УДК 004.056:316.472.4

І. О. Бондаренко
А. Р. Магденко

АНАЛІЗ СОЦІАЛЬНИХ ДЖЕРЕЛ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ СПІЛЬНОТ І ТРЕНДІВ

Вінницький національний технічний університет

Анотація

У тезах представлено комплексне дослідження методів аналізу соціальних мереж (Social Network Analysis, SNA) для виявлення прихованих спільнот і виявлення трендів. Розглянуто сучасні алгоритмічні підходи до детекції спільнот (структурні, стохастичні та методи оптимізації модульності), методи вивчення тимчасової динаміки мереж і алгоритми для виявлення трендів у текстових потоках соціальних платформ (методи тематичного моделювання, ембеддинги слів, трансформери та алгоритми виявлення аномалій). Проведено аналіз переваг і обмежень основних підходів, описано експериментальні сценарії для оцінки якості детекції (модульність, NMI, ARI) та підходи до синтезу даних і боротьби з шумом і ботами. Представлено результати порівняння класичних і сучасних алгоритмів (Girvan–Newman, Louvain/Leiden, спектральні методи, динамічні підходи) у контексті соціально-мовних даних, а також запропоновано методологію комбінованого підходу: графова детекція спільнот у поєднанні з семантичним кластеруванням (LDA/BERTopic/transformer-ембеддинги) для поліпшення виявлення "прихованих" спільнот і раннього виявлення трендів. Практична частина містить рекомендації щодо вибору інструментів, вимог до даних та процедур валідації для застосування в дослідженнях та прикладних системах моніторингу.

Ключові слова: аналіз соціальних мереж, детекція спільнот, модульність, Louvain, Leiden, Girvan–Newman, темпоральні мережі, тематичне моделювання, LDA, трансформери, тренди, виявлення аномалій, бот-активність.

Abstracts

The abstract presents a comprehensive study of social network analysis (SNA) methods for identifying hidden communities and detecting trends. It considers modern algorithmic approaches to community detection (structural, stochastic, and modularity optimization methods), methods for studying the temporal dynamics of networks, and algorithms for identifying trends in text streams on social platforms (methods of thematic modelling, word embeddings, transformers, and anomaly detection algorithms). The advantages and limitations of the main approaches are analyzed, experimental scenarios for assessing detection quality (modularity, NMI, ARI) and approaches to data synthesis and combating noise and bots are described. The results of a comparison of classical and modern algorithms (Girvan–Newman, Louvain/Leiden, spectral methods, dynamic approaches) in the context of social language data are presented, and a methodology for a combined approach is proposed: graph-based community detection combined with semantic clustering (LDA/BERTopic/transformer embeddings) to improve the detection of 'hidden' communities and early detection of trends. The practical part contains recommendations on the selection of tools, data requirements and validation procedures for use in research and applied monitoring systems.

Keywords: social network analysis, community detection, modularity, Louvain, Leiden, Girvan–Newman, temporal networks, topic modelling, LDA, transformers, trends, anomaly detection, bot activity.

Вступ

Соціальні мережі вже давно перестали бути просто засобом особистого спілкування – вони перетворилися на складні цифрові екосистеми, у яких формуються громадські наративи, координуються колективні дії, циркулюють інформаційні хвилі та навіть зароджуються організовані групи з прихованою структурою. У сучасному світі такі мережі відіграють вирішальну роль в обміні інформацією, політичних кампаніях, мобілізації громадян, маркетингових кампаніях і, на жаль, в поширенні дезінформації. Тому науковий інтерес до аналізу соціальних мереж (Social Network Analysis, SNA) є надзвичайно актуальним, оскільки цей підхід дає змогу не просто спостерігати за поверхневими взаємодіями, а проникати в глибшу структуру мережі – виявляти заховані спільноти, моделі координації, організовані групи, а також ранні ознаки нових соціальних трендів [1].

Особливо важливим цей напрямок стає в контексті інформаційної безпеки. Українські дослідники дедалі більше звертають увагу на те, як соціальні мережі використовуються для інформаційних впливів, кібер-війни та координації бот-мереж.

Паралельно класичні теорії теорії графів, такі як моделі «малого світу» або показники центральності (наприклад, центральність проміжності, централізація), дають математичну основу для розуміння топології соціальних мереж.

