УДК 342.95:351.746.1:004.8
https://doi.org/10.32703/2663-6352/2026-1-19-62-72
https://orcid.org/0000-0001-9563-6922
Тарасюк А. В.,
доктор юридичних наук, професор,
співробітник Служби безпеки України, полковник
м. Київ, Україна

ПРАВОВІ ТА СТРАТЕГІЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОПЕРАТИВНО-РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ПРОГНОЗУВАННІ ЯК ДЕТЕРМІНАНТИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Анотація. *У статті здійснено аналіз правових та стратегічних аспектів імплементації технологій штучного інтелекту в оперативно-розвідувальну діяльність Служби безпеки України. В умовах сьогодення, коли інтенсивність накопичення інформаційних ресурсів випереджає когнітивні можливості людського аналізу, автор обґрунтовує парадокс вразливості держави за відсутності алгоритмічних інструментів опрацювання даних. Зосереджуючись на статистичних показниках, зокрема на нейтралізації понад 14 000 кіберінцидентів, доведено, що превентивна функція спецслужб безпосередньо залежить від швидкості ідентифікації загроз.*

Окрему увагу приділено концептуалізації «оперативно-розшукового прогнозування» як еволюційного продовження традиційних методів наукового передбачення. Автор звертається до досвіду операції «Павутина», розглядаючи її як ілюстративний приклад складної діалектики між імовірнісним характером алгоритмічних висновків та фактичними підставами для процесуального втручання. Вбачається, що успіх подібних заходів зумовлений не тільки технічною перевагою, але й виваженим підходом до селекції сигналів у зашифрованих каналах зв'язку та цифрових слідах, що дозволяє трансформувати роботу підрозділів із реактивної на превентивну.

Наукова новизна публікації полягає у розробці авторського алгоритму інтеграції штучного інтелекту, що ґрунтується на принципі «human-in-the-loop» (людського контролю). Зокрема, запропонована модель функціонує як детермінований чотирьохетапний цикл, що бере свій початок від превентивного автоматизованого скринінгу аномальних поведінкових патернів і логічно завершується актом безпосередньої людської верифікації у поєднанні з процедурою так званого «негативного відбору» масивів даних.

Врешті-решт, у статті резюмується, що штучний інтелект має виступати виключно інтелектуальним орієнтиром, а не визначальним суб'єктом прийняття кінцевих процесуальних рішень. Обґрунтовано, що адаптація законодавства України до вимог цифрової епохи є фундаментальною детермінантою збереження національного суверенітету в умовах гібридної агресії. Безумовно, окреслений у роботі підхід створює наукове підґрунтя для подальшого вдосконалення законодавства, гармонізуючи безпекові потреби держави з європейськими стандартами забезпечення прав людини.

Ключові слова: *штучний інтелект; оперативно-розвідувальна діяльність; інформаційно-аналітичне прогнозування; оперативно-розшукова діяльність; національна безпека; Служба безпеки України; прогностична аналітика.*

TARASYUK A. LEGAL AND STRATEGIC ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN THE OPERATIONAL AND INTELLIGENCE ACTIVITIES OF THE SECURITY SERVICE OF UKRAINE AND IN INFORMATION AND ANALYTICAL FORECASTING AS DETERMINANTS OF NATIONAL SECURITY.

Abstract. *This article analyses the legal and strategic aspects of implementing artificial intelligence technologies in the operational and intelligence activities of the Security Service of Ukraine. In the current climate, where the rate of accumulation of information resources outstrips the cognitive capabilities of human analysis, the author highlights the paradox of state vulnerability in the absence of algorithmic data processing tools. Focusing on statistical indicators, in particular the neutralisation of over 14,000 cyber incidents, it is demonstrated that the preventive function of the special services directly depends on the speed of threat identification.*

Particular attention is paid to the conceptualisation of 'operational and investigative forecasting' as an evolutionary continuation of traditional methods of scientific prediction. The author draws on the experience of Operation «Spiderweb», considering it as an illustrative example of the complex dialectic between the probabilistic nature of algorithmic conclusions and the factual grounds for procedural intervention. It appears that the success of such measures is determined not only by technical superiority, but also by a balanced approach to signal selection in encrypted communication channels and digital traces, which allows the work of units to be transformed from reactive to preventive.

The scientific novelty of the publication lies in the development of an original algorithm for integrating artificial intelligence, based on the «human-in-the-loop» principle (human control). In particular, the proposed model functions as a deterministic four-stage cycle, beginning with preventive automated screening of anomalous behavioural patterns and logically concluding with direct human verification combined with a procedure of so-called «negative selection» of data sets.

