ISSN 2524-0374

УДК 351.746.1:[343.985 + 004.8] (1-87)
DOI https://doi.org/10.32782/2524-0374/2025-11/36

ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ ПРОСТОРОВО-ЧАСОВОГО АНАЛІЗУ ТЕЛЕФОННОГО ТРАФІКУ ЯК МЕТОДУ ПОВЕДІНКОВОГО ПРОФІЛЮВАННЯ В РОЗВІДУВАЛЬНІЙ АНАЛІТИЦІ

FOREIGN EXPERIENCE IN USING SPATIOTEMPORAL ANALYSIS OF TELEPHONE TRAFFIC AS A METHOD OF BEHAVIORAL PROFILING IN INTELLIGENCE ANALYTICS

Ханькевич А.М., к.ю.н., професор,
ст. викладач кафедри теорії та практики інформаційної безпеки
Національний юридичний університет імені Ярослава Мудрого
orcid.org/0000-0002-6897-347X

Статтю присвячено дослідженню зарубіжного досвіду та методологічних засад застосування просторово-часового аналізу телефонного трафіку як методу поведінкового профілювання в розвідувальній аналітиці. Актуальність теми зумовлена тим, що в умовах гібридної війни та зростання загроз національній безпеці традиційні підходи до аналізу телефонних зв'язків є недостатньо ефективними. Зазначено, що оскільки традиційні підходи мають реактивний, а не превентивний характер, виникає гостра науково-практична потреба в обґрунтуванні застосування прогностичних методик.

Пояснюється концепція «поведінкового профілю», що формується шляхом побудови «базової матриці» звичних дій та подальшого виявлення аномальних відхилень від неї. Розкрито, як саме такі аномалії слугують високоточними розвідувальними індикаторами для виявлення прихованої протиправної діяльності.

Досліджено технологічні аспекти вдосконалення методології, зокрема через комплексне застосування аналізу соціальних мереж із алгоритмами машинного навчання для виявлення складних, неочевидних закономірностей у великих масивах даних.

Окреслено фундаментальну нормативно-правову проблему між превентивним збором даних у межах Закону України «Про контррозвідувальну діяльність» та процедурою їх подальшої легалізації як доказів у кримінальному провадженні згідно з Кримінальним процесуальним кодексом України. Встановлено, що ця процесуальна колізія поглиблюватиметься при використанні машинного навчання через складність судової верифікації логіки його алгоритмів.

Запропоновано шляхи вирішення колізії через адаптацію законодавства, а саме: впровадження механізму сертифікації відповідних аналітичних програмних комплексів як спеціальних технічних засобів та нормативне закріплення процедури використання їхніх автоматично згенерованих звітів як допустимих похідних електронних доказів, що підлягають подальшій експертній інтерпретації в межах слідства.

Ключові слова: розвідувальна аналітика, забезпечення державної безпеки, поведінкове профілювання, просторово-часовий аналіз, аналіз електронних комунікаційних даних, машинне навчання, допустимість доказів.

The article is dedicated to the study of international experience and the methodological foundations for applying spatio-temporal analysis of telephone traffic as a method of behavioral profiling in intelligence analytics. The relevance of the topic is conditioned by the fact that in the context of hybrid warfare and increasing threats to national security, traditional approaches to the analysis of telephone communications are insufficiently effective. It is noted that since traditional approaches are reactive rather than preventive, there is an acute scientific and practical need to substantiate the application of prognostic (predictive) methodologies.

The concept of a «behavioral profile» is explained, which is formed by constructing a «baseline matrix» of habitual actions and subsequently identifying anomalous deviations from it. It is revealed how such anomalies serve as high-precision intelligence indicators for detecting concealed illicit activities.

Technological aspects of improving the methodology are explored, particularly through the complex application of social network analysis with machine learning algorithms to identify complex, non-obvious patterns in large datasets.

A fundamental legal and regulatory problem is outlined concerning the conflict between preventive data collection under the Law of Ukraine «On Counterintelligence Activity» and the procedure for its subsequent legalization as evidence in criminal proceedings according to the Criminal Procedure Code of Ukraine. It is established that this procedural conflict will be exacerbated by the use of machine learning due to the difficulty of judicial verification of its algorithmic logic.

Pathways to resolve this conflict through legislative adaptation are proposed, namely: implementing a certification mechanism for the relevant analytical software systems as special technical means, and normatively securing the procedure for using their automatically generated reports as admissible derivative electronic evidence, subject to further expert interpretation within the investigation.

Key words: intelligence analytics, ensuring state security, behavioral profiling, spatio-temporal analysis, analysis of electronic communication data, machine learning, admissibility of evidence.

Вступ. В умовах повномасштабної збройної агресії та безпрецедентного зростання загроз національній безпеці України, вивчення передового зарубіжного досвіду в галузі розвідувальної аналітики набуває стратегічного значення. Противник активно використовує сучасні технології для ведення розвідувально-підривної діяльності, координації діяльністю агентурних мереж та актів підготовки диверсій. У цьому контексті електронні комунікаційні мережі залишаються не лише основним каналом зв'язку для громадян, але й критично важливим середовищем для обміну інформацією між учасниками протиправних формувань.

Традиційні підходи до аналізу телефонного трафіку, що здебільшого обмежуються констатацією факту з'єднання між абонентами, вже не відповідають складності сучасних викликів. Вони дозволяють лише реагувати на події, що вже відбулися, але є недостатньо ефективними для превентивного виявлення загроз, що зумовлює гостру науково-практичну потребу у переході від описового аналізу до прогностичного, до розробки та впровадження методології, здатної не просто фіксувати зв'язки, а моделювати поведінку об'єктів аналізу, виявляти приховані закономірності та прогнозувати їхні подальші дії.

Саме тому дослідження зарубіжного досвіду застосування просторово-часового аналізу як інструменту

поведінкового профілювання є надзвичайно актуальним. Розробка такої методології дозволить вітчизняним аналітичним підрозділам, що виконують завдання у сфері забезпечення державної безпеки, перейти на розуміння нового рівня розвідувальної аналітичної роботи: виявляти підготовку до протиправних дій на ранніх етапах через аналіз аномалій у сталих моделях поведінки, виявляти складні, ієрархічно організовані мережі осіб, причетних до протиправної діяльності.