Разом із тим, зростання обсягів даних, темп появи нових постів, коментарів і взаємодій у соціальних медіа вимушує науковців застосовувати не лише класичні графові алгоритми, а й сучасні методи машинного навчання та обробки природної мови (NLP). Особливо перспективними є трансформерні моделі (наприклад, BERT та його варіанти), які дозволяють моделювати семантику повідомлень, виділяти приховані теми і кластеризувати контент за смисловим навантаженням. У поєднанні з алгоритмами детекції спільнот (наприклад, Louvain, Leiden) та методами динамічного аналізу мереж (temporal sliding windows, incremental updates) це дає змогу побудувати гібридні системи, здатні не просто виявляти структури, а й відслідковувати їх еволюцію та тенденції [1].

Це дослідження має на меті глибоко проаналізувати такі гібридні підходи до SNA – зосередитись на методах, що поєднують структурний аналіз, семантичні моделі та часову динаміку – з метою виявлення прихованих спільнот і трендів у соціальних мережах, а також оцінити переваги й обмеження таких підходів, виходячи з українського та міжнародного досвіду.

Результати дослідження

Методи аналізу соціальних мереж давно поділяються на кілька основних парадигм. З одного боку, є класичні підходи, засновані на теорії графів: вимірювання центральності, модульності, кластеризація за структурою, спектральні методи. Ці підходи дозволяють оцінювати, які вузли відіграють ключову роль (наприклад, вузли з високою проміжною центральністю, які часто виступають «мостами» між спільнотами), які групи користувачів утворюють щільні субмережі, і як побудувати карту взаємозв’язків.

З іншого боку, сучасні задачі виявлення прихованих спільнот вимагають врахування не лише структури, а й змісту: хто з ким взаємодіє – і про що вони говорять. Тут на сцену виходить машинне навчання, особливо методи NLP: тематичне моделювання (наприклад, LDA), ембеддинг-схеми, побудовані на трансформерах, кластеризація векторних представлень тексту. У поєднанні з графовими підходами це створює подвійний підхід, коли спершу виявляються структурні компоненти (спільноти), а потім в їхніх межах – тематичні підгрупи.

Також виокремлюють динамічні моделі мереж: оскільки соціальні мережі часто змінюються, спільноти можуть з’являтися, об’єднуватися, розпадатись. Тому алгоритми, які враховують часову компоненту – наприклад sliding window, incremental update, динамічний Leiden – є критично важливими. Вони дозволяють відслідковувати епохи активності, виявляти швидкі “вибухи” нових тем або нових спільнот, а також оцінювати сталість або плинність спільнот (community persistence, churn rate) [1].

Один із викликів при аналізі соціальних мереж – це наявність бот-мереж та програмних агентів, які можуть створювати ілюзію органічної активності, координації або навіть масовості певної ідеї. Українські дослідники запропонували цікавий підхід: використання великих мовних моделей (LLM) для побудови “детекторів” програмних ботів у соціальних мережах. Метод поєднує аналіз метаданих (наприклад, частота публікацій, час активності), графову структуру (як акаунти взаємодіють) та текстовий аналіз повідомлень із LLM, що значно підвищує точність виявлення ботів порівняно з традиційними методами [2].

Поєднання графового аналізу та семантичного кластерування

Гібридна методологія, яка складається з кількох кроків:

1. Збір та підготовка даних: дані соціальних мереж (наприклад, пости, коментарі, лайки, ретвіти, загальні взаємодії) збираються через API або веб-скрапінг з дотриманням етичних та правових норм. Важливо структурувати дані так, щоб побудувати граф взаємодій (з вершинами – акаунти, ребрами – взаємодії) та текстовий корпус (вміст повідомлень).

2. Побудова соціального графа**:** використовується підхід теорії графів. Граф може бути орієнтований або неорієнтований, залежно від природи взаємодій (наприклад, ретвіт як напрямок). Для побудови графа використовуються бібліотеки, такі як NetworkX, GraphX або Neo4j, що дають змогу масштабовано представити дані. Розраховуються структурні характеристики: ступінь вузлів, центральність (проміжна, близькості, власна), кластеризація, коефіцієнт кластеризації, середня довжина шляху, діаметр мережі, модульність тощо.