Ultimately, the article concludes that artificial intelligence should serve solely as an intellectual guide, rather than as the decisive entity in making final procedural decisions. It is argued that the adaptation of Ukrainian legislation to the requirements of the digital age is a fundamental determinant of the preservation of national sovereignty in the context of hybrid aggression. Undoubtedly, the approach outlined in this work provides a scientific basis for the further improvement of legislation, harmonising the state's security needs with European standards for the protection of human rights.

Key words: *artificial intelligence; operational intelligence; information and analytical forecasting; operational investigation; national security; Security Service of Ukraine; predictive analytics.*

Вступ. Парадокс сучасної безпекової реальності полягає в тому, що, чим інтенсивніше держава накопичує інформаційні ресурси, тим вразливішою стає без належних інструментів їх опрацювання. В даному випадку штучний інтелект (далі – ШІ) є одним із визначальних чинників формування нової моделі оперативно-розвідувальної діяльності. За оцінками Європейської Комісії, понад 80% усіх даних у сфері безпеки залишаються неструктурованими та фактично не використовуються традиційними методами аналізу, що істотно знижує ефективність реагування на загрози [1]. Водночас, за даними Агентства з питань обслуговування систем інформації та зв'язку НАТО, впровадження алгоритмічних систем аналізу даних дає змогу скоротити час виявлення потенційних загроз щонайменше на 60%, що у воєнних умовах без перебільшення може визначати результат операцій [2].

В сьогоднішніх реаліях питання інформаційно-аналітичного прогнозування набуває якісно нового значення, оскільки, за даними Служби безпеки України (далі – СБУ), з початку повномасштабного вторгнення нейтралізовано понад 14000 кіберінцидентів та кібератак, значна частина з яких виявлялася із застосуванням автоматизованих систем аналізу трафіку та поведінкових моделей [3]. У низці випадків алгоритмічні рішення дозволяли виявити загрози ще до їх фактичної реалізації, зокрема під час протидії диверсійним групам, які координували свої дії через зашифровані канали зв'язку, що також підтверджує практичну ефективність аналітичного прогнозування у сфері державної безпеки.

Слід зазначити, що у відповідь на наростаючі загрози, слідчі СБУ нині розслідують понад 90 000 кримінальних проваджень, пов'язаних із воєнними злочинами, що становить щонайменше

85% усіх справ цієї категорії, відкритих правоохоронними органами України [4]. Очевидно, що такий масштаб діяльності потребує високого рівня організації процесуальної роботи, а також чіткої системи статистичного обліку та контролю. СБУ як орган досудового розслідування зосереджений на злочинах, що загрожують національній безпеці, у тому числі на воєнних злочинах, злочинах проти основ національної безпеки та злочинах, пов'язаних із тероризмом. За даними з відкритих джерел, у 2022 році за підслідністю до СБУ передано понад 44 800 кримінальних проваджень, з яких щонайменше 285 обвинувальних актів уже скеровано до суду, тоді як близько 9 500 справ на стадії досудового розслідування залишаються в процесуальному опрацюванні [5, с. 3].

Варто відмітити, що підготовка доказової бази, повідомлення про підозру та оформлення обвинувальних актів у межах СБУ має суттєві відмінності від практики інших органів досудового розслідування. На противагу цьому, міжнародний досвід, зокрема ЄС та держав-членів ЄС, обґрунтовує необхідність використання автоматизованих систем збору й обробки даних, а також аналітичних платформ для прогнозування потенційних загроз. Так, у Німеччині та Франції застосовуються методи статистичного аналізу і картування ризиків для пріоритизації проваджень, що забезпечує слідчим органам умови для раціональнішого розподілу ресурсів та оперативного доведення справ до суду [6, с. 1078].

СБУ активно співпрацює з прокуратурою та міжнародними партнерами, направляючи запити про правову допомогу та екстрадицію, що безпосередньо впливає на ефективність досудового розслідування і доведення проваджень до суду. За даними Офісу Генерального прокурора, у 2024 році було направлено понад 581 запит про правову допомогу, у тому числі 224 про екстрадицію [7].

Вбачається, що врахування статистичних показників підслідності, обсягів проваджень та практики доведення справ до суду є не тільки критерієм ефективності роботи СБУ, але й детермінантою національної безпеки. Звертаючись до окресленої проблематики, слід наголосити, що зростаюче навантаження на слідчі підрозділи вимагає вдосконалення методів аналітики та прогнозування ризиків, запозичуючи найкращі практики європейських держав, щонайменше в аспектах оптимізації обробки інформації та прискорення процесуальних дій.

