного розвитку [3, с.80]. Додамо, що ці положення, на нашу думку, зберігають свою актуальність і для освіти правоохоронців. Здатність фахівців інформаційно-аналітичного забезпечення зберігати визначений законом рівень конфіденційності оброблюваних даних та протистояти спробам кібершпигунства є фундаментальною умовою для підтримання національної безпеки та здійснення ефективної розвідувальної діяльності.

Швидкий розвиток технологій штучного інтелекту та їхня інтеграція в системи збору й обробки даних вимагають від фахівців формування компетентностей щодо ефективної взаємодії з цими інструментами, які значно пришвидшують обробку великих масивів інформації. Водночас обов'язковим є збереження критичності до результатів, генерованих штучним інтелектом, оскільки алгоритми можуть успадковувати систематичні помилки або бути скомпрометованими, що створює ризик прийняття помилкових стратегічних рішень на державному рівні. Варто також звернути увагу на небезпечні тенденції, пов'язані із використанням штучного інтелекту в аналітичній діяльності. З одного боку, активне застосування його можливостей пов'язано із покращенням якості продукту: точнішими, менш упередженими прогнозами. Однак існують докази того, що внаслідок широкого виростання штучного інтелекту цінність праці аналітиків знижується, що викликає їх звільнення або перерозподіл зусиль в бік соціальних видів діяльності [4]. На нашу думку, такі тенденції утворюють ризики депрофесіоналізації аналітичного середовища, а також можуть сприяти зниженню якості контролю за результатами роботи технологій штучного інтелекту.

Надзвичайно важливе значення для професійної успішності фахівців у сфері інформаційно-аналітичного забезпечення має їхня ціннісно-мотиваційна сфера. Розвинена соціальна та професійна відповідальність, стійка внутрішня мотивація забезпечують прагнення до безперервного саморозвитку й підвищення кваліфікації, обумовлюють конструктивне подолання наслідків стресових ситуацій.

Література

1. Kahneman, D. Thinking, Fast and Slow. New York : Farrar, Straus and Giroux, 2011. 499 p.
2. Славута О. І., Ященко Т. С. Проблеми аналітичного забезпечення в умовах війни. С.102-103. Функціонування суб'єктів економічної діяльності в умовах післявоєнної розбудови: матеріали Всеукр. наук.-практ. конф. (м. Харків, 23-24 листоп. 2023 р.). Харків, 2023. С.102-103.
3. Стасюк В. В. Критичне мислення як інструмент ухвалення управлінських рішень офіцерами в умовах воєнних конфліктів. Гуманітарний форум. 2025. Т.3. №2. С.77-85.
4. Grennan J., Michaely R. Artificial intelligence and high-skilled work: Evidence from analysts. Swiss Finance Institute Research Paper. 2020. № 20-84. URL: https://econpapers.repec.org/paper/chfrpseri/rp2084.htm.

Ящук Валентина Ігорівна

доцент кафедри управління інформаційною безпекою Львівського державного університет безпеки життєдіяльності, кандидат економічних наук, доцент

Рівняк Діана Ростиславівна

здобувач кафедри управління інформаційною безпекою Львівського державного університет безпеки життєдіяльності

СИСТЕМА ПРОАКТИВНОГО КІБЕРМОНІТОРИНГУ ДЛЯ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ: КОНЦЕПЦІЯ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Сучасний стан кібербезпеки органів сектору безпеки і оборони України характеризується високим рівнем динамічності та складності загроз, пов'язаних із трансформацією кіберпростору та активізацією гібридних форм протидії. Постійне зростання кількості кібератак, їх технологічна складність та цілеспрямований характер зумовлюють потребу у впровадженні проактивних механізмів виявлення та нейтралізації потенційних атак до моменту їхнього фактичного розгортання. Традиційні реактивні підходи, що зосереджуються на фіксації інцидентів постфактум, в умовах сучасної кіберзагрози вже не гарантують належного рівня стійкості та оперативності реагування. Натомість проактивний кібермоніторинг забезпечує можливість безперервного аналізу цифрових подій, виявлення аномалій та прогнозування потенційних кібератак, що створює передумови для своєчасного попередження порушень інформаційної безпеки.

В умовах воєнної агресії проти України значно зросла потреба у формуванні ефективної системи ситуаційної обізнаності, здатної інтегрувати інформацію з різних джерел — від внутрішніх телеметричних систем до зовнішніх потоків даних кіберрозвідки. Особливого значення набуває створення уніфікованої моделі обробки даних, яка дозволить органам сектору безпеки отримувати оперативну, точну та релевантну аналітичну

інформацію для ухвалення рішень. Проактивний кібермоніторинг передбачає широке застосування інтелектуальних технологій, зокрема машинного навчання, методів поведінкового аналізу та автоматизованих механізмів кореляції подій. Використання таких підходів сприяє мінімізації часу від виявлення індикаторів компрометації до локалізації та усунення загрози.