3. Первинна кластеризація спільнот: застосовуються алгоритми детекції спільнот, такі як Louvain або Leiden. Особливо цінним є Leiden, тому що він покращує якість кластеризації та забезпечує більш

стабільні спільноти, а також краще масштабується. Цей етап визначає великі компоненти мережі – потенційні спільноти – на основі структурної щільності зв'язків.

4. Семантичне кластерування в межах компонент**:** після виявлення структурних спільнот, всередині кожного кластеру виконується тематичний або семантичний аналіз тексту. Для цього використовуються два рівні підходів: (а) тематичне моделювання (наприклад, LDA) – корисне для виявлення основних тем у великих корпусах текстів; (б**)** ймовірні моделі на основі трансформерів (наприклад, BERT / Multilingual BERT / Ukrainian-BERT), які дають векторні ембеддинги повідомлень. Потім ці ембеддинги кластеризуються за допомогою алгоритмів, таких як HDBSCAN або k-means, для виявлення підтем або підгруп всередині спільнот.

5. Динамічний аналіз (часові аспекти)**:** щоб розуміти, як спільноти еволюціонують, ми використовуємо підхід sliding window або інкрементальні оновлення графу. З його допомогою можна простежити, коли спільноти з'являються, зливаються, розпадаються або змінюють свою структуру, а також виявити «вибухові» теми (burst detection) – раптові сплески активності в певній підтемі. Також вимірюються метрики темпоральної стабільності, такі як persistence (стійкість спільноти) та churn rate (ступінь змін складу), що дає можливість кількісно оцінити динаміку.

6. Ідентифікація бот-мереж і координованих кампаній**:** комбінуючи графові сигнали (щільність зв'язків, синхронність публікацій, швидкість відповіді, циклічні патерни) з мовними ознаками (із семантичного кластерування) та поведінковими ознаками (частота, час постів), застосовується класифікація (наприклад, Random Forest, SVM, нейронні мережі або навіть LLM) для виявлення ботів та координації. Це дозволяє визначити, чи є спільнота «органічною» групою реальних користувачів або ж це мережа ботів, які працюють координаційно для просування певних тем чи наративів.

7. Валідація та інтерпретація: результати кластеризації та класифікації верифікуються за допомогою метрик якості (модульність, NMI, ARI), а також через інтерв'ю, семплування або ручну експертизу (human-in-the-loop). Інтерпретація семантичних кластерів здійснюється шляхом аналізу ключових слів, representative повідомлень та часових шаблонів активності. Особливо важливо для наукової та практичної цінності – створення інтерпретованих (explainable) моделей, щоб аналізовані спільноти могли бути описані і пояснені аналітикам, політикам або операторам систем моніторингу [3].

Ще одним важливим напрямом дослідження в аналізі соціальних мереж є виявлення структурної неоднорідності мереж і формування багаторівневих моделей групової поведінки. Сучасні підходи дедалі частіше розглядають соціальну мережу не як однорідний граф взаємодій, а як сукупність накладених один на одного множин зв'язків, які можуть мати різну природу та різний рівень стабільності. Це дозволяє виявляти приховані шари комунікацій, які не завжди очевидні при класичному аналізі зв'язності. Наприклад, у деяких спільнотах сильні зв'язки можуть бути слабко відображені в комунікаційних даних, але активно проявляються у патернах взаємодій – часі реакцій, синхронізації активності, повторюваності тем. Такі підходи доповнюються методами моделювання потоків інформації всередині мережі. Дослідження останніх років показують, що навіть у великих соціальних мережах інформаційні хвилі поширюються не рівномірно, а мають властивість "фокусуватися" на ключових маршрутах – так званих інформаційних коридорах. Їх виявлення дозволяє прогнозувати, яким чином новий контент може стати вірусним та які групи найшвидше реагують на зміни у середовищі комунікацій. Виявлення таких коридорів базується на поєднанні метрик центральності, часових характеристик взаємодій та кластеризації за поведінковими особливостями користувачів.