До слова, за даними Організації економічного співробітництва та розвитку, глобальні інвестиції у технології ШІ в сфері безпеки перевищили 50 мільярдів доларів США у 2024 році, причому значна частина цих коштів спрямовується саме на розробку систем автоматизованого прогнозування ризиків та поведінкових моделей [8].

У цьому контексті Україна, декларуючи курс на європейську та євроатлантичну інтеграцію, вже поступово здійснює кроки у напрямі імплементації сучасних технологічних рішень, зокрема шляхом співпраці з Європейським Союзом у межах програм цифрової трансформації та кібербезпеки, зокрема – участь у ініціативі EU4Digital, яка передбачає розвиток аналітичних інструментів для державного сектору [9]. Безперечно, подібні проєкти створюють підґрунтя для подальшого впровадження ШІ у діяльність СБУ, проте, загострюють питання щодо їх законодавчого регулювання.

Метою статті є теоретичне обґрунтування та розробка практичних рекомендацій щодо використання алгоритмічних систем у діяльності СБУ як детермінанти зміцнення національної стійкості.

Матеріали та методи. Беручи до уваги складність об'єкта дослідження, матеріали та методи даної праці було обрано з огляду на потребу в поєднанні нормативно-правового аналізу та оцінки праксеологічних аспектів діяльності спецслужб. У відповідь на виклики цифрової епохи, емпіричну базу дослідження склали міжнародно-правові акти, спеціальне законодавство України, а також узагальнені результати практичної діяльності правоохоронних органів, що станом натепер перебувають у відкритому доступі.

Методологічна стратегія дослідження ґрунтується на засадах діалектичного підходу, що дало змогу розглянути еволюцію засобів і методів оперативно-розвідувальної діяльності як динамічний процес адаптації до гібридних загроз сьогодення. Системно-структурний метод став підґрунтям для аналізу інформаційної структури СБУ, де алгоритмічні системи розглядаються як детермінуючий елемент цілісної системи національної безпеки. Своєю чергою, застосування порівняльно-правового методу забезпечило можливість кореляції авторських пропозицій із західними правовими концептами, тоді як логіко-юридичний метод дозволив виявити та проаналізувати протиріччя між статичною природою правових норм і стрімким розвитком кібертехнологій.

Окремо варто зупинитися на використанні методу прогностичного моделювання, за допомогою якого було сформульовано авторський чотириетапний цикл інтеграції інтелектуальних систем, що дає можливість превентивно мінімізувати ризики суб'єктивізму в оперативній роботі.

Зрештою, слід вказати, що обрана автором методологія дозволила не тільки констатувати наявні правові проблеми, але й запропонувати алгоритм їх подолання.

Результати. Історично діяльність спеціальних служб ґрунтувалася на антропоцентричній моделі збору, оцінки та інтерпретації інформації, втім, сьогодні алгоритмічні системи все частіше виконують функції, які раніше були радше прерогативою аналітиків, зокрема щодо ідентифікації загроз, прогнозування можливих сценаріїв розвитку кризових ситуацій та визначення ймовірнісних моделей поведінки суб'єктів безпеки.

Насамперед слід звернутися до приписів Закону України «Про Службу безпеки України» від 25.03.1992 р. №2229-XII, який у ст. 2, 24 та 25 закріплює повноваження щодо здійснення контррозвідувальної діяльності, оперативно-розшукових заходів та інформаційно-аналітичного забезпечення [10], однак не містить спеціальних норм, що безпосередньо регламентують застосування алгоритмічних систем аналізу даних, залишаючи значний простір дискреції у частині визначення меж допустимості автоматизованих рішень. У цьому контексті, як наголошувалося у працях С. Албул, ефективність оперативно-розшукової діяльності значною мірою залежить від якості аналітичного опрацювання інформації [11, с. 10], однак автор виходив із традиційної парадигми людського інтелекту, що, безумовно, нині потребує переосмислення з огляду на технологічний фактор.

Сьогодні ж застосування ШІ в діяльності СБУ варто розглядати крізь призму Закону України «Про оперативно-розшукову діяльність» від 18.02.1992 р. №2135-XII, де у ст. 8 встановлений перелік оперативно-розшукових заходів, в тому числі збір інформації з відкритих і закритих джерел [12]. З наведеного фактично маємо підстави для використання технологій Big Data та машинного навчання, хоча прямого закріплення таких інструментів законодавець не передбачив. Відтак виникає питання щодо легітимності алгоритмічного втручання у приватну сферу особи, особливо у випадках, коли рішення приймаються без безпосереднього людського контролю.