У цьому контексті актуальним є комплексне наукове дослідження, спрямоване на розроблення концепції системи проактивного кібермоніторингу, яка враховуватиме специфіку функціонування оборонного сектору України, обмеження ресурсів та високу інтенсивність зовнішніх впливів. Важливою складовою є також оцінювання викликів, пов'язаних з інтеграцією таких систем у наявну інфраструктуру, зокрема проблеми стандартизації, сумісності та захисту даних. Крім того, формування проактивної архітектури має розглядатися у контексті довгострокових перспектив розвитку національної системи кібербезпеки, включно з адаптацією до майбутніх технологічних ризиків. Таким чином, тема дослідження є як науково актуальною, так і практично спрямованою, оскільки її результати можуть бути використані підрозділами кіберзахисту та аналітичними центрами оборонного сектору України.

Концептуальна модель системи проактивного кібермоніторингу для органів сектору безпеки і оборони України ґрунтується на інтегрованій багаторівневій архітектурі, що забезпечує безперервний збір, кореляцію, поведінковий аналіз і прогнозування кіберподій з метою раннього виявлення загроз та підвищення рівня кіберстійкості інформаційних систем (рис.1). Центральним елементом моделі є підсистема збору кіберданих, яка забезпечує агрегування, нормалізацію та первинну структуризацію інформації з широкого спектра джерел, включаючи журнали мережевого трафіку, системи запобігання вторгненням, кінцеві пристрої, сервіси контролю доступу та зовнішні платформи кіберрозвідки. Отримані дані приводяться до уніфікованих форматів відповідно до стандартів STIX/TAXII чи CEF/LEEF, що дозволяє забезпечити їхню сумісність та підвищити якість подальшої аналітичної обробки.

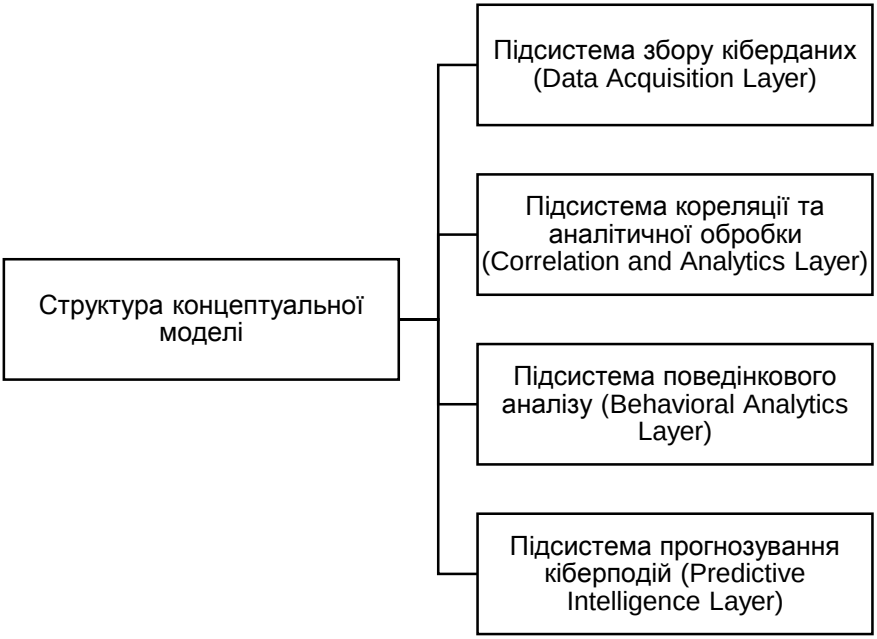

Рис. 1 Структура концептуальної моделі системи проактивного кібермоніторингу

Наступним рівнем концептуальної моделі виступає підсистема кореляції подій, яка здійснює логічне поєднання окремих інформаційних фрагментів у структуровані інциденти. Кореляція здійснюється за часовими ознаками, параметрами джерела та приймача подій, семантичними характеристиками, а також за критичністю активів, що дозволяє виявляти багатоступеневі сценарії атак, приховані залежності між подіями та TTP зловмисників відповідно до методології MITRE ATT&CK. Результатом цього етапу є формування зведених подій з підвищеною аналітичною цінністю, що створює підґрунтя для подальшого поведінкового аналізу.