Метою статті є вивчення та обґрунтування методологічних засад застосування просторово-часового аналізу як методу поведінкового профілювання в розвідувальній аналітиці, з урахуванням провідного зарубіжного досвіду.

Декларація щодо використання технологій штучного інтелекту. Відповідно до «Рекомендацій щодо відповідального використання штучного інтелекту в закладах вищої освіти» Міністерства освіти і науки України та Міністерства цифрової трансформації України (квітень 2025) та з урахуванням положень Концепції розвитку штучного інтелекту в Україні до 2030 року (Розпорядження КМУ від 02.12.2020 № 1556-р), декларую використання можливостей ШІ у процесі підготовки матеріалу наукової статті.

На етапі формування структурно-логічної побудови та первинного упорядкування тематичних блоків статті застосовувалася модель Gemini 2.5 Pro від Google для оптимізації процесу систематизації ключових проблемних аспектів. Роль ШІ обмежувалася технічною підтримкою організаційного етапу дослідження. Безпосередньо планування дослідження питань, змістовне наповнення статті, аналіз правозастосовної практики, критична оцінка доктринальних позицій, формулювання авторських висновків і пропозицій здійснювалися виключно дослідником. Усі текстові фрагменти, опрацьовані за допомогою ШІ, підлягали ретельній верифікації на предмет відповідності фаховим стандартам та специфіці правничої науки.

Автор дотримується принципів академічної доброчесності згідно зі статтею 42 Закону України «Про освіту» (№ 2145-VIII від 05.09.2017) та усвідомлює важливість прозорості у використанні сучасних технологій відповідно до Концепції розвитку штучного інтелекту в Україні до 2030 року.

Огляд зарубіжних досліджень та стану розробленості питання. Дослідження просторово-часового аналізу в контексті розвідувальної аналітики має виразну міждисциплінарну природу, поєднуючи комп'ютерні науки, когнітивну психологію, криміналістику та теорію безпеки. Аналіз зарубіжних наукових публікацій свідчить про глибоку розробку окремих методологічних компонентів.

Фундаментальною основою для сучасного аналізу розвідувальних даних вважаються праці М. Сперроу (M. Sparrow), який ще на початку 1990-х років оцінив перспективи застосування мережевого аналізу в кримінальній розвідці, водночас вказавши на обмеження його класичних, статичних форм. Саме ця дихотомія стала предметом подальших досліджень, зокрема у роботі Р. Томпсона (R. Thompson), який чітко артикулював концептуальну різницю між статичним («хто з ким пов'язаний») та динамічним («як, де і коли») аналізом.

Цей зсув парадигми знайшов відображення у прикладних дослідженнях , які обґрунтовують переваги поведінкового аналізу (Behavior Analysis) над традиційним аналізом зв'язків для проактивної оцінки загроз. Ключовою методологією в цьому напрямі став «Аналіз патернів життя» (Pattern-of-Life, далі – PoL), концептуальні засади якого описані в джерелах. Ця методологія фокусується на виявленні «базового рівня» нормальної активності суб'єкта, що є відправною точкою для подальшого пошуку аномалій.

Технологічна реалізація цього підходу стала можливою завдяки розвитку технології машинного навчання. Широкий пласт зарубіжних досліджень присвячений саме технічним аспектам:

– виявлення аномалій: праці Ф. Ванга (F. Wang) та ін. пропонують огляд методів глибокого навчання для виявлення аномалій у багатовимірних часових рядах;

– просторово-часовий аналіз: дослідження С. Ченга (X. Cheng) та ін. та Д. Чена (J. Chen) фокусуються на методах виявлення та інтерпретації просторово-часових аномалій у людській діяльності;

– прикладний аналіз: роботи М. Кумара (M. Kumar) та ін., М. Заври (M. A. Zawra) та ін. та М. Окті (M. Oktay) та ін. демонструють практичне застосування аналізу записів деталізації телефонних з'єднань для розслідування злочинів, мережевого аналізу та моделювання поведінки;

– аналіз соціальних мереж: праці К. Робертсон (C. Robertson) та ін. та К. Чжао (K. Zhao) та ін. розкривають потенціал аналізу соцмереж та інших новітніх методів для ідентифікації прихованих ролей та структур у мережах;

– загальні огляди ШІ: Н. Махмуд (N. H. Mahmood) та ін. та Е. Едозі (E. Edozie) та ін. надають системний огляд застосування машинного навчання для виявлення аномалій в електронних комунікаційних мережах.

Окремий важливий напрям досліджень становить інтеграція ШІ у сферу національної безпеки. Праці Б. Дженсена (B. Jensen) , М. Аріфа (Md Habibul Arif) та ін., М. Таддео (M. Taddeo) та ін. та Л. Векеси (L. W. Wekesa) аналізують як потенціал ШІ для оцінки ризиків та прогнозування загроз, так і фундаментальні проблеми, пов'язані з його використанням.

Таким чином, огляд зарубіжних джерел показує, що технологічна та методологічна база для поведінкового профілювання є потужною та активно розвивається. Однак, питання її практичної імплементації, зокрема інтеграції результатів автоматизованого аналізу у правове поле, залишається однією з ключових невирішених проблем, що й визначає актуальність нашого подальшого дослідження.

Виклад основного матеріалу. У традиційній практиці розвідувальної аналітики домінуючим методологічним підходом виступає «аналіз зв'язків», який характеризується переважно статичною природою. В його класичному застосуванні, зокрема під час моделювання діаграм за методологією опрацювання аналітичних даних «Anacapa», акцент робиться на візуалізації структурної організації мереж: ідентифікації суб'єктів взаємодії, характеру їхніх контактів та визначенні ключових фігур. Таким чином, даний метод зорієнтований на вирішення питання суб'єктної ідентифікації («Хто?») при дослідженні мережевих структур.

Однак, як зазначає М. Сперроу (M. Sparrow) у своєму фундаментальному дослідженні, застосування мережевого аналізу в кримінальній розвідці має суттєві обмеження [1]. Спрощена ідентифікація центральних акторів (наприклад, за кількістю зв'язків) часто призводить до тактики «нейтралізації ключових осіб». В ієрархічних та стійких злочинних або розвідувальних структурах нейтралізація такої фігури лише звільняє «кар'єрну сходинку» для наступника актора, не руйнуючи саму систему. Отже такий аналіз є реактивним – він констатує структуру, що вже склалася.

Сучасні виклики вимагають переходу до динамічного «аналізу поведінки», який, на відміну від статичного оцінює систему під час її роботи. Це становить фундаментальну методологічну парадигму: аналізується не просто наявність зв'язку (статичний код), а характер його використання у часі та просторі (виконання коду). Динамічний підхід дозволяє виявляти приховані, неочевидні закономірності та вразливості, які статичний аналіз не в змозі ідентифікувати [2].

Таким чином відбувається когнітивний зсув в аналітичній доктрині: від питань «Хто з ким пов'язаний?» до питань «Як, де і коли ця взаємодія відбувається?» і, зрештою, «Чому взаємодія відбувається саме так?». Як зазна-

чається у сучасних дослідженнях, аналіз зв'язків з'єднує точки даних, але саме аналіз поведінки дозволяє зрозуміти закономірності та сигналізувати про ризики [3]. Цей зсув має вирішальне значення, оскільки дозволяє аналітичним підрозділам перейти від нейтралізації структури (яка є стійкою і має тенденцію до самовідновлення) до дезорганізації функції – тобто зриву конкретної операції противника (конспіративної зустрічі, сеансу зв'язку, акту диверсії) ще на етапі її підготовки [4], що повною мірою реалізує превентивну функцію аналітичних підрозділів та є критично важливим в умовах гібридної війни.

Основою динамічного аналізу є створення «поведінкового профілю» об'єкта аналізу, який у західній розвідувальній доктрині відомий як «Pattern-of-Life Analysis (PoL)» (аналіз патернів життя – наше) [5], метою якого є детальне документування щоденних звичок та рутинної діяльності об'єкта для встановлення «базового рівня «нормальної» або повторюваної активності» [6]. Цей процес є формою розвідки на основі активності «Activity-Based Intelligence», що інтегрує дані з різноманітних джерел (у нашому випадку – записи про виклики та дані про місцезнаходження) для виявлення стійких просторово-часових кореляцій.

Технологічно це реалізується через побудову еталонної моделі поведінки, яку ще називають базовою матрицею «Baseline Behavior Model» [7]. Ця модель створюється на основі аналізу збережених телекомунікаційних даних за тривалий період і слугує точкою відліку, відносно якої вимірюються майбутні відхилення (аномалії).

Базова матриця формується трьома ключовими компонентами:

– комунікаційними патернами (стале коло контактів, типова частота з'єднань, тривалість та час комунікацій);

– часовими патернами (звичні періоди комунікаційної та фізичної активності/спокою (наприклад, «робочий час», «час сну»));

– просторовими патернами (типові географічні маршрути, регулярні локації («дім», «робота», місця регулярного відвідування) та швидкість переміщення між ними) [5].

Концепція створення базової матриці «звичної» поведінки об'єкта є відправною точкою для проведення розвідувального аналізу, який передбачає систематичний аналіз збережених даних об'єкта з метою встановлення повторюваних, передбачуваних патернів у його комунікаціях та переміщеннях. Цей процес дозволяє відповісти на такі питання:

– з ким об'єкт регулярно спілкується?

– в який час доби та дні тижня він є найбільш активним?

– яка типова тривалість його розмов?

– які його звичні маршрути пересування (наприклад, дім-робота)?

– які локації він відвідує регулярно?

Створення такого профілю перетворює величезний масив необроблених даних на структуровану «еталонну модель» життєдіяльності об'єкта.

Важливо підкреслити, що термін «еталонна модель» не повинен вводити в оману щодо її статичності – життя людини динамічне, і звична поведінка може змінюватися (зміна роботи, місця проживання, поява нових соціальних зв'язків). Жорстка, статична еталонна модель буде генерувати велику кількість хибних спрацьовувань, й тому сучасні методології передбачають механізми адаптивного оновлення еталонної моделі [7]. Це, у свою чергу, створює ключову аналітичну дилему для оперативника: як відрізнити доброякісну зміну патерну (наприклад, об'єкт почав відвідувати спортзал) від оперативно значущої (об'єкт почав відвідувати конспіративну квартиру)? Вирішення цієї дилеми полягає у встановленні кореляції між конкретною аномалією та іншими розвідувальними індикаторами. Це є головним завданням взаємодії аналітика (оперативника) з автоматизованою системою і водночас ядром розвідувальної методології, що розглядається.

Аномалія – це будь-яке суттєве відхилення від встановленої «базової матриці» поведінки особи. У контексті аналізу телефонного трафіку, ми маємо справу з багатовимірними даними (час, локація, абонент-А, абонент-Б, тривалість тощо), й тому технологічно задача вирішується методами виявлення аномалій у багатовимірних часових рядах («Multivariate Time Series Anomaly Detection» [8]. Такі аномалії можуть слугувати потужними індикаторами підготовки до протиправної діяльності, координації дій або зміни в оперативній обстановці.

Класифікація аномалій дозволяє структурувати процес пошуку розвідувальних індикаторів:

– *часові аномалії*: нетипова комунікаційна активність (наприклад, дзвінки у звичний «час сну»), зміна середньої тривалості або частоти сеансів зв'язку. Такі аномалії ефективно виявляються моделями прогнозування (Forecasting-Based Models), які, базуючись на історії телефонних з'єднань, передбачають очікувану поведінку, і сигналізують при розбіжності прогнозу з реальністю [8];

– *комунікаційні аномалії*: раптова поява нових стійких контактів, особливо якщо вони є «аномальними» для всієї групи, або різке припинення спілкування з усталеним колом осіб;

– *просторові аномалії*: відхилення від звичних маршрутів, відвідування нетипових локацій (особливо таких, що не мають очевидної соціальної чи комерційної інфраструктури), нехарактерно тривале перебування у транзитній зоні [9];

– *комбіновані просторово-часові аномалії*: це найцінніший тип індикаторів. Прикладом є регулярні короткі з'єднання або короткочасні появи об'єкта в одній і тій самій нетиповій локації у чітко визначений час (наприклад, кожна п'ятниця о 23:00) – класична ознака сеансу зв'язку або обслуговування схованки («закладки»).

Процес поведінкового профілювання перетворює роль аналітика (оперативника) з пасивного збирача даних на активного інтерпретатора та конструктора моделей. Аналітик/оперативник не просто знаходить «аномалії», – він будує наратив та психологічну модель об'єкта, щоб пояснити його поведінку та спрогнозувати майбутні дії. Однак цей інтерпретаційний процес несе в собі значний когнітивний ризик – упередження підтвердження. Формуючи гіпотезу щодо об’єкта (наприклад, «ця особа є агентом ворожої розвідки»), аналітик/оперативник ризикує підсвідомо тлумачити неоднозначні дані на користь власного початкового припущення. Так, серія обірваних дзвінків може бути тлумачена як витончена тактика протидії стеженню, а не просто як результат поганого покриття мережі. Це підкреслює критичну потребу у структурованих аналітичних методиках та процедурах «червоної команди» в розвідувальних підрозділах для оскарження припущень та запобігання появи «тунельного зору».

Наукова новизна та практична ефективність методології просторово-часового аналізу телефонного трафіку як методу поведінкового профілювання в розвідувальній аналітиці полягає у тому, що вибір математичного інструменту для виявлення аномалій має відповідати розвідувальній гіпотезі про тип поведінки, яку шукає аналітик/оперативник. Не існує єдиного «детектора аномалій». Дослідження у сфері просторово-часового аналізу пропонують диференційовані підходи [10]:

1. Статистичний контроль процесу (Multivariate SPC): ефективний для виявлення поодиноких, рідкісних аномалій.

2. Статистика сканування (Scan Statistics): оптимальна для виявлення кластеризованих аномалій.

3. Тензорне розкладання (Tensor Decomposition): найкраще підходить для ідентифікації прихованих циклічних патернів.

Таким чином, інтерпретація аномалії починається ще до її виявлення – з вибору аналітиком/оперативником (на основі його когнітивного досвіду та оперативної інформації) того математичного інструменту, який відповідає психологічній моделі очікуваної поведінки об'єкта аналізу.

Цей диференційований підхід систематизовано у таблиці «Матриця відповідності розвідувальних індикаторів та методів їх виявлення»:

Окреслена вище методологія поведінкового профілювання має пряме прикладне значення для вирішення конкретних аналітичних завдань у сфері забезпечення державної безпеки. Хоча кейси з практики спецслужб є переважно закритими, методологічна база є спільною для розвідувальної аналітики й кримінального аналізу, де вона широко висвітлена.

Основоположним набором даних для аналізу телефонного трафіку є записи деталізації дзвінків, або Call Detail Records (далі – CDR). CDR – це метадані, які генеруються та зберігаються операторами мобільного зв'язку для кожного комунікаційного сеансу в їхній мережі. Важливо підкреслити, що CDR зазвичай не містять змісту розмови чи повідомлення, а фіксують лише технічні параметри транзакції. Типовий CDR містить такі ключові поля даних:

– ідентифікатор абонента, що телефонує (номер мобільного телефону ініціатора дзвінка);

– ідентифікатор абонента, що приймає дзвінок (номер телефону отримувача дзвінка);

– час і дата початку телефонного з'єднання (точна часова мітка початку комунікації);

– тривалість з'єднання (час, протягом якого з'єднання було активним);

– тип послуги з'єднання (дзвінок, SMS, MMS, використання даних);

– ідентифікатори стільникових веж (Cell ID – ідентифікатори базових станцій, до яких були підключені телефони обох абонентів на початку та в кінці сеансу зв'язку). Це поле є критично важливим, оскільки воно надає просторовий вимір даним, дозволяючи відстежувати геолокацію та переміщення об'єктів.

Аналіз детального запису про виклик – CDR та даних геолокації активно використовується для розслідування та прогнозування злочинної діяльності [11]. Зокрема, просторово-часовий аналіз довів свою ефективність у моделюванні поведінки серійних злочинців (наприклад, визначення їхнього «якірного» місцезнаходження – дому чи роботи) [12] та у прогнозуванні «гарячих точок» (Hot Spots) майбутніх злочинів [13]. Ця ж логіка є повністю переносимою на завдання у сфері забезпечення державної безпеки. Аналіз телефонних даних також застосовується для картування та деструкції мереж наркотрафіку, які за своєю структурою та вимогами до конспірації є близькими аналогами агентурних мереж.

Розглянемо гіпотетичний, але методологічно обґрунтований кейс виявлення конспіративної зустрічі, який демонструє переваги динамічного аналізу поведінки над статичним аналізом зв'язків.

Кейс: «Комунікаційна чорна діра».

Об'єкти: Об'єкт №1 (співробітник українського підприємства критичної інфраструктури) та Об'єкт №2 (громадянин «А», що підозрюється у роботі на розвідку іноземної держави).

Конспірація: об'єкти дотримуються високого рівня конспірації і ніколи не здійснюють прямих дзвінків один одному.

Результат статичного аналізу: традиційний аналіз зв'язків (Link Analysis) не показує жодного контакту між двома об'єктами . Для нього вони невидимі як мережа.

Результат динамічного аналізу (PoL + Аномалії):

1. *Побудова PoL.* Для обох об'єктів побудовано «базові матриці». Система знає їхні звичні маршрути «дім-робота», типові години активності та звичні комунікаційні патерни (дзвінки родині, колегам тощо).

2. *Виявлення просторової аномалії.* Система фіксує, що в певний день Об'єкт №1 та Об'єкт №2 одночасно відхиляються від своїх звичних маршрутів і зближуються в одній нетиповій для них локації (наприклад, міський парк).

3. *Виявлення комунікаційної аномалії.* Система фіксує корельовану негативну аномалію: обидва об'єкти, які зазвичай демонструють певну фонову телефонну активність, повністю припиняють будь-які дзвінки та передачу даних за годину до і під час перебування у точці зближення (ймовірно, вимкнули телефони для унеможливлення пеленгації та перехоплення).

Інтерпретація. Система фіксує надпотужний комбінований індикатор: збіг у просторі (аномальне зближення) + корельована «комунікаційна чорна діра» (аномальна відсутність зв'язку). Отже, цей патерн, невидимий для статичного аналізу, є високо ймовірною ознакою проведення конспіративної зустрічі.

Тепер звернемо увагу на перспективи автоматизації та застосування розширених інструментів, серед яких особливе місце займає аналіз соціальних мереж (Social Network Analysis, далі – SNA) у просторово-часовому аналізі телефонного трафіку.

Аналіз соціальних мереж – це не просто візуалізація зв'язків, а потужний математичний інструмент для визначення пріоритетних цілей та виявлення прихованих ролей в мережі [14]. Застосовуючи метод аналізу до даних телефонного трафіку, SNA дозволяє ідентифікувати ключових фігур не за їхнім формальним статусом, а за їхньою мережевою функцією (активністю), що розраховується через метрики «центральності» (Centrality) [1]:

– *центральність за ступенем* (Degree Centrality): «Лідер» або «Хаб». Особа з найбільшою кількістю прямих контактів;

– *центральність за посередництвом* (Betweenness Centrality): «Посередник», «Брокер» або «Гейткіпер». Об'єкт, що знаходиться на найкоротших шляхах між іншими учасниками мережі, які не пов'язані напряму. Його нейтралізація призводить до фрагментації мережі;

Тип аномалії	Розвідувальний індикатор (приклад)	Опис патерну (гіпотеза)	Оптимальний метод виявлення
Просторова	«Маршрут розвідки місцевості»	Поодиноке, нетипове відхилення об'єктів від звичних маршрутів з відвідуванням критичної інфраструктури	Multivariate SPC
Комбінована (Простір-Час)	«Узгодження дій групою»	Одночасне (у часі) та/або збіжне (у просторі) аномальне переміщення або комунікаційна активність групи об'єктів	Scan Statistics
Комбінована (Простір-Час)	«Сеанс зв'язку» / «Закладка»	Регулярні, циклічні, короткочасні з'єднання або відвідування однієї нетипової локації у визначений час	Tensor Decomposition
Часова / Комунікаційна	«Підготовка до акції»	Будь-яке різке, неочікуване відхилення від багатовимірної «базової матриці» (часу, тривалості, локації)	MTSAD (на основі моделей прогнозування)

– *центральність за близькістю* (Closeness Centrality): «Ключовий комунікатор». Об'єкт, який може найшвидше поширити інформацію на всю мережу [15, с. 202–208].

Сучасні підходи до SNA виходять за межі простих метрик і використовують машинне навчання, зокрема Network Representation Learning (наприклад, алгоритми DeepWalk, Node2vec), що дозволяє перетворити складну структуру мережі у векторний простір і дає змогу автоматично кластеризувати мережу (виділяти окремі осередки) та виявляти ієрархічні лідерські структури [16].

Ключова ж перевага досягається при взаємодії SNA та PoL-аналізу. Ці інструменти не є взаємовиключними, вони збагачують один одного. SNA надає контекст, ідентифікуючи мережеву роль об'єкта (наприклад, «посередник» з високим показником «Betweenness Centrality» [1]. Ця роль, у свою чергу, калібрує «базову матрицю» поведінки. Наприклад, для «посередника» нормою є постійні короткі контакти з різними, не пов'язаними між собою гілками мережі. Відповідно, аномалією для нього буде не просто відхилення від маршруту (як для виконавця), а раптова зміна моделі комунікації: наприклад, припинення спілкування з однією гілкою мережі і фокусування на іншій. Таким чином, відбувається перехід від профілювання особи до профілювання мережевої функції, яку ця особа виконує.

Беручі до уваги вищевикладене, зазначимо, що обсяги даних телефонного трафіку унеможливлюють їх ефективну ручну обробку. Застосування машинного навчання (Machine Learning, далі – ML) та глибокого навчання (Deep Learning, далі – DL), зокрема рекурентних (Long Short-Term Memory, далі –LSTM) та згорткових нейронних мереж (Convolutional Neural Network, далі – CNN), є єдиним реалістичним шляхом для автоматизації виявлення аномалій у поведінці. Ці сучасні алгоритми здатні обробляти величезні багатовимірні потоки даних у реальному часі та виявляти складні, неочевидні відхилення, які людина не в змозі помітити [8; 17; 18; 19].

Наступним кроком є прогностичне моделювання. ML вже широко використовується для оцінки ризиків [20] та прогнозування загроз [21]. У сфері державної безпеки ML-моделі застосовуються для поведінкового моделювання з метою виявлення обману, оцінки довіри до джерел, прогнозування інсайдерських загроз та навіть терористичних атак [22].

Однак, головна цінність ML в розвідувальній аналітиці полягає не стільки в автоматизації пошуку відомих індикаторів (як у наведеній вище таблиці), скільки у викритті раніше невідомих. Аналіз, що базується на гіпотезі «Я шукаю циклічність для виявлення незвичайного», є, по суті, керованим аналізом. Натомість, некероване машинне навчання (Unsupervised ML) [17] не потребує початкової гіпотези – оскільки воно аналізує сукупні просторово-часово-комунікаційні дані мережі телефонних з'єднань і самостійно шукає будь-які статистично значущі закономірності.

Саме тут виявляються так звані «невідомі невідомі» (Unknown Unknowns). Наприклад, некерована ML-модель, проаналізувавши дані, що передували кільком диверсійним актам, може виявити складний, неочевидний для людини-аналітика патерн: «За 48 годин до диверсії Об'єкт «А» завжди на 30% збільшує тривалість дзвінків до «чистих» (не скомпрометованих) номерів, Об'єкт «Б» зменшує добову мобільність на 60%, а об'єкт «В» одноразово з'являється у локації «Х» о 03:00». Аналітик/оперативник тільки з маленькою долею ймовірності самостійно сформулював би таку складну комбіновану гіпотезу. Таким чином, ML-модель відкриває цей патерн як новий, надійний та неочевидний розвідувальний індикатор.

Отже, у попередньому тексті була обґрунтована теоретична та технологічна спроможність просторово-часового аналізу як методу профілювання для сфери державної безпеки, продемонстровано, як сучасні методи, зокрема SNA та машинне навчання, дозволяють автоматизувати виявлення неочевидних патернів у поведінці людини та навіть прогнозувати загрози.

Однак, сама по собі технічна можливість виявити розвідувальний індикатор не є тотожною його практичній користі для слідства. Впровадження таких потужних та глибоких методів аналізу, що безпосередньо втручаються у приватність комунікацій, неминуче стикається з фундаментальними питаннями законності. Ефективність просторово-часового аналізу телефонного трафіку як методу поведінкового профілювання в діяльності органів забезпечення безпеки в умовах правової держави визначається не лише його аналітичною потужністю, але й здатністю інтегрувати отримані результати у процесуальне поле, перетворивши їх на допустимі докази [23, с. 335–336]. Саме тому критично важливим є аналіз нормативно-правового забезпечення, який регулює цю діяльність.

Застосування описаної методології нерозривно пов'язане з суворим дотриманням правового режиму. Аналіз чинного законодавства виявляє фундаментальну подвійність та певні колізії у правовому регулюванні збору та використання електронних комунікаційних даних.

Наприклад, з одного боку, Закон України «Про контррозвідувальну діяльність» регулює спеціальний вид діяльності у сфері забезпечення державної безпеки, який, аналогічно до оперативно-розшукової діяльності, здійснюється переважно до початку досудового розслідування. Підставами для проведення контррозвідувальної діяльності є, зокрема, «наявність достатньої інформації, що потребує перевірки за допомогою спеціальних форм, методів і засобів» (п. 1 ч. 1. ст. 6) [24] Метою цієї діяльності є «попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України» та «припинення розвідувальних, терористичних та інших протиправних посягань» (ч. 1 ст. 2). Хоча науковці та практики зазначають, що матеріали контррозвідувальної діяльності... повною мірою відповідають вимогам, що висуваються ст. 99 Кримінального процесуального кодексу України (далі – КПК) [24] до документів і можуть використовуватись як докази у кримінальному провадженні, сам механізм їх легалізації залишається вкрай дискусійним. Ключова проблема полягає в тому, що порядок проведення контррозвідувальної діяльності не регулюється положеннями КПК, що створює ту саму процесуальну колізію, яка існує і для матеріалів оперативно-розшукової діяльності.

З іншого боку, КПК регулює діяльність в рамках зареєстрованого кримінального провадження, де збір інформації має на меті формування доказової бази.

Аналогічна правова колізія стосується і закону України «Про розвідку» – стаття 14 цього Закону [26] встановлює, що документи, які стосуються розвідувальної діяльності, не підлягають розголошенню та використанню для доведення фактів у кримінальному провадженні [27]. Водночас на практиці оперативні підрозділи, отримавши розвідувальну інформацію, намагаються легалізувати її через інструменти КПК. Таким чином, існує суттєва правова невизначеність щодо того, чи може інформація, зібрана превентивно в межах попередньої аналітичної роботи, бути легально трансформована у доказ в рамках КПК. У межах кримінального провадження КПК надає дві ключові можливості для отримання телекомунікаційних даних, які методологічно відповідають двом етапам профілювання:

1. Тимчасовий доступ до речей і документів (ст. 159–166 КПК) [24] – захід забезпечення, що застосовується для отримання збережених цифрових даних. Щодо нашої теми, це ухвала слідчого судді, яка зобов'язує оператора електронної комунікаційної мережі надати існуючі збережені дані за минулий період: лог-файли з'єднань,

CDR, дані білінгу та інформацію про місцезнаходження абонентів (збережені дані з базових станцій). Аналітичне значення цієї можливості полягає в тому, що вона є єдиним законним процесуальним способом отримання масиву даних, необхідних для побудови «базової матриці» поведінки (PoL-аналізу).

2. Зняття інформації з електронних комунікаційних мереж (ст. 263 КПК) – негласна слідча (розшукова) дія (далі – НС(Р)Д), що є різновидом втручання у приватне спілкування. Це проспективний захід[1], який полягає у «спостереженні, відборі та фіксації змісту інформації» та сигналів, що передаються каналами зв'язку в реальному часі. Аналітичне значення цього підходу зводиться до того, що він забезпечує динамічний моніторинг дій об'єктів оперативної уваги та виявлення аномалій у момент їх виникнення.

Аналіз цих норм виявляє суттєву процесуальну невизначеність: ст. 159 КПК дає нам «сирі» дані у вигляді архівних лог-файлів, а ст. 263 КПК – «сирі» дані поточного трафіку. Але, сам «поведінковий профіль» та «звіт про аномалію» є похідним аналітичним продуктом, створеним шляхом інтелектуальної або автоматизованої (ML) обробки цих «сирих» даних. Чинний КПК не містить чіткої процедури для долучення до матеріалів кримінального провадження саме цього аналітичного висновку, що призводить до того, що слідчі змушені долучати до матеріалів справи тисячі сторінок «сирих» лог-файлів, які суд фізично не в змозі осягнути, а сам аналітичний продукт, що викриває протиправну поведінку, залишається поза увагою або має лише статус допоміжного документа, але ж ніяк не процесуально значимого.

Ключова проблема легалізації – це допустимість доказів. Згідно зі ст. 86 КПК, доказ є допустимим, якщо він отриманий у порядку, встановленому Кодексом. Результати попереднього аналізу, зібрані до реєстрації провадження, часто визнаються недопустимими саме на цій підставі [26].

Для електронних доказів (якими є і «сирі» дані, і аналітичний продукт) критерії належності (підтвердження обставин справи) [23, с. 336] та допустимості (автентичності) є вирішальними. І саме тут виникають практичні бар'єри для легалізації таких аналітичних продуктів:

1. Проблема «Автора» доказу – судова практика вимагає можливості встановити суб'єкта, що застосував технічні засоби та отримав інформацію. В державних практичних органах таким суб'єктом може бути оперативний співробітник або співробітник оперативно-технічного підрозділу, допит якого в суді (для збереження конспірації та державної таємниці) є вкрай небажаним або неможливим.

2. Проблема «Технічного засобу» – необхідно правдиво вказати технічні характеристики засобу (програмного забезпечення), що використовувався для аналізу. Якщо приховати ці характеристики (наприклад, через державну таємницю), це може бути розцінено судом як спроба фальсифікації доказів [28, с. 120–121].

Застосування передових методів машинного навчання для виявлення неочевидних аномалій у поведінці об'єктів оперативної уваги під час проведення просторово-часового аналізу експоненційно погіршує цю проблему, створюючи те, що можна назвати «Проблемою Чорної Скриньки». Якщо аналіз робить людина, її (теоретично) можна допитати про логіку висновків. Але якщо аномалію виявила нейронна мережа або модель некерованого навчання, ми не можемо повною мірою пояснити, чому алгоритм прийняв те чи інше рішення. Хто є «автором» такого доказу? Яка його логіка? Суд, не маючи можливості перевірити логіку «чорної скриньки», з високою ймовірністю визнає такий доказ недопустимим, оскільки його походження є неперевірюваним.

Описана вище правова колізія, зокрема проблема легалізації доказів, отриманих за допомогою «чорної скриньки» машинного навчання, не є унікальною лише для України. Вона є частиною глобальної дискусії щодо впровадження штучного інтелекту у сферу забезпечення національної безпеки.

Зарубіжні експерти активно досліджують цю проблематику. Наприклад, М. Таддео (M. Taddeo) та ін. у своєму звіті детально аналізують «проблему передбачуваності» (The Predictability Problem) штучного інтелекту [21]. Суть проблеми полягає в тому, що багато потужних ML-моделей (зокрема, глибокі нейронні мережі) є за своєю природою непрозорими. Неможливість повною мірою пояснити, чому алгоритм дійшов того чи іншого висновку (наприклад, ідентифікував аномалію), створює фундаментальний бар'єр для їх використання у суді та у процесах прийняття критичних рішень, де вимагається підзвітність.

Ця технологічна проблема має прямі наслідки для правової системи. Б. Дженсен (B. Jensen), виступаючи щодо наслідків ШІ для національної безпеки, також підкреслює складність створення механізмів нагляду та контролю за такими технологіями [19]. Відтак, проблема, з якою стикається українська правова система – як інтегрувати докази, згенеровані ШІ, у кримінальний процес, – знаходиться в руслі одного з ключових викликів, що стоять перед західною розвідувальною та правовою думкою. Запропонований у цій статті підхід щодо сертифікації програмних комплексів як «спеціальних технічних засобів» [23, с. 336] є одним із можливих шляхів вирішення цієї глобальної проблеми, зміщуючи фокус доказування з логіки «чорної скриньки» на верифікацію та надійність сертифікованої системи «вхід-вихід».

Шлях вирішення цієї правової та технологічної колізії лежить у зміщенні фокусу доказування. Наукова література та судова практика вказують на важливий виняток: вимога про наявність автора не застосовується до електронних відображень, які автоматично генеруються інформаційною системою [23, с. 336].

Отже – замість того, щоб намагатися пояснити логіку «чорної скриньки» ML у суді, необхідно заздалегідь сертифікувати весь програмно-апаратний комплекс (який виконує PoL-аналіз та детекцію аномалій) як спеціальний технічний засіб, який використовується уповноваженими підрозділами (наприклад, спеціалізованими аналітичними). У такому випадку, процедура доказування в суді може бути структурована наступним чином:

1. Доказ-1 (вхід) – «сирі» електронні комунікаційні дані, отримані на підставі законної ухвали слідчого судді (ст. 159 або ст. 263 КПК).

2. Доказ-2 (обробка) – протокол, автоматично згенерований сертифікованою системою, що фіксує на кшталт: «На вхід подано [Доказ-1]. На виході системою виявлено [Аномалія Х]». Це вирішує проблему «автора», оскільки ним є сертифікована система [23].

3. Доказ-3 (інтерпретація) – висновок експерта (або свідчення аналітика/оперативника), який інтерпретує оперативне та криміналістичне значення «Аномалії Х» для конкретної ситуації (не пояснюючи, «ЯК» алгоритм її знайшов, а «ЩО» вона означає в контексті справи).

Такий підхід дозволяє вирішити правову колізію та «проблему чорної скриньки», надаючи суду надійний, верифікований (на рівні «вхід-вихід») та допустимий електронний доказ.

Підсумовуючи зазначене вище, можна стверджувати, що:

– просторово-часовий аналіз є потужним методом поведінкового профілювання для забезпечення потреб у сфері державної безпеки, який забезпечує необхідний методологічний зсув від статичного «аналізу зв'язків» до динамічного аналізу поведінки, що дозволяє виявляти не лише структуру мережі, але і її функціонування у просторі та часі, ідентифікуючи аномалії відносно «базових матриць» поведінки об'єктів;

[1] Проспективний захід – зорієнтований на отримання результатів, корисних у майбутньому.

– поєднання можливостей аналізу соціальних мереж з машинним навчанням дозволяє автоматизувати виявлення складних взаємозв'язків, профілювати мережеві функції об'єктів та відкривати раніше невідомі розвідувальні індикатори;

– головною перешкодою для впровадження методології є нормативно-правові виклики через існування процесуальної колізії між збором даних в межах аналітичної діяльності та їх легалізацією як доказів у кримінальному провадженні. Проблема поглиблюється складністю розкриття та верифікації логіки ML-алгоритмів, що ускладнює доведення допустимості результатів у суді. Вирішення цієї колізії лежить у площині адаптації законодавства, зокрема, через сертифікацію аналітичних комплексів як спеціальних технічних засобів та використання їхніх автоматично згенерованих звітів як допустимих похідних доказів, що підлягають подальшій експертній інтерпретації.

ЛІТЕРАТУРА

1. Sparrow M. K. The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks. 1991. Т. 13, № 3. С. 251–274. URL: https://doi.org/10.1016/0378-8733(91)90008-h (дата звернення: 01.08.2025).
2. Thompson R. Static VS. Dynamic Analysis. Medium. URL: https://medium.com/@thealltommo/static-vs-dynamic-analysis-b09a6d85e6d4 (дата звернення: 13.08.2025).
3. The Science of Threat Assessment: How Behavior Analysis Helps Prevent Incidents. Kaseware.com. URL: https://www.kaseware.com/post/the-science-of-threat-assessment-how-behavior-analysis-helps-prevent-incidents (дата звернення: 04.10.2025).
4. Behavioural Analysis in Transaction Monitoring: Boosting Fraud Detection Accuracy with AI Prospero AG. Prospero AG. URL: https://www.prospero.systems/insights/how-behavioural-analysis-enhances-transaction-monitoring (дата звернення: 04.10.2025).
5. Contributors to Wikimedia projects. Pattern-of-life analysis. Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Pattern-of-life_analysis (дата звернення: 13.08.2025).
6. Edwards S., Brignoni A. Forensic Pattern Of Life Analysis. forensicfocus.com. URL: https://www.forensicfocus.com/articles/forensic-pattern-of-life-analysis/ (дата звернення: 01.11.2025).
7. Perdices D., de Vergara J. E. L., Ramos J. Deep-FDA: Using Functional Data Analysis and Neural Networks to Characterize Network Services Time Series. IEEE Transactions on Network and Service Management. 2021. Т. 18, № 1. С. 986–999. URL: https://doi.org/10.1109/tnsm.2021.3053835 (дата звернення: 13.08.2025).
8. A Survey of Deep Anomaly Detection in Multivariate Time Series: Taxonomy, Applications, and Directions / F. Wang та ін. Sensors. 2025. Т. 25, № 1. С. 190. URL: https://doi.org/10.3390/s25010190 (дата звернення: 04.10.2025).
9. Multi-scale detection and interpretation of Spatio-Temporal Anomalies of human activities represented by time-series / X. Cheng та ін. Computers, Environment and Urban Systems. 2021. Т. 88. URL: https://doi.org/10.1016/j.compenvurbsys.2021.101627 (дата звернення: 01.11.2025).
10. Chen J. Anomaly Detection in Spatio-Temporal Data: Theory and Application. arXiv preprint arXiv. 2023. С. 46–50. URL: https://arxiv.org/pdf/2309.09878 (дата звернення: 13.08.2025).
11. Kumar M., Hanumanthappa M., Suresh Kumar T. V. Crime investigation and criminal network analysis using archive call detail records. Eighth International Conference on Advanced Computing. 2017. URL: https://api.semanticscholar.org/CorpusID:26760712 (дата звернення: 01.11.2025).
12. Zawra M. A., Emam O. E., Shehab M. E. A Survey of Call Detail Records (CDR) Analysis. International Journal of Computer Applications. 2023. Т. 185, № 13. С. 27–29. URL: https://doi.org/10.5120/ijca2023922808 (дата звернення: 13.08.2025).
13. A Systematic Review of Mobile Phone Data in Crime Applications: A Coherent Taxonomy Based on Data Types and Analysis Perspectives, Challenges, and Future Research Directions / M. Okmi та ін. Sensors. 2023. Т. 23, № 9. С. 43–50. URL: https://doi.org/10.3390/s23094350 (дата звернення: 01.11.2025).
14. Untangling SNA: The Use and Underuse of Social Network Analysis Among Crime Analysts / C. Robertson та ін. Police Practice and Research. 2025. С. 1–21. URL: https://doi.org/10.1080/15614263.2025.2574317 (дата звернення: 11.09.2025).
15. Засоби аналітичної розвідки. Основи роботи в i2 Analyst's Notebook : Навч.-практ. посіб. / А. Ханькевич та ін.; Вступне слово: В. Малюк, О. Користін. Харків: Ін-т Служби безпеки України Нац. юрид. ун-ту ім. Ярослава Мудрого, 2024. 306 с.
16. Social Network Forensics Analysis Model Based on Network Representation Learning / K. Zhao та ін. Entropy. 2024. Т. 26, № 7. URL: https://doi.org/10.3390/e26070579 (дата звернення: 04.10.2025).
17. Machine Learning for Network Anomaly Detection A Review / N. H. Mahmood та ін. The Indonesian Journal of Computer Science. 2025. Т. 14, № 1. URL: https://doi.org/10.33022/ijcs.v14i1.4703 (дата звернення: 05.10.2025).
18. Artificial intelligence advances in anomaly detection for telecom networks / E. Edozie та ін. Artificial Intelligence Review. 2025. Т. 58, № 4. URL: https://doi.org/10.1007/s10462-025-11108-x (дата звернення: 05.10.2025).
19. Center for Strategic & International Studies. Testify with Benjamin Jensen: Addressing the National Security Implications of AI, 2023. YouTube. URL: https://www.youtube.com/watch?v=d6LCWyZKS4w (дата звернення: 05.10.2025).
20. AI-Driven Risk Assessment in National Security Projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects / Md Habibul Arif та ін. Journal of Computer Science and Technology Studies. 2025. Т. 7, № 2. С. 71–85. URL: https://doi.org/10.32996/jcsts.2025.7.2.6 (дата звернення: 05.10.2025).
21. Artificial Intelligence for National Security: The Predictability Problem / M. Taddeo та ін. Oxford: Centre for Emerging Technology and Security, 2022. 62 с. URL: https://cetas.turing.ac.uk/sites/default/files/2022-09/research_report_ai_predictability_problem_vfinal_3.pdf. (дата звернення: 05.10.2025).
22. Wekesa L. W., Korir S. Enhancing intelligence source performance management through two-stage stochastic programming and machine learning techniques. Frontiers in Big Data. 2025. Т. 8. URL: https://doi.org/10.3389/fdata.2025.1640539 (дата звернення: 05.10.2025).
23. Гребенькова М. С. Належність і допустимість електронних відображень як джерел доказів у кримінальному провадженні. *Юридичний науковий електронний журнал.* 2021. № 12. С. 335–338. URL: https://doi.org/10.32782/2524-0374/2021-12/84 (дата звернення: 11.09.2025).
24. 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: 11.09.2025).
25. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374-IV : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text(дата звернення: 11.09.2025).
26. Про розвідку : Закон України від 17.09.2020 № 912-IX : станом на 30 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text(дата звернення: 11.09.2025).
27. Актуальні проблеми використання у кримінальному провадженні інформації, отриманої в результаті розвідувальної діяльності, та можливі шляхи їх вирішення. Верховний Суд. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1634649/ (дата звернення: 11.09.2025).
28. Галстян Г. Г. Проблемні аспекти використання оперативної техніки та інформації, отриманої у процесі її використання. *Науковий* вісник Херсонського державного університету. Серія *Юридичні науки*. 2018. Т. 2, № 1. С. 119–124. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/734125 (дата звернення: 11.09.2025).

Дата першого надходження рукопису до видання: 11.11.2025
Дата прийнятого до друку рукопису після рецензування: 11.12.2025
Дата публікації: 30.12.2025