Окремим напрямом, що набуває зростаючого значення, є аналіз "втручань" у мережеву структуру та моделювання впливу зовнішніх подій на формування трендів. Соціальні мережі все частіше розглядаються як складні адаптивні системи, де зовнішні чинники можуть різко змінювати патерни взаємодій. Наприклад, у періоди політичної турбулентності або кризових інформаційних ситуацій спостерігається різке зростання міжкластерної активності – тобто користувачі різних спільнот починають взаємодіяти інтенсивніше, ніж у нормальні періоди. Це, у свою чергу, впливає на формування нових структурних вузлів та трансформацію старих комунікативних груп. Такий режим високої турбулентності складно виявити за допомогою статичних моделей, проте аналіз динаміки графів та поведінкових кластерів дозволяє із високою точністю встановити причини та наслідки таких структурних зрушень.

Сучасні дослідження також відзначають важливість багатошарових графів (multilayer networks), де кожен шар відповідає певному типу взаємодій: дружби, коментарів, поширень, вподобань, участі у спільнотах, перетинів інтересів. Моделювання таких мереж дозволяє значно точніше виявляти приховані структури, адже не всі зв'язки мають однакову вагу або вплив на поведінку користувачів. У

багатьох випадках саме міжшарові зв'язки пояснюють формування трендів, які неможливо зрозуміти, якщо аналізувати лише один шар комунікацій [4].

Важливо також відзначити розвиток моделей прогнозування еволюції мережевих структур. Методи машинного навчання, включно з Long Short-Term Memory (LSTM) та Temporal Graph Networks (TGN), дають змогу не лише аналізувати поточний стан спільнот, а й моделювати їхню майбутню динаміку. Це критично важливо для визначення потенційних точок зародження нових трендів та оцінки ризиків, пов'язаних з інформаційними маніпуляціями або зміненими патернами поведінки бот-мереж. Важливо, що такі методи дозволяють виявляти "насіння трендів" – невеликі групи активних користувачів, чиї повідомлення з високою ймовірністю формуватимуть майбутні інформаційні хвилі. Їх ідентифікація суттєво підвищує ефективність моніторингу інформаційного середовища [5].

Практичні імплементації та інструменти

Для реалізації підходу рекомендується використовувати поширені та потужні інструменти:

– NetworkX або igraph (Python) – для побудови й аналізу соціального графа: розрахунок центральностей, модульності, кластеризація, візуалізація [6];

– Neo4j – для зберігання великого графу та виконання запитів, особливо коли дані великі, великовузлові [7];

– Hugging Face Transformers – для трансформерних моделей (BERT, Ukrainian-BERT чи мультимовні варіанти): отримання ембеддингів тексту [8];

– HDBSCAN – для кластеризації векторних представлень (ембеддингів), оскільки він добре працює з даними різного масштабу та щільності [9];

– Pandas, NumPy, scikit-learn – для обробки даних, класифікації, оцінки моделі (метрики)[10];

– для динамічного аналізу: власні скрипти або бібліотеки, які підтримують sliding window або incremental graph updates.

При цьому дуже важливо враховувати етичні й правові моменти: збір даних повинен здійснюватися з дотриманням правил платформи (API, правила конфіденційності), а також з урахуванням законодавства про захист персональних даних. У них також слід інтегрувати людський компонент у перевірку кластерів і інтерпретацію результатів, щоб уникнути помилкових висновків та спотворення реального соціального контексту.

Аналіз може перетворитися на інструмент для стеження, якщо не буде правильно регульований. Тому важливо встановити чіткі рамки: збір даних лише з публічних акаунтів або тих, для яких є дозвіл; анонімізація даних там, де це потрібно; прозорість процесу інтерпретації кластерів (експерти повинні розуміти, що саме означає "спільнота" у контексті). Крім того, з погляду інформаційної безпеки, аналіз може бути використаний для виявлення координації негативних або шкідливих кампаній – тому існує ризик зловживань. Українські науковці вже привертають увагу до цих аспектів: наприклад, вказують на необхідність створення моделей Explainable AI (пояснюваних моделей), щоб роз'яснювати, як система ідентифікує спільноти дезінформації або ботів [11].