Поведінковий аналіз у межах концептуальної моделі виконується у спеціалізованій підсистемі, яка застосовує методи User and Entity Behavior Analytics (UEBA), машинне навчання без учителя та алгоритми виявлення аномалій з метою ідентифікації нетипових і потенційно зловмисних дій користувачів, службових облікових записів, мережевих

вузлів або програмних компонентів. Завдяки прогнозуванню нормальних моделей поведінки система здатна виявляти аномальні патерни, що характерні для складних та малопомітних атак, зокрема lateral movement, несанкціонованого підвищення привілеїв чи прихованого витоку даних. Додатково поведінковий аналіз інтегрується з базами даних кіберзагроз та відомими техніками зловмисників, що підвищує точність визначення невідомих або Zero-Day атак.

Ключовою інноваційною складовою моделі є підсистема прогнозування кіберподій, що базується на методах статистичного аналізу та глибинного навчання. Вона дає змогу визначати ймовірність реалізації певних векторів атак, прогнозувати розвиток загроз у часовому вимірі, формувати сценарні моделі настання інцидентів та оцінювати потенційний вплив атак на критичні інформаційні активи. Використання моделей LSTM, GRU або графових нейронних мереж дозволяє системі здійснювати довгострокове та короткострокове прогнозування на підставі складних взаємозв'язків між подіями та поведінковими характеристиками системи. На основі прогнозів формуються рекомендації щодо превентивних заходів, оптимізується пріоритезація обробки інцидентів та підвищується загальний рівень ситуаційної обізнаності.

Таким чином, запропонована концептуальна модель формує цілісну методологічну основу для побудови проактивної системи кібермоніторингу, яка дозволяє перейти від реактивного реагування до випереджувального, забезпечуючи органи сектору безпеки і оборони України інструментарієм для раннього виявлення загроз, глибокого аналізу їхніх характеристик та прогнозування подальших дій зловмисників. Реалізація такої моделі сприятиме підвищенню кіберстійкості державних структур, зміцненню їхньої здатності протистояти сучасним та майбутнім кібератакам і забезпеченню захищеності критичних компонентів національної безпеки.

У результаті дослідження встановлено, що сучасні виклики у сфері кібербезпеки вимагають переходу до проактивних моделей кіберзахисту, які забезпечують раннє виявлення ознак потенційних атак та формують підґрунтя для оперативного реагування. Запропонована концептуальна

модель системи проактивного кібермоніторингу ґрунтується на інтеграції методів поведінкового аналізу, машинного навчання та кореляції подій, що значно підвищує ефективність обробки великих обсягів даних. Визначено низку викликів, серед яких — необхідність стандартизації інформаційних потоків, забезпечення інтероперабельності систем та підвищення рівня захисту чутливих даних. Перспективи розвитку системи пов'язуються з розширенням можливостей національних центрів ситуаційної обізнаності, інтеграцією з зовнішніми джерелами кіберрозвідки та вдосконаленням аналітичних алгоритмів. Реалізація запропонованих підходів сприятиме підвищенню кіберстійкості сектору безпеки і оборони України та посилить його здатність протистояти сучасним і майбутнім кіберзагрозам.

Література

1. Ящук В.І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами / Ящук В.І. // Scientific Collection «InterConf+», 45(201): with the Proceedings of the 8thInternational Scientific and Practical Conference «International Scientific Discussion: Problems, Tasks and Prospects» (May19-20, 2024; Brighton, United Kingdom)/ comp. by LLC SPC «InterConf».Brighton: A.C.M. Webb Publishing Co Ltd., 2024. 678p.(P.632-641).
2. Ящук В.І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави / В.І.Ящук // Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 364 (С. 259-286).
3. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). INTEGRATIVE APPROACH TO THE ANALYSIS, MODELING, AND ENSURING CYBER SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE UNDER MODERN THREATS. Baltic Journal of Economic Studies, 11(2), 273-286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286

4. Ящук В., Івануса А., Маслова Н., Ткачук Р., Брич Т. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки. Вісник ЛДУБЖД, № 31, 2025, 126-139. DOI: https://doi.org/10.32447/20784643.31.2025.13

Зміст

Наукове видання

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
26 грудня 2025 року

Опубліковано в авторській редакції

Формат 60×84/8. Умовн. друк арк. 9,3.
Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.
Свідоцтво про внесення суб'єкта видавничої справи до
Державного реєстру видавців, виготівників і розповсюджувачів
видавничої продукції ДК № 2541 від 26 червня 2006 р.

І 78 **ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ**: матеріали Науково-практичної конференції (Львів, 26 грудня 2025) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2025. 346 с.

У збірнику вміщено наукові статті за матеріалами доповідей учасників Науково-практичної конференції «Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України», що проводилася 26 грудня 2025 року у Львівському державному університеті внутрішніх справ.

УДК 004