Окремо варто зупинитися на ролі розвідки на основі відкритих джерел (англ. OSINT) у структурі інформаційно-аналітичного забезпечення, яка нині детермінує принципово нову якість оперативно-розшукового прогнозування. Сьогодні значний масив оперативно значущої інформації розміщений у публічному цифровому просторі – від соціальних мереж до супутникових знімків та реєстрів, а отже, використання методик OSINT є важливим з точки зору виявлення розвідувально-підривних загроз. Зокрема, імплементація інструментів OSINT дає змогу здійснювати первинну селекцію даних без безпосереднього втручання у приватну сферу особи на ранніх етапах, що повною мірою корелює з принципом пропорційності та верховенства права.

В даному випадку доречно апелювати до принципів оперативно-розшукової діяльності, закріплених у чинній редакції ст. 4 Закону, зокрема – верховенства права, законності та дотримання прав і свобод людини [12]. Якщо ж звернутися до положень відповідного законопроєкту №1229 від 02.09.2019 р., спостерігаємо істотне розширення цього переліку за рахунок принципів наступальності, конспіративності, поєднання гласних і негласних заходів, взаємодії з іншими суб'єктами, а також відповідності та адекватності застосованих заходів ступеню суспільної небезпечності [13]. І саме в цьому, більш широкому розумінні принципів оперативно-розшукової діяльності, простежується місце і межі використання сучасних аналітичних технологій.

Звертаючись до практичної площини, варто підкреслити, що визначення оперативно-розшукових заходів, закріплене у ст. 11 проєкту Закону, є наступним: «…передбачена чинним законодавством система дій, спрямованих на використання оперативно-розшукових засобів та методів, що здійснюють у межах своєї компетенції спеціально уповноважені підрозділи та їх службові особи, із метою вирішення конкретних завдань оперативно-розшукової діяльності та забезпечення кримінального судочинства» [13]. Отже, суб'єкт законодавчої ініціативи виходить із презумпції наявності факту для застосування таких заходів. В той же час, алгоритмічні системи, які використовуються для аналізу даних, працюють із імовірнісними моделями, що певною мірою зміщує акцент із факту на прогноз. У перспективі, можна констатувати, що алгоритмічний аналіз може формувати оперативний інтерес, а оперативно-розшукові заходи – підтвердити чи спростувати його.

Однак з огляду на вимоги закону, подібна взаємодія не може бути довільною. Суб'єкт оперативно-розшукової діяльності зобов'язаний діяти в межах приписів законодавства, які передбачають не тільки наявність обґрунтованих підстав, але й їх належну фіксацію. Як наслідок, використання результатів алгоритмічного аналізу як єдиного обґрунтування для застосування, наприклад, негласного проникнення чи контролю комунікацій, викликає обґрунтовані сумніви з точки зору дотримання принципів законності та пропорційності.

Також доречно звернутися до категорії оперативно-розшукового прогнозування, яка є формою інформаційно-аналітичної роботи в межах оперативно-розшукової діяльності, що полягає в організації процесу наукового передбачення розвитку подій на основі аналізу вже наявної оперативної інформації, а також узагальнення даних про минулі та актуальні тенденції [14, с. 56]. Фактично йдеться про інтелектуалізований етап оперативної діяльності, де результатом є не фіксація факту, а формування обґрунтованого припущення щодо можливих версій розвитку подій, що, безумовно, корелює із сучасними підходами до аналітики даних.

Разом із тим, у межах оперативно-розшукового прогнозування традиційно виділяють стратегічний та оперативно-тактичний рівні, кожен з яких має власне функціональне навантаження [14, с. 57-58]. Стратегічне прогнозування орієнтоване на моделювання загальних тенденцій розвитку оперативної обстановки – як у межах окремого регіону, так і на рівні держави чи навіть групи держав. Також формуються уявні моделі, що відображають ймовірність активізації організованих злочинних структур, у тому числі транснаціонального чи терористичного характеру, можливість появи нових каналів незаконного обігу зброї, наркотичних засобів чи інших заборонених предметів, а також потенційні зміни у міграційних потоках. Не менш значущим є аналіз впливу соціально-економічних, демографічних та інших факторів на криміногенну ситуацію, що дає змогу оцінити динаміку злочинності в контексті ширших суспільних процесів.

Своєю чергою, оперативно-тактичне прогнозування має більш прикладний характер і пов'язане з розробленням конкретних оперативно-розшукових версій розвитку подій. На цьому рівні відбувається трансформація аналітичних узагальнень у практичні рішення – визначення доцільності проведення тих чи інших заходів, уточнення напрямів оперативного супроводу,

зосередження ресурсів на найбільш ризикованих ділянках. Власне, окреслений рівень прогнозування найбільш наближений до повсякденної діяльності оперативних підрозділів, оскільки безпосередньо впливає на прийняття управлінських і процесуальних рішень.

З наведеного стає очевидним, що сама ідея використання алгоритмічних інструментів не є концептуально новою для оперативно-розшукової діяльності, а радше виступає еволюційним продовженням вже існуючого інституту прогнозування. Відмінність полягає лише у засобах: якщо раніше прогноз формувався переважно на основі професійного досвіду та обмежених аналітичних ресурсів, то сьогодні потенційно можливим є використання більш складних моделей обробки інформації. Але принципова вимога залишається незмінною – будь-який прогноз, незалежно від способу його формування, не може підміняти собою фактичні підстави для втручання у права особи, а має слугувати лише інтелектуальним орієнтиром для подальшої, процесуально врегульованої діяльності.

При цьому, фактична реалізація повноважень, про які йшлося вище, виходить за межі традиційного розуміння оперативно-розшукової діяльності як сукупності винятково агентурних чи технічних заходів. Скажімо, у реальній роботі підрозділів, які здійснюють оперативний супровід кримінальних проваджень щодо злочинів проти основ національної безпеки, первинний масив інформації може охоплювати тисячі контактів, десятки каналів комунікації, цифрові сліди, геолокаційні прив'язки, транзакційні операції. В ручному режимі встановити причинно-наслідкові зв'язки між такими елементами або надто складно, або взагалі неможливо, адже це виходить за межі людських когнітивних можливостей у часових рамках, відведених для реагування. В даному випадку ШІ може використовуватися як інструмент попередньої селекції інформації, ранжування ризиків та виявлення аномальних поведінкових патернів. Подібним чином, під час проведення негласних слідчих (розшукових) дій або оперативного супроводу кримінальних проваджень, алгоритмічні моделі дозволяють визначити, які саме контакти, переміщення або транзакції потребують подальшої перевірки.

Беручи до уваги об'єктивно великі обсяги інформації, які потребують опрацювання, без додаткового використання алгоритмічних систем оперативно-розшукова діяльність фактично втрачає свою превентивну функцію і перетворюється на реактивну. Іншими словами, оперативний підрозділ дізнається про подію вже після її настання – після вибуху, витоку інформації, фактичного контакту особи з структурами держави-агресора. До прикладу, при відпрацюванні осіб, які потенційно можуть бути залучені до розвідувально-підривної діяльності, обсяг комунікацій, переміщень і цифрових взаємодій настільки значний, що традиційний підхід – через ручний аналіз контактів, деталізацію з'єднань, зіставлення часових інтервалів – об'єктивно не дає можливості вчасно виявити ключові зв'язки.

Більш того, на практиці трапляються випадки, коли окремі сигнали – наприклад, нетипова активність у мережі, короткочасні контакти з різними абонентами, часті зміни геолокації – самі по собі не створюють достатніх підстав для реагування. Проте в сукупності вони можуть свідчити про підготовку до протиправної діяльності. Своєю чергою, без інструментів, здатних аналізувати подібні ознаки, ці сигнали залишаються розрізненими і не стають оперативно значущою інформацією. Відтак, потенційна загроза не ідентифікується на ранньому етапі.

Власне тут і виникає одна з найбільш дискусійних площин сучасної оперативно-розшукової діяльності: чи можна вважати достатньою підставою для ініціювання оперативно-розшукових заходів результат алгоритмічного аналізу? Чи є допустимим використання таких даних як орієнтиру для проведення негласних слідчих (розшукових) дій? І, зрештою, де проходить межа між допустимим інформаційним аналізом і втручанням у приватне життя особи, якщо сама підстава такого втручання має ймовірнісний, а не фактичний характер? Як видається, сам по собі алгоритмічний висновок не може підміняти передбачені законом підстави, однак

може використовуватися як первинний індикатор, який спонукає до подальшої перевірки процесуально визначеними засобами, про що вже наголошувалося раніше.

На цьому тлі важливим є питання контролю. Якщо законодавчо встановлені оперативно-розшукові заходи підлягають внутрішньому та судовому контролю, то алгоритмічні інструменти фактично залишаються поза його межами. Відтак доволі перспективний елемент прийняття рішень – аналітична модель – є найменш врегульованим з точки зору права.

У протилежному випадку, коли такі інструменти не застосовуються, оперативно-розшукова діяльність нерідко зводиться до реагування на вже встановлені факти або повідомлення ззовні – заяви громадян, інформацію інших органів, результати вже вчинених правопорушень. А тому, з практичної точки зору, найбільш виваженим підходом видається збереження за людиною виключної компетенції щодо прийняття кінцевих процесуальних рішень, тоді як ШІ виконує функцію допоміжного аналітичного інструменту. Тобто, алгоритм може підказати, але не має визначати.

Прикметно, що Закон України «Про захист персональних даних» від 01.06.2010 р. №2297-VI встановлює принципи обробки інформації, зокрема законності, пропорційності та цільового призначення [15], що прямо корелює з вимогами до систем ШІ, які здійснюють профілювання осіб, особливо в контексті ст. 8 Конвенції про захист прав людини і основоположних свобод [16]. Тут доцільно приділити увагу і принципу пропорційності, який за своїм змістовим навантаженням передбачає, що втручання у приватне життя має бути необхідним і співмірним поставленій меті. При здійсненні оперативно-розшукової діяльності окреслена вимога реалізується через наявність конкретних підстав і обмеження обсягу втручання. Проте алгоритмічні системи аналізують значно ширші масиви даних, ніж ті, що безпосередньо стосуються конкретної особи. Відповідно, в процесі профілювання можуть оброблятися дані осіб, які не мають жодного відношення до протиправної діяльності, але потрапляють у площину аналізу як частина інформаційного середовища. В даному випадку виникає питання, чи можна вважати таку обробку пропорційною, якщо вона потенційно стосується невизначеного кола осіб.

У цьому вимірі доречно звернути увагу на положення вищезгаданого Закону України «Про оперативно-розшукову діяльність», які конкретизують обов'язки суб'єктів оперативно-розшукової діяльності при роботі з інформацією, зокрема тією, що обробляється із застосуванням автоматизованих систем. Так, підрозділи, що використовують автоматизовані інформаційні системи в оперативно-розшуковій діяльності, зобов'язані забезпечити можливість надання відомостей про особу на запити органів досудового розслідування, прокуратури та суду, що фактично формує процесуальний міст між оперативною інформацією та доказовою базою кримінального провадження (ч. 11 ст. 9 Закону [12]). Одночасно законодавець висуває імперативні вимоги щодо забезпечення достовірності такої інформації та належного рівня її захисту в місцях зберігання, що при використанні складних аналітичних систем є особливо вагомим. Адже будь-яка зміна даних або порушення режиму їх збереження здатне не тільки нівелювати результати оперативної роботи, але й поставити під сумнів допустимість відповідних відомостей у подальшому судовому розгляді.

Більше того, Закон встановлює принципово важливе обмеження щодо обігу інформації, отриманої в ході оперативно-розшукової діяльності: відомості, що стосуються особистого життя, честі та гідності особи і не містять даних про вчинення протиправних діянь, не підлягають зберіганню та мають бути знищені (ч. 12 ст. 9 Закону [12]). У наведеному приписі фактично втілюється ідея «негативного відбору» інформації, коли держава зобов'язана знищувати дані за відсутності правових підстав для їх подальшого використання. У контексті застосування алгоритмічних систем це видається дещо складним, оскільки такі системи за своєю природою оперують значними масивами інформації, що можуть охоплювати в тому числі дані про осіб, не причетних до протиправної діяльності.

Окремо слід відзначити, що законодавець допускає більш тривале зберігання відомостей, пов'язаних із підготовкою або вчиненням терористичних актів, - до п'яти років. Відповідно, спостерігаємо диференційований підхід до інформації залежно від ступеня суспільної небезпечності відповідних діянь (ч. 12 ст. 9 Закону) [12].

Принцип цільового призначення, своєю чергою, вимагає, щоб персональні дані використовувалися виключно для конкретно визначеної мети. В оперативно-розшуковій діяльності такою метою є запобігання, виявлення та припинення кримінальних правопорушень. Однак застосування ШІ фактично розширює цю мету до прогнозування поведінки, виходячи тим самим за межі фіксації вже існуючих фактів.

Зосереджуючись на європейському досвіді, доцільно відзначити Регламент Європейського Союзу 2024/1689 («EU AI Act»), який запроваджує ризик-орієнтований підхід до використання ШІ, класифікуючи системи, що застосовуються у сфері правоохоронної діяльності, як такі, що належать до категорії високого ризику, з відповідними вимогами щодо прозорості, підзвітності та людського нагляду [17]. У відповідь на ці положення, Україна, декларуючи євроінтеграційний курс, вже імплементує окремі стандарти, зокрема через Концепцію розвитку штучного інтелекту в Україні, схвалену розпорядженням Кабінету Міністрів України від 02.12.2020 р. №1556-р [18], однак, вбачається, що цього недостатньо для повноцінного правового регулювання діяльності спецслужб.

Доволі цікаво, що у Сполучених Штатах Америки ще з початку 2010-х років функціонує система «Sentient», розроблена за участю Intelligence Advanced Research Projects Activity (Управління перспективних дослідницьких проєктів у сфері розвідки) і офіційно розсекречена у 2019 році, яка здійснює автоматизований аналіз супутникових зображень для виявлення аномальної активності, і, за відкритими даними, її застосування дозволило підвищити ефективність розвідувальних операцій на 30% [19]. У Великій Британії служба MI5 використовує алгоритмічні системи для обробки великих масивів комунікаційних даних, що, за інформацією парламентського комітету з питань розвідки та безпеки, сприяло попередженню щонайменше 12 терористичних актів лише за один рік [20].

Своєю чергою, у Німеччині Федеральна служба захисту конституції вже використовує системи аналізу великих масивів даних для виявлення радикалізації, при цьому діяльність зазначених систем суворо контролюється Федеральним уповноваженим із захисту даних [21]. Разом із тим, у Франції закон «Loi relative au renseignement» дозволяє застосування алгоритмів для виявлення терористичних загроз, однак передбачає обов'язковий контроль з боку Національної комісії з контролю за розвідувальною діяльністю [22].

Думається, вищенаведені приклади висвітлюють спільну для демократичних держав тенденцію: технологічне посилення розвідувальних та контррозвідувальних спроможностей невід'ємно супроводжується інституціоналізацією механізмів контролю, які покликані мінімізувати ризики свавільного втручання у права людини.

У вітчизняному контексті ілюстративним підтвердженням висловлених раніше тез є операція «Павутина» (2025 рік), аналіз якої дає змогу окреслити складну діалектику між традиційними методами ведення розвідки та новітніми аналітичними підходами. Коли ми говоримо про дешифрування багаторівневих мережевих структур противника, стає зрозуміло, що успіх подібних заходів безпосередньо корелює зі здатністю суб'єктів оперативно-розшукової діяльності опрацьовувати критичні обсяги розрізненої інформації.

Прикметно, що в межах «Павутини» простежувалася тенденція до пріоритетності виявлення нетипових кореляцій, які за своїм змістовим навантаженням могли б свідчити про підготовку до протиправних дій ще до моменту їх фактичної маніфестації [23]. Беручи до уваги складність сучасних гібридних загроз, вбачається, що саме інтелектуалізація процесу селекції

сигналів – від фінансових транзакцій до цифрових слідів у зашифрованих каналах зв'язку – виступає тією детермінантою, що дозволяє спецслужбі діяти превентивно.

Однак, сьогодні слід звернутися до питання правової регламентації таких процесів, адже аналогічно до європейської практики, будь-яка аналітична модель має слугувати виключно інтелектуальним орієнтиром, а не обґрунтованою підставою для втручання у приватну сферу особи. У відповідь на виклики, що постали під час операції «Павутина», дещо гостріше окреслилася потреба балансування між наступальністю оперативних підрозділів та принципом законності. Зрештою, використання результатів складного інформаційного моделювання, незалежно від ступеня їх автоматизації, безумовно потребує належного процесуального механізму контролю. Тим не менш, досвід «Павутини» лише підкреслює: за будь-яких умов кінцеве рішення та юридична відповідальність за ініціювання негласних заходів мають залишатися прерогативою людини, тоді як технологічні рішення є лише допоміжним інструментом у подоланні когнітивних обмежень аналітика.

Висновки. У світлі проведеного аналізу вбачається, що основними науковими здобутками є обґрунтування зміни оперативно-розвідувальної діяльності від реактивної моделі до превентивно-прогностичної. Встановлено, що в умовах сьогодення критичне накопичення інформаційних ресурсів без належних інструментів їх опрацювання стає детермінантою вразливості держави. Разом із тим, доведено неможливість повноцінного виявлення розгалужених злочинних мереж виключно антропоцентричними методами, оскільки обсяги цифрових слідів об'єктивно перевищують когнітивні можливості аналітика. Окремо варто зупинитися на тому, що правова природа алгоритмічного аналізу визначена не як заміна фактичних підстав для втручання у права особи, а як первинний індикатор для ініціювання процесуально врегульованих заходів. Безумовно, наукову новизну становить також адаптація принципів пропорційності та цільового призначення до умов функціонування систем із високим рівнем автономності, що також узгоджується з європейським вектором правового розвитку України.

Беручи до уваги потребу в чіткій регламентації, пропонується наступна послідовність дій («алгоритм непрямого сприяння»), що ґрунтується на збереженні за людиною виключної компетенції щодо прийняття юридично значущих рішень:

1. етап автоматизованої селекції та ранжування («Data Screening»): здійснюється постійний моніторинг великих масивів даних («Big Data») із відкритих та закритих джерел для виявлення аномальних поведінкових патернів. Система маркує об'єкти, чия активність (транзакції, переміщення, комунікаційні зв'язки) статистично відхиляється від норми;
2. формування прогностичної моделі загрози («Risk Profiling»): на основі виявлених аномалій алгоритм формує ймовірнісну модель розвитку подій (оперативно-тактичне прогнозування). На цьому етапі ШІ лише сигналізує про потенційний оперативний інтерес, не створюючи правових наслідків для особи;
3. верифікація та санкціонування («Human-in-the-loop»): отриманий аналітичний висновок передається уповноваженій особі (слідчому або оперативному співробітнику). Останній, апелюючи до власного досвіду та наявних фактичних даних, оцінює обґрунтованість припущення алгоритму. Тільки після людської верифікації приймається рішення про відкриття оперативно-розшукової справи або внесення відомостей до ЄРДР.
4. у разі, якщо в ході перевірки припущення ШІ не знайшло підтвердження, отримана інформація, що стосується особистого життя, підлягає негайному знищенню згідно з вимогами ст. 9 Закону України «Про оперативно-розшукову діяльність» [12]. У відповідь на підтверджені загрози дані використовуються для оптимізації негласних слідчих (розшукових) дій.

Зрештою, окреслений алгоритм дозволяє нівелювати ризики алгоритмічних систем, забезпечуючи при цьому високу ефективність протидії транснаціональним та терористичним загрозам, що без перебільшення є запорукою стійкості національної безпеки.

ЛІТЕРАТУРА

1. AI and Security Opportunities and Risks. Towards a trustworthy AI based on European values. PASAG report 3 – 2020 – AI and security. URL: https://share.google/5Ig7N558YSBWPDI7D
2. NATO Communications and Information Agency. URL: https://www.ncia.nato.int/
3. СБУ нейтралізувала понад 14 000 масштабних кібератак на Україну з початку повномасштабного вторгнення РФ. 27.01.2026. URL: https://www.ukrinform.ua/amp/rubric-society/4084571-sbu-nejtralizuvala-ponad-14-000-masstabnih-kiberatak-na-ukrainu-z-pocatku-povnomasstabnogo-vtorgnenna-rf.html
4. Слідчі СБУ розслідують понад 90 тисяч справ, пов'язаних із агресією Росії. 2025. URL: https://www.ukrinform.ua/amp/rubric-society/3990276-slidci-sbu-rozsliduut-ponad-90-tisac-sprav-povazanih-iz-agresieu-rosii.html
5. Звіт Національної поліції України про результати роботи у 2022 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf
6. Shyshenko A.A. Investigative actions in Ukraine, Germany and France: Comparative legal analysis of regulations and application practice. Аналітично-порівняльне правознавство. 2025. №2. С. 1076-1082. DOI: https://doi.org/10.24144/2788-6018.2025.02.160
7. Analysis of statistics from the Prosecutor General's Office. 2024. URL: https://vbpartners.ua/en/news-en/analysis-of-statistics-from-the-prosecutor-generals-office
8. Assessing potential future artificial intelligence risks, benefits and policy imperatives. OECD Artificial Intelligence Papers. №27. OECD Publishing. DOI: https://doi.org/10.1787/3f4e3dfb-en
9. ЄС для цифрової України. URL: https://eu4digitalua.eu/uk/
10. Про Службу безпеки України: Закон України від 25.03.1992 №2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12
11. Албул С.В. Оперативно-розшукова діяльність: сучасні доктринальні та праксеологічні концепти. Воєнний стан: теоретико-праксеологічні проблеми юриспруденції: колективна монографія. Lviv-Torun: Liha-Press. 2024. С. 1-24. DOI: https://doi.org/10.36059/978-966-397-421-7-1
12. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 №2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text
13. Проєкт Закону про оперативно-розшукову діяльність №1229 від 02.09.2019. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66597
14. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А.В. Мовчан. Львів: ЛьвДУВС, 2017. 244 с.
15. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
16. European Convention on Human Rights of 04.11.1950. URL: https://www.echr.coe.int/documents/d/echr/convention_ENG
17. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

18. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 №1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
19. Sentient Program. National Reconnaissance Office. 2019. URL: https://www.nro.gov/Portals/65/documents/foia/declass/ForAll/051719/F-2018-00108_C05113688.pdf
20. MI5. URL: https://en.wikipedia.org/wiki/MI5
21. Verfassungsschutzbericht 2023. Bundesamt für Verfassungsschutz. URL: https://surli.cc/iaetpz
22. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899
23. Операція «Павутина». URL: https://surli.cc/isoihp

Дата першого надходження рукопису до видання: 10.02.2026
Дата прийнятого до друку рукопису після рецензування: 27.03.2026
Дата публікації: 17.04.2026