Висновки

Аналіз соціальних мереж у сучасному вигляді є комплексним багаторівневим підходом, який поєднує методи теорії графів, машинного навчання, обробки природної мови, мультимодального аналізу та динамічного моделювання. Розширені концепції, такі як багатошарові мережі, тимчасові графи, поведінкові кластери, інформаційні коридори та динамічні ембеддінги, дозволяють значно глибше зрозуміти приховану структуру комунікацій та механізми формування трендів. Дослідження показують, що соціальні мережі є нелінійними адаптивними системами, де поєднання різних типів взаємодій створює складну багатовимірну архітектуру зв'язків, яка постійно змінюється під впливом зовнішніх та внутрішніх факторів.

Інтеграція мультимодальних даних, аналіз еволюції мережевих структур та прогнозування поведінки спільнот відкривають можливості не лише для виявлення прихованих груп, але й для глибшого розуміння того, як зароджуються та поширюються інформаційні тренди у цифровому середовищі. Розвиток сучасних інструментів – від динамічних графових нейромереж до спеціалізованих бібліотек для обробки великих та складних мереж – створює підґрунтя для високоточної аналітики, яка має значний потенціал у сферах безпеки, медіадосліджень, соціології, журналістики даних та державних комунікацій.

Водночас актуальним залишається етичний аспект збору та обробки даних, оскільки аналітика соціальних мереж часто включає чутливу інформацію. Тому розвиток цього напряму потребує не лише технічної досконалості, а й створення чітких норм відповідального використання алгоритмів та результатів дослідження. Загалом аналіз соціальних мереж є ключовим інструментом для розуміння

цифрових взаємодій і відіграє визначальну роль у дослідженні сучасного інформаційного простору, відкриваючи перспективи для подальших міждисциплінарних наукових розвідок.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Comparative Analysis of Community Detection Algorithms on the SNAP Social Circles Dataset. *arXiv.org e-Print archive*. URL: https://arxiv.org/html/2502.04341v1 (date of access: 20.11.2025).
2. Люшенко Л., Перегуда Я. СПОСІБ ПОБУДОВИ ПРОГРАМНИХ ДЕТЕКТОРІВ ДЛЯ ВИЯВЛЕННЯ ПРОГРАМНИХ БОТІВ В СОЦІАЛЬНИХ МЕРЕЖАХ. *Інформаційні технології та суспільство*. 2024. Т. 1, № 12. С. 56–64. URL: https://doi.org/10.32689/maup.it.2024.1.8.
3. Методи реалізації виявлення дезінформації у соціальних мережах на основі штучного інтелекту / М. Назаркевич та ін. *Кібербезпека: освіта, наука, технік*. 2025. Т. 2, № 30. С. 209–223. URL: https://doi.org/10.28925/2663-4023.2025.30.965.
4. Predicting popularity trend in social media networks with multi-layer temporal graph neural networks - Complex & Intelligent Systems. *SpringerLink*. URL: https://link.springer.com/article/10.1007/s40747-024-01402-6 (date of access: 21.11.2025).
5. Predicting Critical Nodes in Temporal Networks by Dynamic Graph Convolutional Networks. *MDPI*. URL: https://www.mdpi.com/2076-3417/13/12/7272 (date of access: 21.11.2025).
6. NetworkX – Python Library for Graph Analysis. URL: https://networkx.org/ ((date of access: 21.11.2025).
7. Neo4j – Graph Database Platform. URL: https://neo4j.com/ ((date of access: 23.11.2025).
8. Transformers Documentation – Hugging Face. URL: https://huggingface.co/docs/transformers/index ((date of access: 23.11.2025).
9. HDBSCAN: How HDBSCAN Works. URL:https://hdbscan.readthedocs.io/en/latest/how_hdbscan_works.html ((date of access: 24.11.2025).
10. NumPy vs Pandas vs Scikit-Learn: Key Differences Explained. URL: https://medium.com/@adityaranjan92/numpy-vs-pandas-vs-scikit-learn-key-differences-explained-9b04b0760dbe ((date of access: 24.11.2025).
11. IBM. What is Explainable AI (XAI)? | IBM. *IBM*. URL: https://www.ibm.com/think/topics/explainable-ai (date of access: 25.11.2025).

Магденко Анастасія Романівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anastasiiamahdenko@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна*** **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Mahdenko Anastasiia R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasiiamahdenko@gmail.com

Supervisor*:* ***Bondarenko Iryna O.*** **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua