КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

Кваліфікаційна наукова
праця на правах рукопису

ДМИТРІЄНКО КАТЕРИНА АНАТОЛІЇВНА

УДК 004.056.5:004.942

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ІДЕНТИФІКАЦІЇ КЛЮЧОВИХ ВУЗЛІВ У СОЦІАЛЬНИХ МЕРЕЖАХ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Спеціальність 125 Кібербезпека та захист інформації

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ К.А. Дмитрієнко

Науковий керівник:
КОРШУН Наталія Володимирівна
доктор технічних наук, професор

КИЇВ – 2025

АНОТАЦІЯ

Дмитрієнко К.А.. Моделі та методи ідентифікації ключових вузлів у соціальних мережах для забезпечення інформаційної безпеки держави. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації». – Київський столичний університет імені Бориса Грінченка, Київ, 2025.

У дисертації розв’язано актуальне наукове завдання, що полягає в розробці моделей і методів ідентифікації ключових вузлів у соціальних мережах з метою підвищення рівня інформаційної безпеки держави. Зважаючи на стрімкий розвиток цифрових технологій, соціальні мережі перетворилися з платформи особистої комунікації на глобальний інструмент масового впливу, що охоплює мільйони користувачів у реальному часі. Їх роль в сучасному інформаційному просторі полягає не лише в передачі повідомлень, а й у формуванні суспільної думки, зумовленій як природними механізмами взаємодії користувачів, так і алгоритмами персоналізованої видачі контенту.

Алгоритмічні стрічки новин, механізми рекомендацій, а також функції репостів і вподобань створюють сприятливі умови для стрімкого поширення як правдивої, так і хибної інформації. У поєднанні з психологічними ефектами, такими як емоційне зараження, ефект підтвердження або групового мислення, це створює високий ризик масових інформаційних викривлень.

У контексті гібридних загроз і триваючих інформаційних війн такі особливості функціонування соціальних платформ роблять їх надзвичайно вразливими до зловживань — для маніпуляцій громадською думкою, підриву

суспільної стабільності, а також здійснення цілеспрямованих кампаній дезінформації.

В роботі вперше запропоновано метод аналізу синхронізації інформаційних процесів у соціальних мережах на основі базової моделі Курамото з урахуванням індивідуальної сприйнятливості користувачів та сили зв'язків між ними, що дозволяє моделювати колективні ефекти інформаційної динаміки.

В роботі запропоновано комплексний підхід до аналізу поширення інформації в соціальних мережах на основі вдосконалених моделей Курамото. Базова модель Курамото, яка традиційно використовується для опису синхронізації в складних системах, була адаптована до умов інформаційних процесів у соціальних мережах шляхом інтеграції додаткових моделей:

– Каскадної моделі поширення інформації, що забезпечує можливість моделювання лавиноподібного передавання інформації в мережах при досягненні порогових значень активності вузлів;

– Епідемічної моделі, яка враховує перехід користувачів між станами: сприйнятливий, інфікований та відновлений, що дозволяє точно описувати динаміку поширення дезінформації;

– Моделі поширення чуток, що враховує етапи передачі, ігнорування та забуття інформації, а також її втрату актуальності з часом;

– Моделі впливових користувачів, що дозволяє ідентифікувати найбільш впливових користувачів, відповідальних за поширення інформації в мережі.

Завдяки поєднанню цих підходів удосконалена модель Курамото дозволяє не лише аналізувати динаміку поширення інформації, але й передбачати її вірусний ефект, визначати ключових поширювачів контенту, оцінювати стійкість інформаційної системи до маніпуляцій та дезінформаційних атак і планувати заходи протидії.

Практична частина дослідження передбачає моделювання процесів поширення інформації в соціальних мережах із використанням реальних

даних. Для цього розроблено програмне забезпечення, яке дозволяє візуалізувати інформаційні потоки, проводити чисельні експерименти та тестувати ефективність запропонованих підходів.

Набув подальшого розвитку метод ідентифікації ключових вузлів за рахунок інтеграції моделі Курамото та епідемічної моделі, що дозволяє виявляти вузли, найбільш схильні до ініціювання або підсилення дезінформаційних процесів. Запропонований підхід враховує як структурні характеристики мережі (центральність вузлів), так і динамічні аспекти інформаційного впливу, що виникає внаслідок взаємодії між користувачами. Завдяки цьому стало можливим не лише визначати джерела дезінформації, але й прогнозувати її подальше поширення та вплив на інформаційну стабільність у соціальному середовищі.

Також було розроблено метод для визначення ключових вузлів у соціальних мережах, заснований на вдосконаленій моделі Курамото з використанням методів аналізу впливових користувачів. Цей підхід дозволяє ідентифікувати вузли, що відіграють роль лідерів думок і здійснюють вирішальний вплив на формування та поширення інформаційних потоків у мережі.

Визначення таких користувачів дає змогу виявити основні канали ретрансляції інформації, критичні для управління інформаційним простором, що є актуальним для протидії дезінформації, планування інформаційних кампаній і підвищення ефективності цифрового впливу. Також знаходження таких користувачів є важливим для ефективного таргетування інформаційних кампаній, боротьби з дезінформацією та оптимізації цифрового маркетингу.

Для практичної реалізації моделей було розроблено програмний код, який наочно демонструє їхню роботу в контексті аналізу динаміки поширення інформації у соціальних мережах. Програмна реалізація дозволяє моделювати процеси синхронізації вузлів, візуалізувати структуру мережі та перебіг інформаційних процесів у вигляді графів, а також проводити чисельні експерименти за різних параметрів.

Для кожного з запропонованих методів – зокрема, методу виявлення ключових вузлів, схильних до поширення дезінформації, та методу визначення лідерів думок – було створено окремі програмні модулі. Ці модулі реалізовані таким чином, щоб забезпечити візуалізацію та аналітику результатів: ідентифікацію ключових вузлів, визначення сили зв'язків між ними та моделювання впливу окремих елементів на загальну інформаційну динаміку.

Особливістю реалізованого програмного забезпечення є здатність автоматично виділяти топ-5 найвпливовіших вузлів у мережі, які можуть виступати як ретранслятори дезінформації або як лідери думок. Це створює практичні інструменти для виявлення вразливих точок у мережі, планування превентивних заходів та оптимізації стратегій інформаційного впливу.

Результати дослідження можуть бути ефективно використані в таких галузях, як інформаційна безпека, кібербезпека, цифровий маркетинг, соціологія та державне управління. Запропонована методологія забезпечує можливість створення алгоритмів раннього виявлення дезінформації, розробки автоматизованих систем моніторингу соціальних мереж, а також впровадження інструментів інформаційного впливу і стратегій кризових комунікацій.

Практичне значення одержаних результатів полягає у здатності визначати найбільш впливові категорії контенту, що дозволяє підвищити залученість цільової аудиторії, а також оптимізувати стратегії поширення інформації в соціальних мережах і цифровому інформаційному просторі.

Окрему важливість результати мають у воєнних умовах, де інформаційна складова стала повноцінним елементом гібридної війни. Розроблені моделі дозволяють оперативно реагувати на інформаційні загрози, аналізувати поширення фейкових наративів, визначати їхні джерела та прогнозувати потенційний резонанс. Це створює передумови для ефективного інформаційного захисту, побудови стійкої цифрової комунікації та координації відповідей на зовнішні дестабілізаційні впливи.

Дисертація виконувалась в Київському столичному університеті імені Бориса Грінченка.

Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

Також результати наукових досліджень прийняті до впровадження в діяльність в діяльність Київського столичного університету імені Бориса Грінченка (акт від 14.02.2025 року), Інституту програмних систем Національної академії наук України (акт від 06.01.2025 року) та Національного центру управління та випробувань космічних засобів (акт від 12.05.2025 року).

Ключові слова: модель Курамото, поширення інформації, соціальні мережі, дезінформація, інформаційна безпека держави, ключові вузли, впливові користувачі, каскадна модель, епідемічна модель, модель поширення чуток, модель впливових користувачів, моделювання інформаційних процесів, графова модель, кібербезпека, соціальна інженерія, захист інформації, загрози, інформація, користувач, математичне моделювання**.**

ANNOTATION

Dmytriienko K.A. Models and methods for identifying key nodes of social networks to ensure the information security of the state. – A Qualification Research Paper Manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 125 "Cybersecurity and Information Protection". – Borys Grinchenko Kyiv Metropolitan University, Kyiv, 2025.

The dissertation addresses a current scientific challenge, namely the development of models and methods for identifying key nodes in social networks in order to enhance the level of national information security. Given the rapid advancement of digital technologies, social networks have evolved from platforms for personal communication into global tools of mass influence, encompassing millions of users in real time. Their role in the modern information space extends beyond message transmission to the shaping of public opinion, driven both by natural user interaction mechanisms and algorithmic content personalization.

Algorithmic news feeds, recommendation systems, as well as features like reposting and liking, create favorable conditions for the rapid dissemination of both accurate and false information. Combined with psychological effects such as emotional contagion, confirmation bias, or groupthink, this significantly increases the risk of widespread informational distortions.

In the context of hybrid threats and ongoing information warfare, such functional features of social media platforms make them highly vulnerable to misuse—for manipulating public opinion, undermining social stability, and conducting targeted disinformation campaigns.

This work introduces, for the first time, a method for analyzing the synchronization of informational processes in social networks based on the classical

Kuramoto model, taking into account users' individual susceptibility and the strength of connections between them. This enables the modeling of collective effects within information dynamics.

This study proposes a comprehensive approach to analyzing the spread of information in social networks based on improved Kuramoto models. The basic Kuramoto model, which is traditionally used to describe synchronization in complex systems, has been adapted to the context of informational processes in social networks through the integration of additional models:

— Cascade information diffusion model, which enables the modeling of avalanche-like transmission of information across the network when nodes reach certain activation thresholds;

— Epidemic model, which considers the transition of users between states such as susceptible, infected, and recovered, allowing for an accurate description of the dynamics of disinformation spread;

— Rumor-spreading model, which takes into account the phases of message transmission, neglect, and forgetting, as well as the loss of relevance over time;

— Influential user model, which allows the identification of the most influential users responsible for spreading information across the network.

By combining these approaches, the enhanced Kuramoto model makes it possible not only to analyze the dynamics of information dissemination but also to predict its viral effect, identify key content distributors, assess the resilience of the information system to manipulation and disinformation attacks, and plan countermeasures.

The practical part of the study involves modeling the processes of information dissemination in social networks using real data. To this end, dedicated software was developed, which enables the visualization of information flows, the conduction of numerical experiments, and the evaluation of the effectiveness of the proposed methods.

The method for identifying key nodes has been further developed through the integration of the Kuramoto model with the epidemic model, which makes it

possible to detect nodes that are most prone to initiating or amplifying disinformation processes. The proposed approach takes into account both the structural characteristics of the network (such as node centrality) and the dynamic aspects of information influence that arise from user interactions. This makes it possible not only to identify sources of disinformation but also to predict its further spread and impact on informational stability within the social environment.

In addition, a method has been developed for identifying key nodes in social networks based on the improved Kuramoto model and using influential user analysis techniques. This approach enables the identification of nodes that serve as opinion leaders and exert a decisive influence on the formation and propagation of information flows within the network.

The identification of such users makes it possible to determine the main information retransmission channels that are critical for managing the information space, which is especially relevant for combating disinformation, planning information campaigns, and increasing the effectiveness of digital influence. Furthermore, locating such users is essential for the effective targeting of information campaigns, disinformation counteraction, and optimization of digital marketing strategies.

For the practical implementation of the models, custom software code was developed to clearly demonstrate their operation in the context of analyzing the dynamics of information dissemination in social networks. The software enables simulation of node synchronization processes, visualization of the network structure and information flows in the form of graphs, as well as conducting numerical experiments under various parameter settings.

For each of the proposed methods—specifically, the method for detecting key nodes prone to spreading disinformation and the method for identifying opinion leaders—separate program modules were created. These modules are designed to provide both visualization and analytics of the results: identification of key nodes, assessment of the strength of connections between them, and modeling the influence of individual elements on the overall dynamics of information.

A distinctive feature of the developed software is its ability to automatically highlight the top 5 most influential nodes in the network, which may act either as retransmitters of disinformation or as opinion leaders. This provides practical tools for identifying vulnerable points in the network, planning preventive actions, and optimizing strategies for information influence.

The results of this research can be effectively applied in areas such as information security, cybersecurity, digital marketing, sociology, and public administration. The proposed methodology enables the development of algorithms for early detection of disinformation, the creation of automated systems for monitoring social networks, as well as the implementation of tools for information influence and crisis communication strategies.

The practical value of the obtained results lies in the ability to identify the most influential content categories, which helps increase audience engagement and optimize strategies for information dissemination in social networks and the broader digital information space.

These results are particularly important in wartime conditions, where the information domain has become a full-fledged component of hybrid warfare. The developed models enable prompt response to information threats, analysis of the spread of fake narratives, identification of their sources, and prediction of their potential resonance. This lays the groundwork for effective information protection, the development of resilient digital communication, and the coordination of responses to external destabilizing influences.

The results of the scientific research were applied at the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok, Faculty of Information Technology and Mathematics, Borys Grinchenko Kyiv Metropolitan University, within the framework of the research project: “Methods and Models for Ensuring Cybersecurity of Information Processing Systems and Functional Safety of Software and Hardware Complexes for Critical Infrastructure Management” (No. 0122U200483, KMUBG, Kyiv).

Additionally, the research findings have been officially adopted for implementation by Borys Grinchenko Kyiv Metropolitan University (statement dated February 14, 2025), the Institute of Software Systems of the National Academy of Sciences of Ukraine (statement dated January 6, 2025), and the The National Space Facilities Control and Test Center (statement dated May 12, 2025).

Keywords: Kuramoto model, information dissemination, social networks, disinformation, state information security, key nodes, influential users, cascade model, epidemic model, rumor spreading model, influential users model, information process modeling, graph model, cybersecurity, social engineering, information protection, threats, information, user, mathematical modeling.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. Дмитрієнко, К. А. (2023). Порівняльний аналіз моделей розповсюдження інформації в інтернет-середовищі. Кібербезпека: освіта, наука, техніка, 4(20), 272–282. DOI 10.28925/2663-4023.2023.20.272282

2. Дмитрієнко, К. А. (2023). Адаптація моделі Курамото для аналізу розповсюдження інформації в соціальних мережах. Кібербезпека: освіта, наука, техніка, 1(21), 309–314. DOI 10.28925/2663-4023.2023.21.309314

3. Дмитрієнко, К. А. (2024). Вдосконалення моделі Курамото для моделювання поширення інформації в соціальних мережах. Телекомунікаційні та інформаційні технології, 4(85), 16–28. DOI: 10.31673/2412-4338.2024.048612

4. Дмитрієнко, К., & Коршун, Н. (2025). Застосування вдосконалених моделей Курамото для ідентифікації дезінформації у соціальних мережах. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 406–416. https://doi.org/10.28925/2663-4023.2025.27.754

Наукові статті, опубліковані у періодичних наукових виданнях, проіндексовані у базі даних Scopus:

1. Ivanichenko, Y., Kozachok, V., Dreis, Y., Nesterova, O., & Dmytriienko, K. (2022). Exposing deviations in information processes using multifractal analysis. CEUR Workshop Proceedings, Vol-3187, 251–259

2. Dreis, Y., Ivanichenko, Y., Nesterova, O., Zhdanova, Y., & Dmytriienko, K. (2022). Restricted Information Identification Model. In Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2022), October 13, 2022, Kyiv, Ukraine (Vol. 3187, pp. 89–95). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-3187/

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DDOS	—	Distributed Denial of Service (Розподілена атака на відмову в обслуговуванні)
SIEM - система	—	Security Information and Event Management (Система управління інформацією та подіями безпеки)
SIER - модель	—	Susceptible-Exposed-Infectious-Recovered (Модель: Сприйнятливі — Вплив — Інфіковані — Вилікувані)
SIR - модель	—	Susceptible-Infectious-Recovered (Модель: Сприйнятливі — Інфіковані — Вилікувані)
TIP	—	Threat Intelligence Platforms (Платформа розвідки загроз)
ЗМІ	—	Засоби масової інформації
ПЗ	—	Програмне забезпечення

ВСТУП

Актуальність теми. Сучасний інформаційний простір характеризується стрімким зростанням обсягів даних, що циркулюють у соціальних мережах. Ці платформи відіграють важливу роль у процесах поширення інформації, впливу на громадську думку, формуванні суспільних настроїв та мобілізації аудиторії. Однак поряд із позитивними аспектами використання соціальних мереж існують і значні загрози, серед яких особливу небезпеку становлять дезінформація, фейкові новини та маніпулятивні інформаційні кампанії. В умовах гібридної війни та інформаційного протистояння дезінформація стала одним із ключових інструментів інформаційного впливу, що може дестабілізувати ситуацію в державі та суспільстві.

Одним із перспективних підходів до аналізу поширення інформації в соціальних мережах є використання математичних моделей, які дозволяють описувати динаміку інформаційних процесів. Зокрема, модель Курамото, яка традиційно застосовується для моделювання синхронізації в складних системах, може бути адаптована для аналізу інформаційних потоків у соціальних мережах. Покращені версії цієї моделі дозволяють враховувати не лише взаємодію між користувачами, а й особливості мережевої структури, динаміку поширення контенту та вплив окремих ключових вузлів на інформаційні процеси.

Актуальність дослідження зумовлена необхідністю розробки ефективних методів знаходження ключових вузлів для ідентифікації впливових користувачів у соціальних мережах, виявлення джерел дезінформації та моделювання процесів поширення інформації з метою забезпечення інформаційної безпеки держави. Використання покращених моделей Курамото дозволяє аналізувати структуру соціальних мереж, прогнозувати динаміку інформаційних кампаній та розробляти стратегії протидії інформаційним загрозам.

Зв'язок роботи з науковими програмами, планами, темами. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертація виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

Мета дослідження

Мета дисертаційного дослідження полягає в розробці та вдосконаленні моделей і методів ідентифікації ключових вузлів у соціальних мережах для забезпечення інформаційної безпеки держави на основі покращеної моделі Курамото

Відповідно до поставленої мети, для вирішення наукового завдання в роботі сформульовано та розв'язано такі часткові **завдання дослідження**:

1. Здійснено аналіз існуючих моделей розповсюдження інформації у соціальних мережах та виявлення їхніх обмежень у контексті інформаційної безпеки;

2. Виконано адаптацію покращених моделей Курамото: моделі із застосуванням каскадної моделі для моделювання процесів поширення інформації; моделі із застосуванням епідемічної моделі для врахування динаміки дезінформації; моделі із застосуванням моделі поширення чуток для аналізу механізмів поширення чуток; моделі із застосуванням моделі впливових користувачів для визначення лідерів думок;

3. Проведено оцінку ефективності вдосконаленої моделі Курамото порівняно з базовою моделлю за допомогою аналізу розповсюдження інформації та показника синхронізації та тестування удосконалених моделей на реальних даних;

4. На основі покращеної моделі Курамото із застосуванням епідемічної моделі розроблено метод ідентифікації ключових вузлів для знаходження дезінформації та розроблено програмний код у вигляді моделі графів;

5. На основі покращеної моделі Курамото із застосуванням моделі впливових користувачів створено метод для виявлення ключових вузлів для знаходження лідерів думок у соціальних мережах та розроблено програмну реалізацію на основі графової моделі для демонстрації результатів.

Об’єкт дослідження – процес ідентифікації ключових вузлів у соціальних мережах з метою підвищення рівня інформаційної безпеки держави.

Предметом дослідження є методи та моделі аналізу соціальних мереж для виявлення ключових вузлів, що впливають на поширення інформації.

Методи дослідження. Для проведення досліджень в дисертаційній роботі використовувалися методи математичного моделювання, теорії графів, чисельне моделювання, програмна реалізація, аналіз даних.

Наукова новизна одержаних результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей знаходження ключових вузлів в соціальних мережах:

1. Вперше запропоновано метод аналізу синхронізації інформаційних процесів у соціальних мережах на основі базової моделі Курамото з урахуванням індивідуальної сприйнятливості користувачів та сили зв’язків між ними, що дозволяє моделювати колективні ефекти інформаційної динаміки.

2. Вперше запропоновано поєднання моделі Курамото з каскадною моделлю поширення інформації, що забезпечує можливість моделювання лавиноподібного передавання інформації в мережах при досягненні порогових значень активності вузлів.

3. Набула подальшого розвитку модель Курамото за рахунок інтеграції епідемічного підходу для ля врахування переходу користувачів між станами:

сприйнятливий, інфікований та відновлений, що дозволяє точно описувати динаміку поширення дезінформації.

4. Удосконалено модель Курамото за рахунок застосування компонентів моделі поширення чуток, що враховують етапи передачі, ігнорування та забуття інформації, а також її втрату актуальності з часом.

5. Набула подальшого розвитку модель виявлення лідерів думок шляхом включення метрик центральності вузлів у модель Курамото, що дозволяє ідентифікувати найбільш впливових користувачів, відповідальних за поширення інформації в мережі.

6. Набув подальшого розвитку метод ідентифікації ключових вузлів за рахунок інтеграції моделі Курамото та епідемічної моделі, що дозволяє виявляти вузли, найбільш схильниі до ініціювання або підсилення дезінформаційних процесів.

7. Вперше запропоновано метод для визначення ключових вузлів у соціальних мережах, який заснований на вдосконаленій моделі Курамото з використанням методів аналізу впливових користувачів, що дозволяє ідентифікувати вузли, які відіграють роль лідерів думок та мають вирішальний вплив на поширення інформації в мережі.

Практичне значення одержаних результатів полягає в наступному, що результати дослідження можуть бути використані для розробки програмного забезпечення, яке допомагатиме органам державного управління, бізнесу та громадським організаціям у виявленні та нейтралізації загроз, пов’язаних із дезінформацією, управлінням інформаційними потоками та ідентифікацією впливових користувачів у соціальних мережах. Визначення ключових осіб дозволяє підвищити ефективність інформаційних кампаній, оптимізувати поширення критично важливої інформації та моніторити комунікаційні вузли для формування стратегій протидії загрозам інформаційної безпеки.

В умовах війни ці методи та моделі можуть бути застосовані для оперативного поширення інформації про евакуацію, гуманітарну допомогу, загрози безпеці та мобілізацію громадської підтримки.

Апробація результатів дисертації.

Основні теоретичні та практичні результати були представлені та обговорені в ході ряду наукових конференцій:

1. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II), 2021.
2. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2022.

Публікації. За результатами проведеного дисертаційного дослідження було опубліковано 6 наукових праць (з них 3 у співавторстві), а саме: 4 статті (з них 1 у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України, 2 статті (з них 2 у співавторстві) у періодичному науковому виданні, що входить до наукометричної бази Scopus. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачкою особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

У статті «Exposing Deviations in Information Processes using Multifractal Analysis», опублікованій у співавторстві, внесок Дмитрієнко К.А. полягає в адаптації методів виявлення аномалій у мережевому трафіку до задач інформаційної безпеки, зокрема — в обґрунтуванні застосування фрактального аналізу для ідентифікації відхилень у динаміці інформаційних процесів, що загалом склало близько 25% змісту статті. Також авторкою було виконано порівняльний аналіз результатів для різних типів користувацької

активності та запропоновано підхід до інтерпретації значень експоненти Герста з точки зору виявлення інформаційних атак.
У статті «Restricted Information Identification Model» внесок Дмитрієнко К. А. полягає у розробці структурної моделі класифікації типів інформації з обмеженим доступом. Зокрема, вона здійснила формалізацію ознак конфіденційної, службової та таємної інформації, що ґрунтується на результатах дисертаційного дослідження і становить близько 20% змісту статті.

У статті «Застосування вдосконалених моделей Курамото для ідентифікації дезінформації у соціальних мережах», опублікованій у співавторстві, внесок Дмитрієнко К.А. полягає в адаптації та впровадженні вдосконаленої моделі Курамото з урахуванням епідемічного підходу та центральності вузлів для ідентифікації джерел дезінформації та впливових поширювачів контенту. У межах дослідження авторкою було здійснено моделювання інформаційних процесів у соціальних мережах, формалізацію алгоритму визначення ключових вузлів та реалізацію програмного забезпечення для візуалізації динаміки поширення дезінформації, що загалом становить приблизно 85% змісту статті.

Структура та обсяг дисертаційного дослідження.

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 146 найменування на 12 сторінках та 12 додатків. Загальний обсяг роботи становить 221 сторінок серед яких 150 сторінок основного тексту, 19 рисунків, 2 таблиці, 10 кодів програм.

РОЗДІЛ 1
ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ З УРАХУВАННЯМ ВПЛИВУ СОЦІАЛЬНИХ МЕРЕЖ

1.1 Аналіз сучасних методів виявлення та запобіганням загрозам в інформаційній безпеці держави

У сучасних умовах розвитку інформаційного суспільства питання забезпечення інформаційної безпеки держави набуває особливої актуальності. Стрімке зростання обсягів інформаційних потоків, широке розповсюдження цифрових технологій та використання соціальних мереж як інструменту впливу зумовлюють появу нових типів загроз, що можуть серйозно вплинути на політичну, економічну та соціальну стабільність держави [14].

З метою систематизації та аналізу загроз, які виникають у сучасному інформаційному просторі, необхідно враховувати як положення чинного законодавства України, так і реальні виклики, що постають у контексті інформаційних воєн, кібератак та масового поширення дезінформації.

Також можна класифікувати інформаційні загрози, враховуючи як законодавчі норми України, так і актуальні реальні загрози.

1. Інформаційні загрози відповідно до законодавства України

Законодавство України визначає ряд інформаційних загроз, що можуть вплинути на національну безпеку та загальну стабільність країни. Основні акти, що регулюють питання інформаційної безпеки, включають Закон України «Про інформацію» [138], Закон України «Про основні засади забезпечення кібербезпеки України» [139], Закон України «Про захист інформації в інформаційно-комунікаційних системах» [135] та інші. Нижче в таблиці 1 наведені основні інформаційні загрози, які визначаються українським законодавством.

Таблиця 1. Основні інформаційні загрози, які визначаються українським законодавством

№ з/п	Основні інформаційні загрози	Суть загрози	Законодавча база
1	Несанкціонований доступ до інформаційних ресурсів	Несанкціонований доступ означає отримання доступу до інформаційних ресурсів без дозволу власника або адміністратора цих ресурсів. Це може призвести до витоку, зміни або знищення важливих даних.	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та інші акти зобов'язують забезпечувати надійний захист інформаційних ресурсів від несанкціонованого доступу [135].
2	Порушення цілісності, конфіденційності та доступності інформації	Загрози для цілісності, конфіденційності та доступності інформації можуть проявлятися у вигляді знищення, зміни або блокування доступу до інформації. Це стосується як державних інформаційних систем, так і приватних даних громадян та компаній	Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», усі інформаційні системи повинні забезпечувати конфіденційність, цілісність і доступність даних [135].
3	Кібератаки та кібертероризм	Кібератаки спрямовані на порушення функціонування інформаційних систем через застосування шкідливого програмного забезпечення або здійснення атак типу DDoS, з метою знищення або викрадення даних. Кібертероризм — це більш масштабні атаки, спрямовані на дестабілізацію роботи критичних інфраструктур.	Закон України «Про основні засади забезпечення кібербезпеки України» визначає заходи щодо боротьби з кіберзагрозами та терористичними діями у кіберпросторі [137].
4	Поширення дезінформації	Поширення неправдивої або маніпулятивної інформації з метою впливу на громадську думку, підриву довіри до державних органів або створення напруженості в суспільстві	Закон України «Про інформацію» передбачає відповідальність за поширення недостовірної інформації, особливо коли вона може призвести до шкоди національній безпеці або громадському порядку [136].
5	Витік державної таємниці та конфіденційної інформації	Це стосується несанкціонованого розголошення або викрадення державної таємниці, що може призвести до серйозної шкоди національній безпеці.	Закон України «Про державну таємницю» та інші нормативні акти регулюють порядок захисту інформації, що належить до державної таємниці, і визначають заходи

			відповідальності за її розголошення [134].
6	Шкідливе програмне забезпечення	Шкідливе програмне забезпечення може використовуватися для викрадення інформації, порушення роботи систем або контролю над ними.	Закон України «Про основні засади забезпечення кібербезпеки України» визначає загрози, пов'язані з використанням шкідливого ПЗ та заходи боротьби з ним [137].

2. Інформаційні загрози, актуальні в Україні

Окрім загроз, які визначаються законодавством, існують низка актуальних інформаційних загроз, що мають особливе значення в умовах нинішнього розвитку інформаційного суспільства, а також загострення геополітичних конфліктів. Деякі з цих загроз, не завжди повністю враховані в законодавстві, але такі, що мають реальний вплив на інформаційний простір, описано в таблиці 2.

Таблиця 2. Інформаційні загрози, які не визначені українським законодавством

№ з/п	Інформаційні загрози	Суть загрози	Приклад
1	Гібридна війна та інформаційні операції	Гібридна війна передбачає застосування різних методів, включаючи інформаційні операції для підриву державних інституцій та впливу на громадську думку. Це може включати як поширення фейкових новин, так і спрямовані атаки на інформаційні системи державних органів.	Російська агресія проти України супроводжується інформаційними атаками, спрямованими на дискредитацію уряду, розповсюдження панічних настроїв серед населення, а також підтримку проросійських наративів у медіапросторі [15], [137].
2	Фейкові новини та маніпулятивні медіакампанії	Фейкові новини та маніпулятивні медіакампанії націлені на спотворення реальної інформації з метою впливу на суспільство, зниження рівня довіри до уряду або стимулювання ворожих дій.	Масові кампанії дезінформації під час виборів або кризових ситуацій (наприклад, пандемії COVID-19, війна) викликають паніку та недовіру до офіційної інформації [137].
3	Соціальна інженерія	Соціальна інженерія — це маніпуляція людьми для отримання конфіденційної інформації або доступу до інформаційних систем. Атакуючі часто використовують техніки	Фішингові атаки, спрямовані на отримання конфіденційної інформації, можуть вплинути як на окремих осіб, так і на державні організації [76].

		обману для отримання паролів, доступу до даних або втручання в роботу систем.	
4	Кібератаки на критичну інфраструктуру	Атаки на критичну інфраструктуру, включаючи енергосистеми, транспортні мережі та державні організації, можуть призвести до серйозних економічних і соціальних наслідків.	Кібератаки на українську енергетичну інфраструктуру у 2015 році, коли було порушено роботу електромереж і значна частина населення залишилася без електроенергії [141].
5	Інтернет-шпигунство	Це стосується шпигунства, що здійснюється через інтернет із метою викрадення конфіденційних даних або промислової розвідки. Атаки можуть бути спрямовані на державні установи або приватні компанії.	Використання шкідливих програм для збору даних з урядових комп'ютерів, з метою отримання стратегічної інформації або промислових секретів [109].
6	Кібербулінг та хактивізм	Кібербулінг — це переслідування або залякування в інтернеті, тоді як хактивізм — це використання кіберзасобів для досягнення політичних або соціальних цілей.	Атаки хакерів на сайти урядових органів або кампанії проти окремих осіб або груп в соціальних мережах з метою дискредитації або залякування [55].

Україна стикається з різноманітними інформаційними загрозами, які регулюються законодавством, проте постійна еволюція кіберзагроз та інформаційних атак вимагає адаптації нормативної бази та впровадження нових підходів до забезпечення інформаційної безпеки. В умовах гібридної війни інформаційний простір стає ключовим полем бою, де кіберзасоби, дезінформація та маніпулятивні технології використовуються для дестабілізації країни.

Ефективне протистояння цим викликам потребує аналізу сучасних методів виявлення та запобігання загрозам, що дозволить розробити дієві механізми захисту інформаційного простору та забезпечити стійкість держави до інформаційних атак.

Аналіз сучасних методів виявлення та запобігання загрозам інформаційній безпеці є важливою частиною будь-якого дослідження в сфері захисту інформації, оскільки він дозволяє оцінити існуючі підходи, виявити їх обмеження і показати потребу в нових методах.

Методи виявлення загроз базуються на різних підходах і використовують різні технології:

1.Сигнатурний аналіз (Signature-based detection)

Сигнатурний аналіз є одним із найпоширеніших методів виявлення загроз. Він працює шляхом порівняння даних, таких як файли або мережеві пакети, із базою відомих сигнатур шкідливого програмного забезпечення. Основною перевагою цього методу є його ефективність у виявленні відомих загроз та висока швидкість аналізу. Проте цей підхід має значні обмеження: він не здатний виявляти нові або модифіковані загрози (наприклад, zero-day атаки) і вимагає постійного оновлення бази сигнатур.

Прикладом застосування сигнатурного аналізу є ESET NOD32 (Словаччина) [42], який використовує широку базу даних сигнатур для виявлення відомих вірусів і шкідливого програмного забезпечення. Також популярним продуктом є Avast (Чехія), що пропонує ефективний інструмент для захисту пристроїв завдяки великій базі сигнатур [8].

2. Метод на основі аномалій (Anomaly-based detection)

Базується на аналізі нормальної поведінки системи, де будь-яке відхилення від звичайних патернів розглядається як потенційна загроза. Основними перевагами цього методу є здатність виявляти нові, невідомі раніше загрози та адаптація до нових умов. Водночас метод часто генерує велику кількість хибнопозитивних результатів, що ускладнює його практичне використання.

Приклади реалізації цього методу включають Zeek (Bro) (США) — інструмент для аналізу мережевого трафіку на основі аномалій [119], а також Palo Alto Networks (США), що пропонує передові системи для виявлення вторгнень через аналіз поведінки [88]. Також, Cisco Stealthwatch (США) — система моніторингу мережевого трафіку для виявлення аномалій [27], IBM Watson Security (США) — платформа на основі штучного інтелекту для аналізу поведінкових загроз [57].

3. Метод на основі правил (Rule-based detection)

Передбачає використання набору заздалегідь визначених правил для виявлення загроз. Наприклад, можна налаштувати правила для аналізу підозрілого трафіку або дій користувачів. Основними перевагами є простота налаштування під конкретні сценарії та легкість використання. Однак метод неефективний для складних або непередбачуваних атак і має обмежений обсяг виявлення.

Прикладом такого підходу є Cisco Secure Firewall (США), який використовує правила для контролю трафіку та виявлення загроз [28], а також Check Point (Ізраїль), що пропонує потужний міжмережевий екран із можливістю гнучкого налаштування політик [21], Fortinet FortiGate (США) використовує методи на основі правил для ідентифікації загроз і обмеження доступу до небажаних ресурсів [44].

4. Інструменти машинного навчання (Machine Learning-based detection)

Дозволяють аналізувати великі обсяги даних для виявлення складних патернів і прихованих загроз, вони здатні самонавчатися на основі нових даних, що робить їх адаптивними до нових видів атак. Основними недоліками є високі вимоги до обчислювальних ресурсів та складність навчання моделей [17].

Прикладами є CrowdStrike Falcon (США), що використовує машинне навчання для аналізу загроз і розпізнавання складних патернів [32], а також Darktrace (Велика Британія), яка застосовує штучний інтелект для виявлення аномальної поведінки в мережах [35]. Інші прикладом може виступати CylancePROTECT (США) — антивірусний продукт на основі машинного навчання [66], Microsoft Defender for Endpoint (США) — рішення для захисту кінцевих точок із вбудованими алгоритмами ШІ [75].

5. Інтеграція з SIEM-системами (Security Information and Event Management)

Рішення дозволяє об’єднувати різні методи виявлення загроз, такі як сигнатурний аналіз і поведінковий моніторинг, забезпечуючи збір і аналіз

подій безпеки в реальному часі. Вони поєднують аналітику великих даних із можливістю виявлення аномалій. Основними перевагами є комплексний підхід, масштабованість і підтримка роботи в реальному часі. Однак впровадження SIEM-систем вимагає значних фінансових витрат і складного налаштування.

Серед прикладів можна виділити Splunk (США) — платформу для моніторингу подій безпеки, яка використовує різні методи для виявлення загроз [94], а також IBM QRadar (США), яка аналізує події безпеки та допомагає у виявленні загроз у реальному часі [58]. Також ArcSight (Micro Focus, США) — SIEM-система для централізованого управління безпекою [7], LogRhythm (США) — платформа для кореляції подій безпеки та автоматизації реагування на загрози [71].

Отже, сучасні методи виявлення загроз інформаційній безпеці мають як переваги, так і обмеження. Їх ефективне застосування залежить від інтеграції різних підходів, таких як сигнатурний аналіз, аналіз аномалій, правила та машинне навчання. Додавання SIEM-систем підвищує рівень моніторингу та виявлення, що забезпечує комплексний захист. Використання сучасного та дозволеного в Україні програмного забезпечення, такого як ESET, Cisco, CrowdStrike та інших, сприяє побудові надійної системи безпеки для захисту даних та інформаційних систем.

Сучасні **методи запобігання загрозам** спрямовані на зниження ймовірності успішної атаки або мінімізацію її впливу. Вони охоплюють широкий спектр підходів, які забезпечують комплексний захист інформаційних систем. Поділяються на:

1. Системи захисту кінцевих точок (Endpoint Protection) забезпечують безпеку робочих станцій, серверів і мобільних пристроїв за допомогою антивірусних програм, міжмережевих екранів (файрволів) і систем виявлення та запобігання вторгненням (IDS/IPS). Вони є ключовими компонентами захисту інфраструктури організації від потенційних атак. Прикладом є ESET Endpoint Security (Словаччина), який забезпечує проактивний захист від

шкідливого програмного забезпечення та фішингових атак [42]. Ще одним прикладом є Sophos Endpoint Protection (Велика Британія), що ефективно захищає кінцеві пристрої від загроз завдяки комплексному моніторингу та поведінковому аналізу [100]. Основною перевагою таких систем є їхня здатність забезпечувати захист у реальному часі, проте вони можуть потребувати значних обчислювальних ресурсів та складного налаштування для великих корпоративних мереж.

2. Міжмережеві екрани та шлюзи (Firewalls and Gateways) контролюють трафік між внутрішньою мережею організації та зовнішнім інтернетом, блокуючи небажані або підозрілі з'єднання. Вони є основним інструментом для захисту від несанкціонованого доступу та мережевих атак. Таким продуктом є Fortinet (США), який пропонує міжмережеві екрани з вбудованими функціями виявлення загроз [44], та Cisco ASA (США), популярний продукт для управління доступом до мережі й блокування небажаного трафіку [29]. Основною перевагою файрволів є їхня простота у налаштуванні та ефективність для базової фільтрації мережевого трафіку. Водночас вони можуть бути неефективними проти складних атак, які обходять традиційні засоби контролю.

3. Шифрування даних є важливим механізмом для запобігання витоку або крадіжці інформації. Навіть якщо зловмисники отримають доступ до зашифрованих даних, вони не зможуть їх використовувати без відповідного ключа. Популярні інструменти шифрування включають VeraCrypt (Франція), який надає можливості для шифрування файлів і дисків із відкритим кодом [113], та OpenSSL, міжнародний проєкт для забезпечення шифрування даних під час передачі через інтернет за допомогою протоколів SSL/TLS [87]. Основною перевагою шифрування є захист даних навіть у разі їх втрати або крадіжки, проте цей метод підвищує вимоги до обчислювальних ресурсів і може ускладнювати доступ до даних у разі втрати ключів дешифрування.

4. Мультирівневий захист (Defense in Depth) є концепцією багатоетапної безпеки, яка включає кілька шарів захисту, таких як мережевий захист,

контроль доступу, шифрування та моніторинг загроз. Такий підхід значно ускладнює реалізацію успішних атак, оскільки передбачає незалежну роботу кількох рівнів безпеки. Прикладом є Check Point (Ізраїль), що забезпечує комплексний підхід до безпеки, інтегруючи міжмережеві екрани, IDS/IPS та шифрування [22]. Інше рішення, Cisco SecureX (США), об'єднує фільтрацію трафіку, моніторинг загроз і шифрування в єдину систему для забезпечення безпеки в реальному часі [30]. Основною перевагою такого підходу є зниження ймовірності успішної атаки, оскільки кожен рівень працює незалежно. Проте складність у налаштуванні та підтримці багаторівневого захисту може вимагати значних ресурсів.

1.2. Особливості розповсюдження інформації в соціальних мережах

Соціальні мережі стали основною платформою для обміну інформацією у сучасному суспільстві. Їхні особливості розповсюдження інформації суттєво відрізняються від традиційних засобів комунікації завдяки інтерактивності, швидкості та можливості охопити широку аудиторію за короткий час.

Однією з ключових характеристик розповсюдження інформації в соціальних мережах є *вірусний ефект* — здатність окремого повідомлення, зображення або відео стрімко поширюватися серед великої кількості користувачів у надзвичайно короткі терміни [65].
Цей феномен став можливим завдяки інтеграції специфічних механізмів взаємодії користувачів із контентом, таких як репости, лайки, коментарі, а також завдяки впровадженню автоматизованих рекомендаційних алгоритмів, які значною мірою визначають, який саме контент буде поширюватися найактивніше.

Репости є базовим механізмом лавиноподібного поширення інформації. Вони дозволяють користувачу буквально у кілька кліків продублювати цікаве

повідомлення на власній сторінці, відкриваючи його для перегляду всій своїй мережі контактів. Кожен наступний репост створює додатковий ланцюг розповсюдження, що в геометричній прогресії збільшує кількість потенційних переглядів. Таким чином формується *ефект лавини*, де початкове джерело може миттєво набрати десятки тисяч або навіть мільйони охоплень без додаткових зусиль з боку автора контенту.

Лайки та *коментарі*, хоча і не забезпечують прямого дублювання повідомлення, виконують важливу роль сигналів для алгоритмів платформи [114]. Коли користувач взаємодіє з певним контентом (натискає "подобається", залишає коментар або зберігає пост), платформа "розуміє", що цей контент має підвищену актуальність і потенційний інтерес для ширшої аудиторії. У результаті така публікація отримує більше шансів з'явитися у стрічках новин інших користувачів або потрапити в спеціальні добірки, такі як "Рекомендоване", "Тренди" чи "Вам може сподобатися".

Рекомендаційні алгоритми є однією з найпотужніших рушійних сил розповсюдження інформації в соціальних мережах. Вони не тільки реагують на безпосередню взаємодію користувачів із контентом, але й проактивно формують їхнє інформаційне середовище. Алгоритми аналізують широкий спектр поведінкових даних: які пости читає користувач, які лайкає, з ким комунікує, які відео переглядає і скільки часу проводить над кожною публікацією. На основі цих даних формується *персоналізована стрічка новин*, у якій пріоритет надається контенту з найвищою ймовірністю зацікавити конкретного користувача [111]. Завдяки такому підходу навіть автори з невеликою аудиторією можуть отримати надзвичайно широке охоплення, якщо їхній контент виявиться "влучним" для алгоритмічного просування.

Разом із цим алгоритми соціальних мереж мають властивість створювати так звані *інформаційні бульбашки* (*echo chambers*), коли користувачі бачать переважно контент, що відповідає їхнім уже сформованим переконанням та інтересам [24]. Це явище призводить до зменшення різноманітності точок зору

у стрічці новин користувача та обмежує його контакт із альтернативною інформацією. Як наслідок, формується закрите інформаційне середовище, де існуючі погляди лише підсилюються, що може сприяти радикалізації думок, поляризації суспільства та зниженню критичного мислення.

Таким чином, вірусне поширення інформації в соціальних мережах базується на складній взаємодії між поведінкою користувачів і алгоритмічними механізмами автоматичного просування контенту. Цей процес забезпечує вражаючу швидкість і масштаби розповсюдження, але водночас створює серйозні ризики, пов'язані з інформаційною однобокістю, маніпуляціями, поширенням дезінформації та вразливістю аудиторій до навмисного впливу.

Ще однією важливою особливістю соціальних мереж є *низький поріг публікації інформації*. Завдяки простоті доступу до цифрових платформ і мінімальним вимогам до створення контенту, будь-який користувач — незалежно від рівня своєї кваліфікації, надійності джерела інформації чи особистих намірів — може миттєво створити текстовий пост, фото, відео або навіть розгорнуту історію й поширити її серед потенційно необмеженої аудиторії.

У порівнянні з традиційними засобами масової інформації (такими як друковані медіа, телебачення чи радіо), де перед публікацією інформація зазвичай проходить через багатоетапний процес перевірки фактів, редакційну обробку і відповідальність за достовірність змісту, соціальні мережі *не передбачають обов'язкових процедур модерації або верифікації* [91], [106].

Ця особливість породжує середовище, в якому поряд із об'єктивними новинами та особистими висловлюваннями поширюються й *різні форми недостовірної інформації:*

- Дезінформація — свідомо створений і поширений неправдивий контент з метою ввести в оману аудиторію.

• Фейкові новини — вигадані або спотворені повідомлення про події, які можуть базуватися на частково правдивих фактах, але інтерпретовані або змінені з певною метою.

• Маніпулятивні повідомлення — контент, що використовує правдиву інформацію у спотвореному або вирваному з контексту вигляді для досягнення політичних, економічних чи соціальних цілей.

Особливо небезпечним є те, що в умовах відсутності чітких і ефективних механізмів перевірки контенту на рівні самих платформ, така інформація має можливість швидко набирати популярності, особливо під час гострих соціальних чи політичних подій [120]. Кризи, вибори, протести, війни створюють інформаційне середовище, де потреба в швидкому обміні новинами переважає над вимогами до їхньої достовірності.

Крім того, соціальні мережі активно стимулюють емоційний характер контенту. Дослідження показують, що повідомлення, які викликають сильні емоції — гнів, страх, шок, радість, захоплення — мають значно більший шанс бути поміченими і поширеними користувачами, ніж нейтральна або стримана інформація [114].

Це пояснюється базовими психологічними механізмами: емоційні реакції стимулюють людину до активних дій, серед яких найпоширенішими є:

- поширення інформації серед друзів чи підписників,
- коментування подій,
- участь у флешмобах чи інформаційних кампаніях.

Соціальні мережі через свої рекомендаційні алгоритми активно підсилюють цей ефект. Алгоритми віддають перевагу тим публікаціям, які отримують вищий рівень взаємодії — лайки, коментарі, репости — саме тому емоційно насичений контент отримує більше показів у стрічках новин. Контент, який викликає інтенсивну емоційну реакцію, краще запам'ятовується користувачами, довше затримує їх увагу, що в свою чергу покращує показники залученості платформи.

У результаті, емоційно забарвлена, але не завжди достовірна інформація,

має набагато більше шансів на широке охоплення, ніж точний, аналітичний, але менш емоційний контент.

Особливо яскраво ця тенденція проявилася під час *повномасштабної війни в Україні*, яка почалася у 2022 році. В соціальних мережах масово поширювалися емоційні фото та відео зруйнованих міст, історії про особисті трагедії мирних жителів, подвиги військових, звернення лідерів думок та публічних осіб. Емоційний контент став не лише способом швидкого інформування світової спільноти про події в Україні, а й потужним засобом мобілізації громадської думки та залучення допомоги. Однак паралельно з цим поширювалася і велика кількість дезінформації, зокрема вигадані історії, постановочні кадри або маніпулятивні інтерпретації реальних подій, що використовували емоційний заряд для досягнення пропагандистських цілей [68].

Таким чином, низький поріг публікації у поєднанні з перевагою емоційного контенту створюють в соціальних мережах середовище, де користувачі стають одночасно споживачами і поширювачами великої кількості інформації, достовірність якої часто залишається неперевіреною. Це не лише ускладнює інформаційний ландшафт, але й підвищує ризики маніпуляцій, поширення дезінформації та загострення соціальних конфліктів.

Важливу роль у процесах розповсюдження інформації в соціальних мережах відіграють тематичні спільноти та лідери думок. Тематичні спільноти об'єднують користувачів навколо спільних інтересів, професійних занять або світоглядних орієнтацій. Це можуть бути групи, орієнтовані на певні сфери — такі як військова аналітика, екологічний активізм, політичні рухи, технології, наука, мистецтво, культура або інші тематики. В межах таких спільнот контент поширюється із підвищеною інтенсивністю завдяки декільком важливим чинникам:

по-перше, високий рівень зацікавленості учасників у специфічній тематиці сприяє активному обміну новинами, аналітичними матеріалами, коментарями;

по-друге, в таких спільнотах формується внутрішній рівень довіри між учасниками, що означає, що контент, який надходить від "своїх", сприймається із меншою критикою та вищою готовністю до поширення [96].

Таким чином, тематичні спільноти виступають локальними центрами прискореного обміну інформацією, що робить їх стратегічно важливими для розповсюдження як достовірних повідомлень, так і для потенційної дезінформації чи маніпуляцій.

Окрім того, центральне місце у процесі впливу на громадську думку в соціальних мережах займають *лідери думок (influencers, opinion leaders*).

Лідери думок — це окремі особистості, які завдяки своїй репутації, експертності, особистим якостям (харизмі, послідовності, активності) та професійній діяльності набули довіри певної аудиторії. До них належать блогери, журналісти, громадські діячі, науковці, активісти, політики, відомі експерти у конкретних галузях.

Публікації лідерів думок часто вирізняються високою динамікою поширення і мають здатність швидко отримувати широкий резонанс серед аудиторії. Завдяки довірі, яку вони здобули серед своїх підписників або учасників спільнот, такі пости не лише швидко набирають популярності, але й істотно впливають на сприйняття подій. Лідери думок можуть формувати або коригувати уявлення аудиторії про ті чи інші явища, події чи процеси, задаючи рамки їхньої інтерпретації.

Крім того, вони здатні спрямовувати громадські настрої у певному бажаному руслі. Це може бути використано як для мобілізації підтримки важливих соціальних ініціатив, так і для маніпулятивного впливу в рамках цілеспрямованих інформаційних кампаній [92].

Особливістю комунікацій через лідерів думок є те, що сприйняття повідомлень від них здійснюється через призму довіри до особистості, а не через незалежну оцінку змісту. Тобто аудиторія частіше схильна приймати інформацію на віру, без додаткової критичної перевірки, що істотно підсилює ефективність впливу.

У природному (органічному) інформаційному середовищі лідери думок можуть відігравати позитивну роль — сприяти поширенню важливої суспільної інформації, мобілізувати людей на підтримку корисних ініціатив, підвищувати обізнаність із соціальними чи гуманітарними питаннями. Проте у випадку цілеспрямованих інформаційних кампаній — наприклад, під час виборів, соціальних протестів або гібридних операцій — лідери думок можуть бути використані як канали маніпулятивного впливу, коли через довіру аудиторії поширюються викривлені, тенденційні або фальсифіковані повідомлення.

Таким чином, роль тематичних спільнот і лідерів думок у поширенні інформації в соціальних мережах є подвійною: вони одночасно виступають потужним інструментом мобілізації громадської думки і можуть бути використані для посилення впливу дезінформаційних або маніпулятивних кампаній.

Крім того, на процес розповсюдження інформації в соціальних мережах значно впливає *географічна та демографічна специфіка аудиторії*. Кожна соціальна платформа має свої характерні групи користувачів [107]:

— Наприклад, **TikTok** популярний серед молоді віком від 16 до 24 років, що впливає на формат контенту (короткі відео, динамічна подача, акцент на емоціях і візуальній привабливості).

— **Facebook** має старшу аудиторію, часто 30+, що визначає популярність довших текстів, публічних дискусій, а також поширення локальних новин.

— **Instagram** фокусується на візуальному контенті і є популярним серед молоді та молодших дорослих, акцентуючи увагу на естетиці, лайфстайлі, особистих історіях.

— **Twitter (X)** традиційно має більш політизовану та новинно орієнтовану аудиторію, що робить його майданчиком для оперативного обміну інформацією під час криз чи надзвичайних подій.

— У країнах Східної Європи, зокрема в Україні, популярність також мають месенджери типу **Telegram**, де інформація поширюється через канали й чати, часто з меншою модерацією і швидким обміном новинами.

Регіональні особливості теж мають значення: контент, що орієнтований на певний регіон або національну аудиторію, має свої мовні, культурні й емоційні акценти. Наприклад, для української аудиторії під час війни важливою є патріотична риторика, використання символіки національної боротьби, а для міжнародної аудиторії — подання фактів із наголосом на гуманітарних аспектах і порушеннях міжнародного права.

Таким чином, ефективне поширення інформації в соціальних мережах залежить не лише від якості контенту, а й від правильного вибору каналів комунікації, врахування впливу тематичних спільнот, лідерів думок, а також специфіки географічної та демографічної структури цільової аудиторії.

Яскравим прикладом впливу тематичних спільнот і лідерів думок стало інформаційне висвітлення війни в Україні у 2022 році. У перші місяці повномасштабного вторгнення Росії багато українських і міжнародних лідерів думок, таких як журналісти, блогери, активісти та громадські діячі, швидко мобілізували свої аудиторії для підтримки України.

Одним із таких прикладів є діяльність відомих українських блогерів та військових кореспондентів, таких як Ілля Пономаренко (журналіст Kyiv Independent), які оперативно публікували репортажі з місця подій англійською мовою для міжнародної аудиторії. Їхні дописи масово поширювалися у Twitter, Telegram і Facebook, допомагаючи формувати об’єктивну картину війни за межами України.

Також варто згадати появу образу "Привида Києва" — символічного українського льотчика-аса, який за повідомленнями в перші дні війни збивав ворожі літаки. Хоча пізніше з'ясувалося, що ця історія була більше міфом, ніж фактом, вона стала потужним психологічним стимулом для підняття бойового духу українців та підтримки у світі. Ця історія поширювалася через численні

тематичні групи у Facebook, Telegram-канали та особисті акаунти лідерів думок, і завдяки емоційній подачі набирала мільйони переглядів.

Крім того, тематичні спільноти в месенджерах (наприклад, канали в Telegram на кшталт "Оперативний ЗСУ", "Українська правда", "DeepState") стали ключовими джерелами новин для мільйонів користувачів всередині України та діаспори, забезпечуючи швидке і широке розповсюдження як новин, так і закликів до дій — донатів, участі в інформаційних кампаніях, гуманітарній допомозі [36], [68], [111], [120].

Ці приклади демонструють, наскільки сильно взаємодіють тематичні спільноти, лідери думок і географічно орієнтовані аудиторії у процесі поширення інформації, особливо в умовах кризи.

Таким чином, розповсюдження інформації в соціальних мережах відзначається високою швидкістю, широким охопленням, емоційністю контенту, значним впливом рекомендаційних алгоритмів і одночасною вразливістю до поширення недостовірної або маніпулятивної інформації.

1.3. Психологічні та соціальні аспекти впливу інформації в мережевих комунікаціях

У сучасних мережевих комунікаціях інформація виконує не тільки роль передачі даних, а й має потужний *психологічний* та *соціальний вплив* на індивідуальну та колективну поведінку користувачів. Особливості сприйняття, обробки та поширення інформації в мережі формуються під дією низки психологічних механізмів і соціальних процесів.

Одним із основних психологічних ефектів є *ефект емоційного зараження* (*emotional contagion*). У контексті соціальних мереж цей ефект полягає у тому, що люди, навіть не усвідомлюючи цього, переймають емоції інших користувачів, з якими взаємодіють. Наприклад, повідомлення, що викликають

тривогу, страх, гнів або ентузіазм, можуть передаватися від однієї особи до іншої через лайки, репости, коментарі або навіть просте читання новинної стрічки.

Емоційно забарвлений контент викликає сильніші реакції порівняно з нейтральним або аналітичним повідомленням. Люди схильні частіше взаємодіяти саме з тим контентом, який викликає у них емоційну відповідь, що автоматично сприяє його подальшому поширенню через алгоритми соціальних платформ. Саме це призводить до *лавиноподібного поширення настроїв* у великих спільнотах. Наприклад, поява великої кількості тривожних новин у стрічці може викликати масову паніку, посилити відчуття безнадійності або страху серед великої кількості користувачів.

Особливо яскраво ефект емоційного зараження проявляється у періоди *кризових подій* — таких як воєнні конфлікти, природні катастрофи чи пандемії. У таких випадках емоційно насичений контент (наприклад, відео з місця обстрілів, свідчення очевидців, емоційні звернення лідерів думок) може швидко охопити мільйони людей і викликати масову мобілізацію суспільства, зміну його поведінки або навіть сприяти ухваленню важливих політичних рішень.

Дослідження Крамера, Гіллорі та Хенкока у 2014 році ("Experimental evidence of massive-scale emotional contagion through social networks") експериментально довело, що навіть незначна зміна емоційного забарвлення контенту у стрічці новин Facebook змінювала емоційний стан користувачів — ті, хто бачив більше позитивного контенту, частіше самі постили позитивні повідомлення, а ті, хто бачив більше негативного — проявляли більше песимістичних настроїв (Kramer, Guillory, Hancock, 2014) [67].

Таким чином, емоційне зараження є потужним механізмом впливу в мережевих комунікаціях, який може змінювати індивідуальні настрої, формувати масові суспільні настрої та істотно впливати на соціальну динаміку під час кризових подій.

Ще одним важливим психологічним феноменом у мережевих комунікаціях є *ефект підтвердження* (*confirmation bias*). Цей ефект полягає у схильності людини звертати увагу переважно на ту інформацію, яка підтверджує її вже існуючі переконання, упередження чи світогляд, і водночас ігнорувати або заперечувати дані, що суперечать її позиції. У контексті соціальних мереж це явище має особливо виразний характер завдяки персоналізації стрічок новин, де алгоритми пропонують контент, який відповідає інтересам і вподобанням користувача [104].

Як наслідок, у мережевих середовищах виникають так звані інформаційні бульбашки (*echo chambers*), коли користувачі опиняються у середовищі, де переважають односторонні точки зору. В межах такої бульбашки людина постійно стикається з контентом, що підтверджує її власну думку, що підсилює її переконаність у власній правоті й знижує здатність критично аналізувати альтернативні позиції. Це призводить до поляризації суспільних поглядів і суттєво ускладнює конструктивний діалог між представниками різних поглядів, оскільки кожна сторона дедалі більше віддаляється від іншої в інформаційному просторі [25].

Паралельно з цим виявляється ще один потужний механізм — *ефект групового мислення (groupthink*). У рамках онлайн-спільнот користувачі схильні адаптувати свої думки і поведінку відповідно до норм і цінностей групи, в якій вони перебувають. Особливо це проявляється у великих тематичних групах або під час масових кампаній у соціальних мережах. Підсвідомий тиск групи часто змушує окремих користувачів змінювати або підлаштовувати свої оцінки подій, навіть якщо внутрішньо вони мають іншу думку [104].

Явище групового мислення призводить до зниження критичності мислення, і навіть до прийняття колективних рішень, які можуть бути ірраціональними, маніпулятивними або небезпечними. Інформація, що суперечить колективній думці, часто сприймається як ворожа або шкідлива, а її носії можуть зазнавати соціального осуду чи витіснення з групи.

Наукові дослідження також підтверджують ці процеси. Наприклад, Касс Санстейн у своїй роботі (Republic: Divided Democracy in the Age of Social Media) (2017) докладно описує, як інформаційні бульбашки і групове мислення в мережі сприяють соціальній поляризації і розмиванню здатності суспільства до здорової демократичної дискусії [104].

Таким чином, психологічні ефекти підтвердження і групового мислення є фундаментальними механізмами формування мережевої поведінки користувачів і мають глибокі наслідки для соціальної структури та процесів прийняття рішень у цифрову епоху.

Також важливим є феномен *вірусного поширення емоційних наративів*. В інформаційному просторі особливу силу має контент, який апелює до базових людських почуттів — страху за особисту безпеку, співчуття до постраждалих, почуття несправедливості, гніву або патріотизму. Такі повідомлення значно ефективніше впливають на свідомість користувачів, ніж нейтральна аналітика чи фактичні дані, оскільки вони діють на глибинні емоційні механізми сприйняття.

Соціальні мережі активно стимулюють поширення такого емоційно насиченого контенту. Завдяки алгоритмам, які надають перевагу публікаціям із високою залученістю (лайки, коментарі, репости), емоційні історії, меми, відео та звернення миттєво поширюються між мільйонами користувачів. При цьому мережеві комунікації нерідко сприяють формуванню громадської думки на основі емоційних імпульсів, а не раціонального осмислення фактів, що може призводити до масових настроїв гніву, страху або ейфорії [114].

Особливо показовими прикладами такого процесу є широке поширення емоційних відео та постів під час кризових подій — наприклад, під час війни в Україні (2022) або пандемії COVID-19, коли історії особистої трагедії чи героїзму ставали каталізаторами громадських кампаній підтримки, мобілізації допомоги або змін у суспільних настроях [91], [114].

Окремої уваги заслуговує вплив *мережевої інформації на психологічний стан особистості.* Постійне перебування у насиченому інформаційному

середовищі, особливо під час кризових періодів (воєн, катастроф, пандемій), часто призводить до *інформаційного перевантаження* (*information overload*). Людина опиняється в умовах постійного потоку тривожної інформації, яка не дає можливості емоційно дистанціюватися від подій.

Така надмірна кількість емоційно насичених повідомлень може викликати зростання рівня стресу, почуття тривоги, виснаження та у деяких випадках — депресивні стани. Соціальні мережі створюють ефект постійної присутності в епіцентрі подій ("ефект інформаційної пастки"), що психологічно виснажує користувача і знижує його здатність до критичного мислення та адекватного сприйняття реальності.

Американська психологічна асоціація у своїй доповіді "Stress in America™ 2020" підкреслює, що тривале перебування в умовах постійного інформаційного тиску підвищує ризик розвитку тривожних розладів, порушень сну та депресії (American Psychological Association, 2020).

Таким чином, емоційні наративи в соціальних мережах мають подвійний ефект: з одного боку, вони можуть мобілізувати суспільство для колективних дій, а з іншого — сприяти емоційному виснаженню та погіршенню психологічного стану великої кількості людей [4].

Таким чином, мережеві комунікації мають складний і багатовимірний вплив на психіку і соціальну поведінку користувачів. Вони одночасно об'єднують людей у спільноти, формують громадські настрої, прискорюють процеси мобілізації, але також можуть посилювати розкол у суспільстві, емоційне виснаження та вразливість до маніпуляцій.

Висновки до першого розділу

1. Проаналізовано особливості розповсюдження інформації в соціальних мережах. Встановлено, що вірусний ефект поширення контенту

забезпечується через механізми репостів, лайків, коментарів і персоналізованих рекомендаційних алгоритмів, що значно прискорює розповсюдження як достовірної, так і маніпулятивної інформації. Низький поріг публікації в соціальних мережах сприяє швидкому поширенню дезінформації та фейкових новин, особливо у кризові періоди. Роль тематичних спільнот і лідерів думок у формуванні громадської думки є критично важливою, а географічні та демографічні особливості аудиторій впливають на формат і характер розповсюджуваної інформації.

2. Визначено психологічні та соціальні аспекти впливу інформації в мережевих комунікаціях. Доведено, що емоційне зараження, ефект підтвердження, інформаційні бульбашки та групове мислення суттєво змінюють сприйняття і поведінку користувачів. Під час кризових подій, таких як війна в Україні або пандемія COVID-19, емоційно забарвлений контент має значно сильніший вплив на формування громадських настроїв, ніж нейтральна інформація. Постійне перебування у тривожному інформаційному середовищі призводить до інформаційного перевантаження, підвищеного рівня стресу і ризику розвитку психологічних розладів серед користувачів.

РОЗДІЛ 2.
АНАЛІЗ І АДАПТАЦІЯ МОДЕЛІ КУРАМОТО ДЛЯ СОЦІАЛЬНИХ МЕРЕЖ

2.1. Класифікація існуючих моделей розповсюдження інформації у соціальних мережах

Класифікація моделей розповсюдження інформації базується на їхньому призначенні, підходах до моделювання та структурних особливостях мереж, у яких відбувається поширення інформації. Поділяються за такими критеріями:

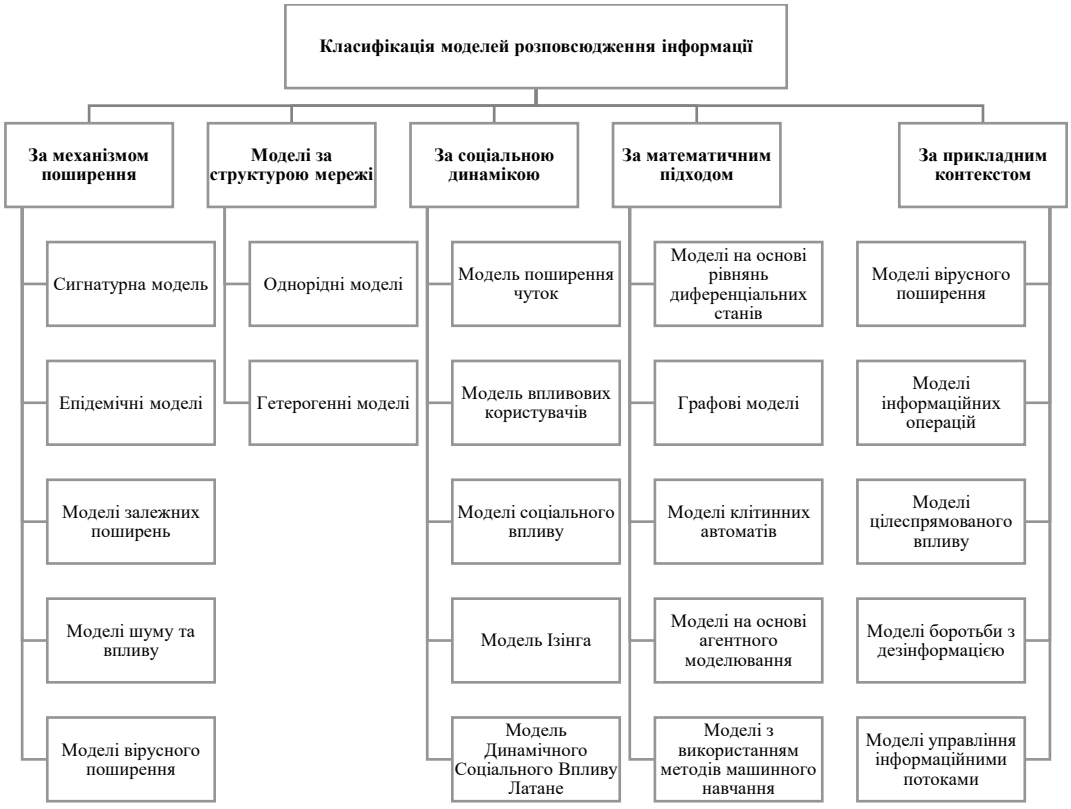


Рис 2. 1. Класифікація моделей розповсюдження інформації

1. За механізмом поширення:

- *Сигнатурні моделі (Threshold Models)* моделюють процес прийняття інформації або рішень у соціальних мережах, базуючись на ідеї, що

користувач (вузол мережі) приймає інформацію лише тоді, коли вплив від сусідів перевищує певний поріг [24], [64]. Цей підхід особливо корисний для аналізу соціального впливу, поширення ідей, поведінки користувачів та динаміки прийняття рішень.

Принцип роботи моделі:

1. Мережа представляється графом G = (V, E), де V – множина вузлів (користувачів), а E – множина зв'язків між ними.

2. Кожен вузол і має свій власний поріг θ_i, який визначає, насскільки сильним має бути соціальний вплив, щоб вузол прийняв інформацію.

3. Вузол і приймає інформацію, якщо загальний вплив сусідів σ_i перевищує його поріг:

$$\sigma_i = \sum_{j \in N(i)} w_{ij} x_j,$$

Де $N(i)$ – множина сусідів вузла i

w_{ij} – вага зв'язку між вузлом i та j

$x_j \in \{0, 1\}$ – стан вузла j: 1, якщо j прийняв інформацію і 0, якщо ні.

4. Вузол i змінює свій стан з 0 на 1, якщо:

$\sigma_i \geq \theta_i$

Динаміка моделі

Процес поширення інформації в моделі відбувається поетапно [116]:

- На першому етапі невелика частина вузлів (ініціатори) отримує інформацію та встановлюється в стані x_i = 1.
- На кожному наступному етапі кожен вузол *i*, стан якого x_i = 0, перевіряє, чи сума впливів його сусідів σ_i перевищує поріг θ_i.
- Процес повторюється доти, поки жоден новий вузол не змінює свій стан.

Модифікація моделі

1. Узагальнена модель з випадковими порогами [64]:

У цій версії поріг θ_i кожного вузла генерується випадковим чином, наприклад, із рівномірного розподілу:

$\theta_i \sim u\ [0,1]$

2. Модель із вагомими зв'язками [54]:

Вплив сусідів нормалізується, щоб урахувати нерівномірність зв'язків:

$$\sigma_i = \sum_{j \in N(i)} \frac{w_{ij} x_j}{\sum_{k \in N(i)} w_{ik}}$$

3. Модель з часовими затримками [116]:

У цій версії враховується затримка між моментом отримання інформації та її поширення:

$$x_i\ (t+1) = \begin{cases} 1, & \text{якщо } \sigma_i(t) \geq \ \theta_i \\ 0, \text{інакше} \end{cases}$$

Сигнатурні моделі знаходять широке застосування в різних реальних сценаріях. У соціальних мережах вони використовуються для аналізу поширення вірусних новин або контенту, дозволяючи зрозуміти, як швидко інформація розповсюджується між користувачами. У сфері маркетингу ці моделі дозволяють прогнозувати ефективність акцій чи рекламних кампаній, а також оцінювати їх вплив на цільову аудиторію .

У політиці сигнатурні моделі допомагають оцінювати ефективність інформаційних кампаній, таких як передвиборчі ініціативи, та передбачати, як політичні повідомлення вплинуть на виборців. В економіці ці моделі застосовуються для моделювання прийняття інновацій, даючи можливість зрозуміти, як нові технології або продукти інтегруються у суспільство.

Загалом, сигнатурні моделі є потужним інструментом для вивчення соціальних систем. Вони надають чітку методологію для прогнозування поведінки вузлів у мережі, враховуючи вплив оточуючого середовища. Це робить їх цінними у контексті аналізу та планування в багатьох прикладних галузях [24], [92].

- Епідемічні моделі (SIR, SEIR)

Епідемічні моделі використовуються для моделювання процесів поширення інформації аналогічно до поширення інфекційних захворювань. Вони засновані на поділі популяції на групи, які змінюють свій стан у залежності від часу та взаємодії з іншими групами [4].

1. SIR (Susceptible-Infectious-Recovered) — базова модель, що описує динаміку поширення інформації через три стани:

S (Susceptible): Вузли (користувачі), які ще не отримали інформацію, але можуть її сприйняти.

I (Infectious): Вузли, які отримали інформацію і активно її поширюють.

R (Recovered): Вузли, які більше не поширюють інформацію (втратили інтерес або завершили поширення).

Диференційне рівняння моделі:

$$\frac{dS}{st} = -\beta SI,$$

$$\frac{dI}{dt} = \beta SI - \gamma I,$$

$$\frac{dR}{dt} = \gamma I,$$

де:

β — коефіцієнт передачі інформації (ймовірність того, що "вразливий" вузол стане "інфікованим").

γ — коефіцієнт відновлення (ймовірність переходу з "інфікованого" стану до "відновленого").

2. SEIR (Susceptible-Exposed-Infectious-Recovered) — розширена версія SIR-моделі, яка враховує ще один стан E (Вузли, які отримали інформацію, але ще не почали її поширювати)

Диференціальні рівняння моделі:

$$\frac{dS}{st} = -\beta SI,$$

$$\frac{dE}{dt} = \beta SI - \sigma E,$$

$$\frac{dI}{dt} = \sigma E - \gamma I,$$

$$\frac{dR}{dt} = \gamma I,$$

Епідемічні моделі, такі як SIR і SEIR, мають свої особливості, які роблять їх придатними для аналізу різних процесів розповсюдження інформації. SIR-модель добре підходить для короткострокових інформаційних кампаній, які завершуються через певний час, тоді як SEIR-модель є більш реалістичною завдяки врахуванню затримки між отриманням інформації та її подальшим поширенням. Ця характеристика робить SEIR-модель кориснішою в контексті більш складних сценаріїв [19], [65].

У соціальних мережах епідемічні моделі застосовуються для аналізу вірусного контенту, зокрема прогнозування швидкості та масштабу поширення популярних постів, відео чи новин. Вони також корисні для оптимізації інформаційних кампаній, дозволяючи розробити стратегії для охоплення максимальної аудиторії. Крім того, ці моделі можуть допомогти в боротьбі з дезінформацією, оцінюючи вплив і швидкість розповсюдження фейкових новин.

Проте епідемічні моделі мають свої обмеження. Вони ігнорують складність соціальних мереж, наприклад, неоднорідність зв’язків між вузлами та вплив ключових вузлів на поширення інформації. Крім того, ці підходи припускають, що кожен вузол взаємодіє з іншими однаково, що не завжди відповідає реальності. Також їм важко враховувати поведінкові та емоційні аспекти, які суттєво впливають на поширення інформації [68], [81].

Незважаючи на ці обмеження, епідемічні моделі залишаються універсальним інструментом для аналізу інформаційних потоків у великих мережах, також їх можна інтегрувати з іншими підходами,

- Моделі залежних поширень (Cascade Models)

Моделі залежних поширень аналізують динаміку передачі інформації, коли вузол поширює її тільки за умови, якщо кількість його сусідів, які вже прийняли цю інформацію, перевищує певний поріг. Ці моделі ефективно використовуються для вивчення взаємозалежностей у соціальних мережах, маркетингових кампаніях і динаміці поведінки.

Принцип роботи моделі

Cascade Models описують процес поширення через активізацію вузлів у мережі:

1. Графова структура:

Мережа представляється у вигляді графу G=(V,E), де V — вузли (користувачі), а E — зв'язки (взаємодії).

2. Активний стан:

Вузол i переходить у стан "активний" (поширює інформацію), якщо частка активних сусідів перевищує заданий поріг θ_i:

$$\frac{\sum_{j \in N(i)} a_j}{|N(i)|} \geq \theta_i,$$

$N(i)$ – множина сусідів вузла i

$a_j \in \{0, 1\}$ – стан сусіда j (1 – активний, 0 - неактивний)

Процес поширення інформації у моделі починається з активації невеликої частки вузлів, які слугують джерелом поширення. Ці активні вузли впливають на своїх сусідів, змушуючи їх переходити в активний стан відповідно до заданого правила. Далі процес поширення продовжується, активуючи все нові вузли, і повторюється, доки не настане стабільний стан, коли більше жоден вузол не змінює свого стану.

Одна із модифікацій каскадної моделі, це імовірнісна каскадна модель, припускає що активація вузла залежить від імовірності p_{ij}, яка визначає силу впливу вузла j на i [19], [66]:

$$P(\text{активація}) = 1 - \prod_{j \in N(i)}(1 - p_{ij}).$$

Моделі залежних поширень знаходять широке застосування в різних галузях. У маркетингу вони дозволяють моделювати поширення рекламних кампаній чи вірусного контенту, прогнозуючи охоплення аудиторії. У соціальних мережах моделі використовуються для аналізу динаміки поширення новин, чуток чи ідей, що дозволяє визначати ключові вузли впливу. У сфері пропаганди та боротьби з дезінформацією вони допомагають оцінювати ефективність інформаційних операцій. Також ці моделі застосовуються у поведінкових науках для вивчення соціальних норм і колективної поведінки, що сприяє кращому розумінню динаміки групових процесів.

Основними перевагами моделей є їхня відносна простота реалізації для статичних мереж, а також ефективність у сценаріях, де інформація поширюється поступово залежно від локальних умов. Це робить їх зручними для використання у багатьох прикладних задачах [19], [92].

Однак моделі мають і обмеження. Вони ігнорують емоційні та соціальні фактори, які можуть суттєво впливати на динаміку поширення. Крім того, моделі є чутливими до початкових параметрів, таких як розподіл порогів, що може ускладнити їхню адаптацію до реальних даних. Вони також не враховують глобальних ефектів, наприклад, зворотного зв’язку між різними частинами мережі, що обмежує їхню точність у складних системах.

1.Сумарний вплив сусідів:

$$\sigma_i = \sum_{j \in N(i)} w_{ij} a_j,$$

Де $N(i)$ – множина сусідів вузла i

w_{ij} – вага зв’язку між вузлом i та j

$a_j \in \{0, 1\}$ – стан вузла j: 1, якщо j прийняв інформацію і 0, якщо ні.

2.Умова активації, якщо вузол i змінює свій стан з 0 на 1, якщо:

$\sigma_i \geq \theta_i$

Каскадні моделі є потужним інструментом для аналізу поширення інформації в соціальних мережах, дозволяючи оцінювати вплив різних вузлів та прогнозувати динаміку поширення залежно від початкових умов [51], [116].

- Моделі шуму та впливу (Noise and Influence Models)

Моделі шуму та впливу використовуються для опису процесів прийняття рішень вузлами у мережі. Вони враховують соціальний вплив сусідів і додають випадкові фактори (шум), які створюють невизначеність у поведінці системи. Ці моделі поєднують як вплив сусідів, так і індивідуальні особливості вузлів.

Кожен вузол у мережі має свою схильність до прийняття інформації, яка залежить від впливу сусідів. Загальний вплив на вузол $\boldsymbol{i}$ можна виразити як:

$$\sigma_i = \sum_{j \in N(i)} w_{ij} x_j,$$

Формула є універсальною через:

- Гнучкість: Вона легко адаптується до різних моделей через зміну параметрів w_{ij} або додавання додаткових умов, таких як шум або порогові значення.
- Загальну топологію мережі: Вона базується на графовій структурі, що є основою для всіх моделей поширення інформації.
- Локальний характер: Формула описує локальний вплив сусідів, що є фундаментальним для будь-якої взаємодії у мережі.

Хоча формула виглядає однаково, її роль і застосування змінюються залежно від специфіки моделі. У каскадних моделях вона використовується для активації вузлів, у сигнатурних — для аналізу порогів, а в моделях шуму та впливу — для моделювання стохастичних процесів [18], [47].

Випадковий шум додається до загального впливу, щоб врахувати випадковість у прийнятті рішень. Математично це виражається так:

$$P(x_i = 1) = \sigma(F_i + \eta_i),$$

де

η_i – випадкова змінна, що моделює шум

$\sigma(z) -$ сигмоїдна функція

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

Рішення про прийняття інформації вузол приймає інформацію з імовірністю P(x_i=1), яка залежить як від соціального впливу, так і від шуму.

Повний вплив на вузол із шумом можна записати як [18], [56]:

$$P(x_i = 1) = \frac{1}{1 + e^{-(\sum_{j \in N(i)} w_{ij} x_j + \eta_i}},$$

Ця формула дозволяє врахувати як вплив сусідів, так і випадкові фактори, що визначають поведінку вузла.

Моделі шуму та впливу надають потужний інструмент для аналізу складних процесів поширення інформації, особливо у системах з високим рівнем невизначеності.

Модифікації моделей шуму та впливу спрямовані на покращення їхньої гнучкості та адаптивності до різних контекстів. Динамічний шум дозволяє моделювати зміни у поведінці вузлів у часі. Наприклад, зовнішні події або коливання в інформаційному середовищі можуть змінювати рівень випадковості (η_i), що впливає на рішення вузлів у мережі. Це особливо корисно для аналізу динамічних процесів у соціальних мережах.

Нерівномірний вплив сусідів враховує зміни ваг зв'язків (w_{ij}) між вузлами залежно від контексту чи часу. Наприклад, під час періодів високої активності в мережі вплив деяких сусідів може значно зрости, що забезпечує реалістичніше моделювання поширення інформації.

Контекстуальні фактори, такі як емоційний стан, рівень довіри до джерела чи специфіка аудиторії, додають додаткові параметри, що дозволяють адаптувати модель до конкретного завдання. Це може включати, наприклад,

моделювання різної реакції на дезінформацію або вплив вірусного контенту [56].

У сфері застосування, моделі шуму та впливу мають широкий спектр використання. У соціальних мережах вони допомагають аналізувати поширення чуток, вірусного контенту або новин, враховуючи випадкові фактори, які впливають на взаємодію користувачів. У маркетингу ці моделі дозволяють прогнозувати ефективність рекламних кампаній, враховуючи невизначеності у поведінці споживачів. В інформаційній безпеці моделі використовуються для аналізу поширення дезінформації та пропаганди, враховуючи вплив випадкових подій [18], [47].

Однак моделі мають свої обмеження**.** Включення шуму ускладнює інтерпретацію результатів, оскільки додає високий рівень невизначеності. Крім того, вибір відповідного розподілу для моделювання шуму може бути складним завданням, особливо в реальних сценаріях із великими мережами.

Особливостями моделей шуму та впливу є їхня гнучкість та здатність адаптуватися до різних контекстів завдяки додаванню додаткових параметрів. Однак ця гнучкість може супроводжуватися складністю у прогнозуванні через високий рівень невизначеності, що характерно для реальних мереж [18].

Загалом, моделі шуму та впливу є потужним інструментом для аналізу складних систем із високою невизначеністю. Вони дозволяють прогнозувати поведінку користувачів у соціальних мережах, оцінювати ефективність маркетингових кампаній і розробляти стратегії боротьби з дезінформацією.

- Моделі вірусного поширення (Viral Spread Models)

Дана модель описує динаміку розповсюдження інформації у соціальних мережах, проводячи аналогію з поширенням інфекцій. Основна мета таких моделей — зрозуміти механізми, що визначають швидкість і масштаб розповсюдження контенту, зокрема новин, відео, чуток або рекламних кампаній [130]. Мережа при цьому моделюється як граф G = (V, E), де V — це вузли (користувачі), а E — зв’язки між ними, які визначають можливість взаємодії.

У таких моделях вузли можуть перебувати в одному з трьох станів. Користувачі у стані S (Susceptible) ще не взаємодіяли з контентом, але можуть це зробити. Користувачі у стані I (Infected) вже отримали контент і поширюють його серед своїх зв’язків у мережі. Нарешті, користувачі у стані R (Recovered) припинили взаємодію з контентом і більше не впливають на його розповсюдження. Перехід між цими станами визначається ймовірностями та залежить від таких факторів, як вага зв’язків між вузлами та швидкість передачі інформації [130].

Відмінність моделей вірусного поширення від епідемічних моделей полягає в контексті та механізмах взаємодії. Епідемічні моделі, такі як SIR або SEIR, спочатку були розроблені для біологічних систем і базуються на ймовірностях передачі вірусу через контакт. Вони фокусуються на природному поширенні "інфекції", мають більш просту структуру взаємодії і зазвичай не враховують мережеву топологію.

Моделі вірусного поширення в соціальних мережах, навпаки, враховують складну структуру зв’язків між вузлами та специфіку поведінки користувачів. Наприклад, у соціальних мережах важливими факторами стають вплив лідерів думок, індивідуальні схильності до поширення інформації та емоційна складова контенту. Крім того, моделі вірусного поширення часто включають механізми затухання інформації, коли певний контент поступово втрачає актуальність і перестає поширюватися, що не є характерним для стандартних епідемічних моделей [130].

Перехід між цими станами описується диференційними рівняннями, подібними до епідемічних моделей, таких як SIR або SEIR:

$$\frac{dS}{st} = -\beta SI, \frac{dI}{dt} = \beta SI - \gamma I, \frac{dR}{dt} = \gamma I,$$

де β – швидкість передачі контенту, γ – швидкість «відновлення» (завершення поширення).

Окрім базових станів, модель вірусного поширення вводить додаткові фактори, які впливають на динаміку:

Імовірність поширення визначається формулою:

$P(\text{взаємодія}) = 1 - \prod_{j \in N(i)}(1 - p_{ij})$.

де p_{ij} — ймовірність поширення між вузлом і та його сусідом j [116], [117].

Часове затухання:

Здатність вузла поширювати контент зменшується з часом:

$$p(t) = p_0 e^{-\alpha t}$$

де α – коефіцієнт затухання [130].

Розширені аналітичні моделі використовуються для опису динаміки поширення інформації серед аудиторії. Вони базуються на математичному підході, який враховує залежність кількості користувачів у різних станах від часу. Модель поділяє аудиторію на три групи:

- A (Активні користувачі): Ті, хто прочитав інформаційну новину та активно поширює її.
- B (Неактивні користувачі): Ті, хто ще не прочитав новину, але є користувачами каналу.
- C (Непідписані користувачі): Ті, хто не є частиною каналу та не читав новину.

Динаміка поширення описується системою диференційних рівнянь:

$$\begin{cases} \dfrac{dA}{dt} = -A(t)\mu + B(t)\varepsilon + C(t)\lambda; \\ \dfrac{dB}{dt} = -B(t)\mu - B(t)\varepsilon + C(t)\lambda(1-\varepsilon); \\ \dfrac{dC}{dt} = (A(t) + B(t)\mu - C(t)\lambda). \end{cases}$$

де:

- λ — інтенсивність підписування на новинного агента,
- μ — інтенсивність відписування від новинного агента,
- ε — інтенсивність прочитування новини .

Задавши початкові умови $A(t) = A_0$, $B(0) = B_0$, $C(0) = C_0$, рішення має вигляд:

$$A(t) = C_1 g + C_2 v e^{t(-\mu-\lambda)} - C_3 e^{t(-\mu-\varepsilon)},$$

$$B(t) = -C_1 r - C_2 u e^{t(-\mu-\lambda)} + C_3 e^{t(-\mu-\varepsilon)},$$

$$C(t) = C_1 + C_2 e^{t(-\mu-\lambda)}.$$

де C1, C2, C3 — коефіцієнти, що залежать від початкових умов

Де $C_1 = \frac{A_0+B_0+C_0u-C_0v}{g-r+u-v}$,

$C_2 = \frac{-A_0-B_0+C_0g-C_0r}{g-r+u-v}$,

$C_3 = \frac{A_0r-A_0u+B_0g-B_0v+C_0gu-C_0ru}{g-r+u-v}$,

а параметри g, r, u, v визначаються:

$g = \left[\frac{\lambda\varepsilon}{\mu} - \frac{\varepsilon(-\lambda\varepsilon+\lambda)}{\mu(-\mu-\varepsilon)}\right]$,

$v = \left[-\varepsilon + \frac{\varepsilon(-\lambda\varepsilon+\lambda)}{\lambda(\lambda-\varepsilon)}\right]$,

$r = \frac{(-\lambda\varepsilon+\lambda)}{-\mu-\varepsilon}$,

$u = \frac{(-\lambda\varepsilon+\lambda)}{\lambda-\varepsilon}$,

Актуальність новин можна трактувати як імовірність зустрічі вибраної новини в усіх джерелах, що розглядаються. Тобто

$$\varphi = \frac{m}{M},$$

m – кількість новинних джерел, які описують вибрану новину;

M – загальна кількість джерел.

Параметр, який характеризує час опублікування новини, визначається наступним чином:

$$\delta = \frac{e}{E},$$

де e – кількість новин за визначеною тематикою, до якої відноситься контрольована новина, що розташовані в новинній стрічці користувача вище контрольованої новини;

E – загальна кількість новин за визначеною тематикою у новинній стрічці користувача.

Активність користувачів (ω):

$$\omega = \frac{s}{(A_0 + B_0)},$$

де s – кількість користувачів, що здійснили одну з дій: лайк або репост;

$(A_0 + B_0)$ – кількість користувачів новинного агента.

Імовірність прочитання новини виражається як:

$$\varepsilon = \varphi\delta\omega.$$

Модель дозволяє розрахувати кількість користувачів у кожному стані *A(t)*, *B(t), C(t)* у будь-який момент часу, прогнозувати зростання охоплення аудиторії, аналізувати динаміку активності та затухання популярності новини.

Модель може бути використана для планування медіа-кампаній. Наприклад, якщо новина про соціальну ініціативу отримала високу актуальність (ϕ), добре позиціонується у стрічці (δ) і має активну взаємодію (ω), можна спрогнозувати швидкість зростання числа активних користувачів і розробити стратегії для підтримки інтересу до ініціативи [130].

2. Моделі за структурою мережі:

- Однорідні моделі

Вони передбачають, що всі вузли та зв’язки в мережі мають однакові властивості. Це означає, що всі учасники мають рівний вплив, однакову кількість зв'язків і рівний потенціал для поширення інформації. Цей підхід спрощує математичне моделювання, оскільки не потрібно враховувати індивідуальні відмінності між вузлами.

Прикладом однорідної мережі може бути мережа на основі випадкових графів (Random Graphs), де кожен вузол має однакову ймовірність бути з’єднаним з іншими вузлами, і всі зв’язки мають однакову вагу. Моделі таких мереж використовуються для вивчення базових процесів поширення інформації, де відсутні значні відмінності між вузлами. Це може бути корисно для аналізу базових сценаріїв або в освітніх цілях, коли необхідно зрозуміти основи поширення в простих системах. [41].

- Гетерогенні моделі

Вони враховують різницю між вузлами мережі. Вони моделюють реальні соціальні або комунікаційні системи, де учасники мають різний рівень впливу, популярності або взаємодії. У цих моделях важливі характеристики вузлів, такі як кількість зв'язків або ступінь їхнього впливу.

Одним із прикладів гетерогенної мережі є соціальні медіа, такі як Facebook або Twitter, де користувачі мають різну кількість друзів або підписників. Відомі блогери або знаменитості мають більший вплив, оскільки вони мають набагато більше підписників, ніж звичайні користувачі [10], [77]. Тут важливу роль відіграють не тільки кількість зв’язків, але й сила цих зв’язків, які можна виміряти через показник центральності (наприклад, степінь центральності), що визначає важливість вузла у мережі.

Мережа наукових цитувань, наприклад, на Google Scholar або ResearchGate, також є прикладом гетерогенної мережі, де дослідники з високим імпакт-фактором (який вимірюється кількістю посилань на їхні роботи) мають більший вплив на розповсюдження ідей або публікацій [77]. Такі мережі мають вузли з різним рівнем активності та впливу, що робить їх гетерогенними.

Гетерогенні моделі дозволяють точніше описати реальні соціальні або комунікаційні мережі, де важливо враховувати, що не всі вузли мають однаковий вплив. Ці моделі використовуються для прогнозування динаміки інформаційного поширення, пошуку впливових користувачів у соціальних мережах або для аналізу маркетингових стратегій [92].

Порівняння однорідних та гетерогенних мереж

- Однорідні моделі спрощують процеси моделювання та аналізу, ідеально підходять для теоретичних досліджень, де потрібно розуміти загальні принципи поширення без детального аналізу структури мережі.

- Гетерогенні моделі дозволяють врахувати реалістичні варіації у мережах, такі як різний рівень впливу, різні кількості зв'язків або роль окремих

ключових учасників. Вони більш складні для аналізу, але дають більш точні результати для реальних мереж.

Ці два підходи можуть комбінуватися для більш комплексного аналізу, коли спершу вивчаються базові процеси в однорідних мережах, а потім переходять до більш складних сценаріїв із гетерогенними моделями.

3. За соціальною динамікою

Соціальна динаміка враховує поведінку індивідів у соціальних мережах, їхню взаємодію і прийняття рішень. Нижче наведено детальний опис моделей поширення інформації, класифікованих за соціальною динамікою.

- Модель поширення чуток (Rumor Spreading Model)

Модель поширення чуток аналізує динаміку поширення інформації у мережах, фокусуючись на поведінкових особливостях користувачів. Ця модель була запропонована в 1965 році Далеєм і Кендаллом (Daley-Kendall Model, DK-модель) і є адаптацією епідемічної моделі SIR для процесів поширення чуток. DK-модель класифікує користувачів на три групи: інформатори, слухачі та забувачі.

Основні компоненти моделі:

1. Групи користувачів**:**

- Інформатори (Spreaders): Активно поширюють чутку серед сусідів у мережі.
- Слухачі (Ignorants): Ще не чули чутку, але можуть сприйняти її та стати інформаторами.
- Забувачі (Stiflers)**:** Припиняють поширення інформації після усвідомлення, що вона неактуальна, неправдива або вже широко відома.

2. Динаміка переходу між станами**.** Інформатори поширюють чутку з ймовірністю β/N, де β — коефіцієнт передачі, а N — загальна кількість користувачів. Ймовірність того, що інформатор зустріне забувача і припинить поширення, моделюється виразом:

$$\gamma \frac{V(V+W)}{N},$$

де γ – коефіцієнт взаємодії, V – кількість інформаторів, W – кількість забувачів.

Процеси поширення чуток описується наступними диференційними рівняннями:

$$\frac{dU}{dt} = -\beta\frac{UV}{N}, \qquad \frac{dV}{dt} = \beta\frac{UV}{N} - \gamma\frac{V(V+W)}{N}, \qquad \frac{dW}{dt} = \gamma\frac{V(V+W)}{N}$$

де:

- U — слухачі (Ignorants),
- V — інформатори (Spreaders),
- W — забувачі (Stiflers)

Особливості моделі

Адаптація SIR-моделі**.** DK-модель використовує підхід епідемічного моделювання, але змінює інтерпретацію груп, адаптуючи їх до інформаційних процесів [34].

Ймовірність припинення розповсюдження**.** Розповсюдження припиняється, коли інформатор зустрічає забувача, що моделюється через взаємодію груп V і W.

Використання параметрів:

β: інтенсивність передачі інформації.

γ: ймовірність припинення поширення.

Модель поширення чуток має широке застосування в різних сферах. У соціальних мережах вона використовується для аналізу динаміки поширення чуток, новин або інформаційних вірусів. Завдяки цьому можна виявляти основні механізми розповсюдження, визначати вузли з найбільшим впливом і прогнозувати, як інформація поширюватиметься у часі.

У маркетингу модель застосовується для прогнозування охоплення вірусного контенту. Вона дозволяє визначити, наскільки ефективно рекламна кампанія охоплює цільову аудиторію, і виявити точки, де можна посилити

взаємодію, щоб максимізувати результат. Такий підхід дозволяє зменшити витрати на рекламу за рахунок більш точного таргетингу.

У боротьбі з дезінформацією модель допомагає виявляти механізми припинення поширення неправдивих новин. Аналізуючи взаємодії між користувачами, можна оцінити, які дії сприятимуть зменшенню поширення фейків, наприклад, через залучення ключових вузлів для спростування інформації.

Модель має низку переваг. Її відносна простота забезпечує легкість реалізації для аналізу статичних мереж. Крім того, вона ефективно моделює припинення поширення інформації через взаємодії між користувачами, що дозволяє прогнозувати, коли і чому поширення чуток може затухати.

Проте модель має і обмеження. Вона є чутливою до початкових умов і вибору параметрів, таких як ймовірність передачі чи швидкість сприйняття інформації. Це може ускладнювати застосування моделі до реальних даних. Окрім того, модель часто не враховує емоційні й соціальні фактори, які суттєво впливають на поширення інформації у реальному житті [38], [129].

Загалом, модель поширення чуток є ефективним інструментом для аналізу інформаційних процесів. Вона допомагає зрозуміти, як чутки поширюються, досягають піку популярності і затухають. Подальший розвиток цієї моделі можливий через інтеграцію поведінкових і соціальних факторів, що підвищить точність прогнозів і розширить можливості її застосування у реальних сценаріях.

- *Модель впливових користувачів (Influential User Model)*

Вона зосереджена на ключових вузлах (інфлюенсерах), які відіграють значну роль у поширенні інформації [138]. Ці вузли визначаються їхнім рівнем впливу, що розраховується на основі кількості зв’язків, активності, і довіри інших користувачів.

Основні аспекти моделі:

1. Рівень впливу вузла: Визначається через кількість зв’язків та активність у взаємодіях.

2. Пріоритетність вузлів: Впливові вузли пришвидшують поширення інформації та формують загальний тон обговорення.

Формули:

Загальна формула впливу вузла:

$$I_v = \alpha * k_v + \beta * a_v$$

де:

I_v — вплив вузла v,

k_v — кількість зв'язків вузла,

a_v — активність вузла,

α,β — вагові коефіцієнти, які показують важливість відповідних характеристик [63].

Модель впливових користувачів має широке застосування в різних сферах. У маркетингу вона використовується для ідентифікації інфлюенсерів, через яких можна поширювати рекламні кампанії для досягнення максимальної аудиторії. Інфлюенсери, як правило, є ключовими вузлами в мережі, які можуть значно прискорити охоплення вірусного контенту завдяки своїй популярності та авторитету.

У соціальних мережах модель дозволяє аналізувати поширення контенту через вузли з високим впливом. Це допомагає зрозуміти, які користувачі відіграють вирішальну роль у передачі інформації, та як оптимізувати стратегії розповсюдження новин або контенту для кращого залучення [61], [138].

Однією з основних переваг моделі є врахування ключових параметрів, таких як кількість зв'язків (зв'язність) та активність користувачів. Це дозволяє чітко виділити найвпливовіші вузли в мережі. Також модель відносно проста в реалізації, особливо якщо використовувати методи обчислення центральності, як-от центральність Каца, що адаптується під різні сценарії.

Попри свої переваги, модель чутлива до вибору параметрів α та β, які визначають вагу зв'язків і активності. Неправильне налаштування цих коефіцієнтів може призвести до неточних результатів. Крім того, модель недостатньо враховує соціальні та психологічні фактори, які впливають на

взаємодію користувачів у реальних мережах, такі як емоційний зв’язок чи рівень довіри.

Модель впливових користувачів є потужним інструментом для аналізу інформаційних потоків у мережах. Її застосування дозволяє ефективно оцінити вірусний потенціал контенту, ідентифікувати ключових гравців та прогнозувати результати маркетингових кампаній. Водночас подальший розвиток моделі може включати інтеграцію поведінкових та емоційних характеристик, що підвищить точність прогнозів [63].

- Центральність Каца

Дозволяє оцінити значущість вузла через сукупність прямих та непрямих зв’язків:

Центральність Каца вимірює відносну важливість вузла мережі *i* шляхом обчислення кількості інших вузлів сусідів першого ступеня, які підключаються до вузла *i* подано як [129].

$$C_{Katz}\,(i) = \sum_{k=1}^{\infty} \sum_{j=1}^{n} \propto^{k} (A^{k})_{ji}$$

Це рівняння показує, що значення на місці *(i,j)* матриці суміжності *A* піднесений до влади *k* такий як A^k представляє загальну кількість *k*-ступеневі зв'язки між вузлом *i* і вузолом *j*.

де *A* — матриця суміжності, *α* — коефіцієнт ослаблення.

У спрощеному вигляді:

$$\overrightarrow{C_{Karz}} = \{(I - \alpha A^{T})^{-1} - I\}\vec{I}$$

де:

- I — матриця ідентичності,
- A^T— транспонована матриця суміжності,
- $\vec{I}$ — вектор ідентичності [129].

- Моделі соціального впливу (Social Influence Models)

Аналізують, як поведінка, думки або переконання користувачів у мережі змінюються під впливом їхнього оточення. Ці моделі ґрунтуються на припущенні, що кожен користувач взаємодіє з певною групою інших

користувачів (сусідів), і його стан залежить від впливу, який на нього чинять ці сусіди [48].

Стан користувача (вузла) змінюється на основі станів його сусідів. Формально це описується формулою:

$$\theta_i\,(t+1) = \frac{1}{|N(i)|}\sum_{j\in N(i)} \theta_j(t),$$

де θ_i - стан вузлів *i*, *N(i)* – сусіди вузла *i*, */N(i)/* — кількість сусідів користувача і,

$\theta_j(t)$ — стан сусіда j у момент часу t.

Ця формула відображає, що новий стан користувача є середнім станом його сусідів. Це дозволяє моделювати процеси, коли думка або поведінка користувача змінюється під впливом колективної думки оточення.

Переваги моделі

1. Простота реалізації: Формула дозволяє швидко та ефективно моделювати зміни в мережах.

2. Гнучкість: Модель може бути адаптована до різних сценаріїв, таких як вивчення соціальних трендів, формування суспільної думки або поширення інформації.

3. Реалістичність: Враховує локальну взаємодію між користувачами, що відповідає реальним процесам у соціальних мережах.

Модель соціального впливу може використовуватися для аналізу, як користувачі починають змінювати свою поведінку, наприклад, переходять на здорове харчування або починають займатися спортом, під впливом постів друзів чи лідерів думок. У такому сценарії модель допоможе зрозуміти, які групи користувачів найбільше піддаються впливу, і визначити ключові вузли, через які інформація поширюється найефективніше.

Моделі соціального впливу є потужним інструментом для аналізу взаємодій у соціальних мережах. Завдяки простоті та гнучкості вони дозволяють моделювати широкий спектр процесів — від формування суспільної думки до прогнозування поширення інформації. Їхнє

вдосконалення через інтеграцію емоційних, поведінкових та соціальних аспектів дозволить отримувати більш точні результати та знайти нові підходи до аналізу складних динамічних систем [48].

- Модель Ізінга

Широко використовується для аналізу фазових переходів у фізичних та соціальних системах. Основна ідея полягає у вивченні взаємодій між сусідніми елементами системи, які можуть перебувати в одному з двох станів. У контексті соціальних мереж ця модель дозволяє моделювати, як думки або дії індивідів змінюються під впливом сусідів.

Модель базується на розподілі елементів системи на вузли, кожен із яких має два можливих стани: "+1" (активний) або "−1" (неактивний). Вибір стану вузлом залежить від його сусідів і впливу зовнішніх факторів. Наприклад:

- Якщо користувач підтримує певну ідею або бере участь у проєкті, його стан встановлюється на "+1".
- Якщо користувач відмовляється від участі або змінює думку, його стан переходить до "−1".

Імовірність зміни стану вузла визначається як:

$$p_i(t) = \frac{1}{1+\exp\left(\frac{\Delta\mu_i(t)}{T}\right)}$$

де:

- $p_i(t)$ — ймовірність зміни стану вузла *i* у момент часу *t*,
- $\Delta\mu_i$ — зміна енергії системи, спричинена переходом вузла *i* до іншого стану,
- T — параметр, що моделює "температуру" системи або рівень зовнішніх впливів.

Зміна енергії системи для вузла *i* обчислюється за формулою:

$$\mu_i(t) = -m_i(t-1)\sum_{j=1}^{n} m_j(t-1)$$

де:

- $\mu_i(t)$ — стан вузла *i* у момент часу *t*,

- $\sum_{j=1}^{n} m_j(t-1)$ — сума станів сусідів вузла i у попередній момент часу.

Модель Ізінга застосовується для моделювання колективної поведінки у соціальних системах:

- Прогнозування поширення думок: Модель дозволяє оцінити, як думки змінюються у мережі під впливом зовнішніх факторів (температура) та взаємодії між сусідами.
- Дослідження групових рішень: Аналізує, як вплив окремих учасників може змінювати глобальну поведінку системи.
- Визначення точок рівноваги: Допомагає знайти стани, коли система досягає стабільності, наприклад, у прийнятті групового рішення [60].

Отже, модель Ізінга є простим, але потужним інструментом для моделювання складних соціальних процесів. Вона ефективно враховує взаємодію між вузлами, але може бути чутливою до початкових умов і параметра температури *T*. Також модель не завжди враховує унікальні індивідуальні характеристики, такі як різний рівень впливовості користувачів.

- *Модель динамічного соціального впливу Латане*

Модель описує процеси прийняття рішень користувачами під впливом їхнього оточення у соціальних мережах. Ця модель враховує психологічні аспекти прийняття рішень, зокрема залежність від внутрішнього порогу чи "шуму". Користувач приймає рішення тоді, коли певна кількість його зв’язків або оточення вже підтримали певну інформацію.

Модель базується на трьох ключових атрибутах взаємодії між джерелом інформації та агентом (користувачем):

1. Відстань між агентом і джерелом: Відображає швидкість передачі інформації.

2. Інтенсивність впливу джерела: Визначає силу впливу на користувача.

3. Кількість джерел**:** Оцінює кількість одночасних впливів на користувача.

Рівень соціального впливу на агента обчислюється за формулою:

$$I_i = -S_i\beta - \sum_{j=1, j\neq 1}^{N} \frac{S_j\ O_j O_i}{d_{i,j}^{\propto}},$$

де I_i – кількість соціального тиску на агента i;

O_i – думка і-го агента (+/- 1) відносно даного запитання; (значення +1 відповідає підтримці, значення -1 – спротиву щодо пропозиції);

S_i – сила соціального впливу ($S_i \geq 0$);

β – спротив агента щодо змін ($\beta > 0$);

$\propto$ – ступінь ослаблення відстані ($\propto \geq 0$);

N – загальна кількість агентів, які взаємодіють;

d_{ij} – відстань між агентами i та j ($d_{ij} \geq 1$).

Параметри моделі

- Спротив до змін (β): Рекомендоване значення β=2, що відповідає дослідженням Латане. Більші значення β означають, що для зміни думки агента потрібен більший тиск.
- Ступінь ослаблення впливу (α)**:** Наприклад, α=2. Це означає, що зі збільшенням відстані між джерелом і агентом потрібна більша величина впливу.

У соціальних мережах модель Латане може бути використана для:

- Дослідження впливу: Виявлення ключових користувачів, які мають найбільший соціальний вплив.
- Прогнозування змін у думках: Визначення умов, за яких користувачі змінюють свої погляди або поведінку.
- Оптимізації інформаційних кампаній**:** Пошук шляхів для максимізації ефективності інформаційного впливу.

Модель Латане є універсальним інструментом для аналізу взаємодій у соціальних мережах. Вона дозволяє враховувати як локальні, так і глобальні фактори, що впливають на поширення інформації. Її гнучкість дає змогу адаптувати підхід до різних сценаріїв, наприклад, для оптимізації рекламних кампаній чи боротьби з дезінформацією [69].

4. За математичним підходом

Моделі розповсюдження інформації за математичним підходом базуються на різних методах і техніках для опису та аналізу динаміки соціальних

процесів у мережах. Ці моделі використовують різноманітні математичні структури та рівняння для відтворення поведінки користувачів і передачі інформації в соціальних мережах [129].

- Моделі на основі рівнянь диференціальних станів

Ці моделі використовують диференціальні рівняння для опису змін стану користувачів з часом. Вони можуть описувати процеси поширення інформації через зміни у популяціях користувачів, розділених на різні стани (наприклад, інформовані, неінформовані, відновлені). Зазвичай використовуються моделі типу SIR або SEIR, які описують процеси, аналогічні поширенню інфекцій.

Основне рівняння для моделі SIR:

$$\frac{dS}{st} = -\beta SI, \qquad \frac{dI}{dt} = \beta SI - \gamma I, \frac{dR}{dt} = \gamma I,$$

де S, I, і R — кількість сприйнятливих, інфікованих і відновлених відповідно; β — коефіцієнт передачі інформації; γ — коефіцієнт відновлення [129].

Може бути використана в якості моделювання поширення чуток у соціальних мережах чи вивчення вірусних маркетингових кампаній.

- Графові моделі (Graph-Based Models)

Графові моделі орієнтовані на опис соціальних мереж як графів, де вузли — це користувачі, а ребра — це взаємодії між ними. Різні математичні операції на графах дозволяють моделювати складні процеси поширення інформації, включаючи пошук важливих вузлів, виявлення кластерів, визначення зв'язності і стабільності мережі.

Соціальні мережі моделюються як графи G=(V,E):

- V — вузли (користувачі), E — ребра (зв’язки).
- Матриця суміжності A[i][j]=1, якщо між вузлами *i* і *j* є зв'язок.

Метрики:

- Ступенева центральність: вузли з найбільшою кількістю зв’язків.
- Міжпосередницька центральність: вузли, що найчастіше з’єднують інші.

- Власна центральність враховує важливість сусідніх вузлів

Спектральний аналіз графів**:**

$$Av = \lambda v,$$

де A – матриця суміжності графа, v – власний вектор, λ – власне значення

Аналіз соціальних мереж для виявлення найбільш впливових користувачів, прогнозування поширення інформації, виявлення кластерів для персоналізованих рекомендацій, оптимізації рекламних кампаній і боротьби з дезінформацією.

Наприклад, графові моделі можуть бути використані не лише для аналізу соціальних мереж, але й для моделювання потоків інформації, управління інфраструктурою та аналізу фінансових транзакцій (наприклад, для виявлення шахрайства).

Графові моделі застосовуються для виявлення ключових користувачів (лідерів думок), прогнозування поширення інформації, аналізу кластерів та боротьби з дезінформацією. Вони дозволяють оптимізувати таргетовану рекламу та інформативні кампанії. Перевагою є їх гнучкість і ефективність в аналізі структур взаємодій, проте складність зростає для великих мереж.

Водночас графові моделі мають недоліки: вони потребують великих обчислювальних ресурсів для аналізу складних мереж, неоднорідність даних у реальних соціальних мережах може ускладнити побудову адекватного графа, а деякі соціальні взаємодії можуть бути невидимими (латентні зв’язки), що впливає на точність моделі. Незважаючи на ці обмеження, графові моделі є потужним інструментом, що розкриває приховані патерни соціальних зв’язків і сприяє прийняттю стратегічних рішень [39], [81].

- Моделі клітинних автоматів

Клітинні автомати — це дискретні моделі, де простір поділений на клітини, кожна з яких може приймати певний стан. Кожна клітина змінює свій стан відповідно до певних правил, враховуючи стан своїх сусідів. Це дозволяє моделювати локальні взаємодії між користувачами мережі та їхній вплив на поширення інформації.

Основний принцип клітинних автоматів:

- Клітинні автомати є дискретними моделями, у яких простір поділений на клітини.
- Кожна клітина може перебувати в одному з певних станів, які змінюються відповідно до визначених правил, зважаючи на стани сусідів.
- Взаємодія між клітинами формується локально, що дозволяє моделювати поширення інформації через мережі.

Зміна стану кожної клітини визначається формулою:

$$C\ (i,j) = f\big(C(i-1,j), C(i+1,j), C(i,j-1), C(i,j+1)\big),$$

де $C\ (i,j)$ – стан клітин на позиції (i,j), а функція f визначає правила переходу станів,

f— це функція переходу, яка залежить від станів сусідів клітини на певному кроці.

Модель клітинного автомата формалізується через співвідношення:

$$y_j\ (\text{t} +1) = \text{F}(y_j(t), O(j), T),$$

Де t – крок ітерації, F – формальне представлене правило переходу до іншого стану; $y_j(t)$ – стан на попередніх ітераціях; $O(j)$ – множина сусідніх клітин (окіл кінцевого клітинного автомату).

Модифікації та застосування. В найпростішому випадку клітинні автомати використовують три стани, аналогічні до DK-моделі (слухачі, інформатори, забувачі). Для більш адекватного моделювання пропонується враховувати "старіння новини" або "поріг реакції". Наприклад, чим більше часу проходить, тим менше клітина може "поширювати" інформацію.

Клітинні автомати також використовуються для моделювання поширення інновацій, нових ідей чи продуктів. Це можливо завдяки здатності автоматів враховувати локальну динаміку взаємодій між сусідами [91].

- Моделі на основі агентного моделювання (Agent-Based Models)

Агентні моделі фокусуються на поведінці окремих індивідів (агентів), які взаємодіють між собою в межах певної мережі. Кожен агент має унікальні характеристики, такі як рівень активності, схильність до поширення

інформації чи довіра до джерела [129]. Основною перевагою цього підходу є його здатність моделювати складні стратегії взаємодії між агентами та враховувати адаптивність їхньої поведінки.

Правила взаємодії агентів:

$$x_i(t+1) = f(x_i(t), \{x_i(t)\}_{j \in N(i)}),$$

де x_i — стан агента *i* у момент часу *t*, *N(i)* — набір сусідів агента, і f — функція, що визначає поведінку агента.

Ця функція може бути задана правилами, які моделюють поведінку агентів, наприклад:

- Довіра: агент приймає рішення на основі середньої думки своїх сусідів, зважуючи її відповідно до довіри до джерел.
- Інтенсивність: враховується кількість взаємодій із сусідами (наприклад, лайки, коментарі чи репости) [38].

Основні переваги агентних моделей включають можливість моделювання складних та нелінійних взаємодій, урахування адаптивності агентів і гнучкість у налаштуванні правил поведінки. Проте ці моделі є ресурсоємними, вимагають значних обчислювальних витрат для аналізу великих мереж і залежать від якості вихідних даних та налаштувань.

Таким чином, агентні моделі є потужним інструментом для аналізу соціальних мереж та прогнозування поширення інформації. Вони дозволяють досліджувати індивідуальну поведінку користувачів та її вплив на загальні процеси, хоча їх складність вимагає обережного підходу до реалізації [129].

- Моделі з використанням методів машинного навчання

Ці моделі використовують статистичні методи для аналізу і прогнозування процесів поширення інформації в соціальних мережах. Завдяки обробці реальних даних, ці моделі дозволяють будувати точні прогнози про поведінку користувачів, виявляти ключові вузли (наприклад, впливових користувачів) та аналізувати ефективність різних типів контенту. Машинне навчання допомагає ідентифікувати закономірності у великих наборах даних, які складно виявити за допомогою класичних методів.

Основні алгоритми, що застосовуються, включають класифікацію, регресію, кластеризацію та глибоке навчання. Наприклад, методи класифікації (логістична регресія, дерева рішень, метод опорних векторів) дозволяють передбачати, який тип контенту матиме найбільший вплив на аудиторію. Алгоритми регресії використовуються для оцінки швидкості поширення інформації або визначення факторів, які впливають на популярність постів. Методи кластеризації допомагають ідентифікувати групи користувачів зі схожими інтересами або поведінкою.

Алгоритми машинного навчання застосовуються для аналізу маркетингових кампаній у соціальних мережах. Наприклад, на основі історичних даних можна спрогнозувати, який контент найкраще взаємодіє з певними сегментами аудиторії. Моделі можуть аналізувати взаємодії (лайки, коментарі, репости) для визначення, які пости будуть вірусними. Крім того, можна прогнозувати ефективність рекламних кампаній, оцінюючи, як швидко інформація поширюватиметься та до яких користувачів вона дійде.

Машинне навчання в соціальних мережах відкриває широкий спектр можливостей для прогнозування і аналізу. Такі моделі дозволяють оцінювати динаміку поширення інформації, виявляти ключових користувачів для таргетованого впливу та створювати оптимальні стратегії для інформаційних кампаній. У майбутньому розвиток цих моделей буде включати інтеграцію соціальних та емоційних факторів, наприклад, аналіз емоційної реакції аудиторії на контент. Це дозволить зробити прогнози ще більш точними та створювати гнучкі інструменти для розуміння складних соціальних процесів [1], [93].

Таким чином, моделі на основі машинного навчання є незамінним інструментом для роботи з великими даними та аналізу поведінки користувачів у соціальних мережах, надаючи нові можливості для ефективного управління інформаційними потоками.

5. За прикладним контекстом

Моделі поширення інформації можна класифікувати за їх прикладним використанням у різних сферах. Цей підхід дає змогу визначити специфіку застосування моделі залежно від цілей, контексту та типу інформації.

- Моделі вірусного поширення (Viral Spread Models)

Ця модель описує процеси швидкої та масштабної передачі інформації, що нагадують вірусні маркетингові кампанії або природне поширення контенту в соціальних мережах.

Ці моделі демонструють, як інформація може поширюватися швидко завдяки масовій взаємодії між користувачами. Основна мета таких моделей полягає в досягненні максимально широкої аудиторії за короткий час [93].

- Моделі інформаційних операцій (Information Operations Models)

Описують процеси маніпулювання, контролю або впливу на інформаційні потоки для досягнення певних стратегічних цілей. Ці моделі враховують різні аспекти інформаційної взаємодії, такі як створення, поширення, модифікація інформації та її сприйняття аудиторією.

Основним елементом моделей є аналіз взаємодії між агентами, які можуть бути джерелами, передавачами чи приймачами інформації. Наприклад, розглядається впливовість вузлів мережі або ймовірність поширення певного повідомлення. Для формалізації таких процесів часто застосовуються математичні моделі, наприклад, рівняння, що описують зміну кількості агентів, залучених до операцій:

$$I_t = \alpha S_t - \beta R_t$$

де I_t — кількість агентів, які активно поширюють інформацію в момент часу t; S_t — кількість потенційних агентів, готових сприймати інформацію; R_t — кількість агентів, які вже припинили поширення інформації; α,β — параметри, що відображають швидкість взаємодії.

Також у моделях враховуються стратегії протидії інформаційним операціям, зокрема обмеження доступу до певних ресурсів або підвищення критичності сприйняття інформації в аудиторії. Наприклад, впровадження

інформаційних фільтрів або зміна тональності контенту може моделюватися через додаткові параметри.

Моделі інформаційних операцій застосовуються в аналізі інформаційної безпеки, прогнозуванні соціальної динаміки та розробці стратегій протидії маніпуляціям у цифрових мережах [39].

- Моделі цілеспрямованого впливу (Targeted Influence Models)

Моделі орієнтовані на оптимізацію процесу поширення інформації в соціальних мережах через ідентифікацію ключових користувачів, які мають найбільший вплив на інші вузли мережі. Ці користувачі, або лідери думок, можуть бути ефективно залучені для поширення інформації з метою досягнення максимального охоплення аудиторії.

Ключові характеристики:

- Фокус на важливих вузлах: Ці моделі зосереджуються на вузлах із високим ступенем зв'язку або значенням центральності в соціальній мережі, оскільки такі вузли мають найбільший потенціал для поширення інформації.
- Максимізація охоплення: Основна мета — поширити інформацію на якомога більшу частину мережі, використовуючи мінімальну кількість ресурсів. Це досягається через таргетований вплив на ключових користувачів.
- Інтеграція графових методів**:** Використовуються різні метрики для аналізу структури мережі та визначення впливових вузлів, такі як центральність за Кацом, центральність за власними значеннями тощо.

Графові підходи до аналізу центральності вузлів:

$$C(i) = \alpha \sum_{j=1}^{n} A(i,j)C(j),$$

де $C(i)$ — центральність вузла i, $A(i,j)$ — матриця суміжності, α — коефіцієнт впливу.

Метод дозволяє визначати вузли з найвищою центральністю, що використовуються як точки старту для поширення інформації.

Моделі цілеспрямованого впливу активно застосовуються у маркетингових кампаніях. Наприклад, бренди залучають інфлюенсерів (лідерів думок), які мають велику аудиторію та високий рівень взаємодії, для

поширення інформації про продукт. Це дозволяє значно збільшити охоплення кампанії та створити ефект вірусного маркетингу.

Головною перевагою таких моделей є їх ефективність, оскільки вони дозволяють мінімізувати витрати, спрямовуючи зусилля лише на найвпливовіших користувачів. Крім того, моделі є масштабованими, що дозволяє адаптувати їх для різних типів соціальних мереж та структур даних.

Однак, моделі мають і свої недоліки. Вони є чутливими до структури мережі, тому у випадку недостатніх або нерелевантних даних результати можуть бути неточними. Також ці моделі часто ігнорують такі важливі аспекти, як емоційний контекст або актуальність інформації, що може впливати на їхню ефективність [37].

У підсумку, моделі цілеспрямованого впливу є потужним інструментом для планування стратегій поширення інформації у великих мережах. Вони допомагають ідентифікувати ключових користувачів, які відіграють центральну роль у комунікації, що робить ці моделі важливими в умовах сучасного цифрового середовища.

- Моделі боротьби з дезінформацією (Misinformation Combat Models)

Моделі боротьби з дезінформацією спрямовані на аналіз процесів поширення неправдивої інформації у соціальних мережах і розробку ефективних стратегій її нейтралізації [114]. Вони враховують різноманітні соціальні, психологічні та інформаційні фактори, які впливають на швидкість і масштаб розповсюдження дезінформації. Одним із ключових аспектів таких моделей є аналіз довіри користувачів до джерел інформації та їх активність у поширенні контенту.

Формули цих моделей часто базуються на модифікованих диференціальних рівняннях. Наприклад, модифікована модель SIR для дезінформації описує динаміку поширення неправдивої інформації у вигляді рівняння:

$$\frac{dI}{dt} = \beta SI - \delta IR,$$

де β — коефіцієнт передачі інформації, δ — коефіцієнт нейтралізації неправдивої інформації, *S, I, R* — кількість сприйнятливих, інфікованих (тих, хто поширює дезінформацію) і "відновлених" (тих, хто перестав її поширювати) [128].

Прикладом використання таких моделей є розробка алгоритмів для соціальних мереж, які автоматично виявляють фейкові новини та обмежують їх поширення. Ці алгоритми можуть використовуватися для пріоритизації перевіреного контенту, створення систем попередження про сумнівну інформацію та блокування дезінформаційних кампаній.

Моделі боротьби з дезінформацією мають важливі переваги, такі як здатність аналізувати великі масиви даних і адаптуватися до змін у поведінці користувачів. Вони сприяють підтримці інформаційної безпеки та зниженню негативного впливу фейкових новин. Проте їхній успіх залежить від доступності достовірних даних, складності алгоритмів та рівня довіри до джерел інформації [131].

Таким чином, моделі боротьби з дезінформацією є важливим інструментом у сучасному цифровому середовищі. Вони допомагають виявляти та нейтралізувати загрози дезінформації, підвищуючи рівень довіри до інформаційного простору.

- Моделі управління інформаційними потоками (Information Flow Management Models)

Моделі управління інформаційними потоками спрямовані на прогнозування, аналіз і керування процесами поширення інформації в реальному часі. Вони особливо актуальні у ситуаціях, де необхідно оперативно доставляти критично важливі повідомлення, наприклад, під час соціальних криз, великих подій чи надзвичайних ситуацій. Завдяки цим моделям можна визначати, які шляхи передачі інформації є найефективнішими, та розробляти оптимальні стратегії її розповсюдження.

Ключовою характеристикою таких моделей є можливість пріоритетного аналізу потоків у складних мережах. Для цього використовуються динамічні

моделі, які дозволяють відстежувати швидкість та інтенсивність розповсюдження інформації у різних сегментах мережі. Основою для аналізу слугують математичні методи, такі як рівняння диференціальних станів:

$$\frac{dx}{dt} = Ax + Bu,$$

де x — стан мережі, A — матриця зв’язків, B — матриця керування.

Прикладом використання таких моделей є оптимізація доставки новин або повідомлень через хмарні сервіси під час великих соціальних подій, таких як вибори, спортивні змагання чи глобальні конференції. Вони допомагають забезпечити своєчасну та цільову доставку інформації до аудиторії, мінімізуючи затримки та перевантаження мережі.

Перевагами моделей управління інформаційними потоками є їх здатність масштабуватися під потреби різних мереж, інтегрувати дані в реальному часі та прогнозувати поведінку інформаційних потоків у складних системах. Це робить їх універсальними для застосування в багатьох сферах, включаючи маркетинг, кризовий менеджмент та медіа.

Однак ці моделі мають і певні обмеження. Висока складність побудови моделей та необхідність обробки великого обсягу даних можуть вимагати значних обчислювальних ресурсів. Крім того, ефективність моделей залежить від якості початкових даних та точності побудованих матриць зв’язків [105].

Таким чином, моделі управління інформаційними потоками є потужним інструментом для аналізу та оптимізації процесів поширення інформації. Вони дозволяють ефективно планувати інформаційні кампанії, підтримувати стабільність мережі в умовах великих навантажень та сприяти досягненню стратегічних цілей в інформаційному просторі.

2.2 Адаптація моделі Курамото до умов поширення інформації в соціальних мережах

Модель Курамото, створена для опису синхронізації осциляторів у фізичних системах, набула популярності не лише у фізиці, а й у соціальних науках. Зокрема, її можна адаптувати для аналізу розповсюдження інформації у соціальних мережах, де користувачі поводяться як осцилятори, а їх думки або стан прийняття інформації можуть бути представлені фазами цих осциляторів.

Модель Курамото можна адаптувати для аналізу розповсюдження інформації в інтернет-середовищі. У цьому контексті осцилятори можуть представляти індивідуальних користувачів або вузли в соціальних мережах, а фаза θ_i - їх думки або стан прийняття певної інформації.

Класична модель Курамото:

$$\frac{d\theta_i}{dt} = \omega_i + \sum_{j=1}^{N} K_{ij}\sin(\theta_j - \theta_i)$$

Де:

- θ_i — фаза *i*-го осцилятора. У випадку аналізу соціальних мереж, це може бути інтерпретовано як стан прийняття інформації або думки користувача.
- $\frac{d\theta_i}{dt}$ — швидкість зміни фази. Це вказує на те, як швидко осцилятор або користувач змінює свій стан або позицію щодо інформації.
- ω_i — природна частота осцилятора. Вона представляє внутрішню схильність кожного осцилятора (користувача) прийняти певну інформацію незалежно від інших.
- K_{ij} — коефіцієнт зв'язку між осциляторами *i* та *j*. Він визначає, наскільки сильно осцилятори впливають один на одного. У контексті соціальних мереж це можна розуміти як ступінь впливу одного користувача на іншого.

• $\sum_{j=1}^{N} K_{ij}\sin(\theta_j - \theta_i)$ - різниця фаз між осциляторами i та j, що моделює різницю у думках або стані прийняття інформації. Синус цієї різниці визначає силу взаємодії між осциляторами (користувачами).

Ця формула більш загальна і може описувати складніші динамічні системи. Вона враховує як індивідуальні характеристики кожного користувача (ω_i), так і змінні сили взаємодії між користувачами (K_{ij}). Це дозволяє моделювати гетерогенні мережі, де різні користувачі можуть мати різний рівень впливу і сприйнятливості до інформації.

Адаптована формула моделі Курамото має такий вигляд:

$$I_i = \alpha_i + \frac{\beta}{N}\sum_{j=1}^{N} \sin(\theta_j - \theta_i)$$

Де:

• θ_i - стан прийняття інформації i -м користувачем (аналоги фаз у моделі Курамото),

• α_i - індивідуальна схильність i -го користувача до прийняття нової інформації (аналог власної частоти),

• β - коефіцієнт взаємодії між користувачами (аналог коефіцієнта зв'язку K),

• N - загальна кількість користувачів,

• $\sum_{j=1}^{N} \sin(I_j - I_i)$ - сума синусів різниць станів прийняття інформації користувачами.

Ця формула описує зміну стану прийняття інформації користувачем i під впливом інших користувачів у мережі. Чим більше користувачів у мережі приймає певну інформацію (чим ближче їх стани I_j до I_i), тим більше шансів, що користувач i також прийме цю інформацію.

Ця формула орієнтована на моделювання розповсюдження інформації з акцентом на індивідуальні схильності користувачів (α_i) та середню взаємодію ($\frac{\beta}{N}$). Вона спрощує взаємодію, роблячи її однаковою для всіх користувачів, і

підходить для випадків, коли необхідно оцінити середній вплив інформації в однорідній групі користувачів.

Порівняння двох моделей

1. Гетерогенність проти однорідності: Оригінальна формула дозволяє моделювати різну силу взаємодії між користувачами, що робить її більш точною для складних мереж із різними рівнями впливу. Спрощена модель припускає, що всі користувачі взаємодіють однаково.

2. Складність розрахунків**:** Оригінальна модель складніша для аналізу, особливо в великих мережах, де кожен користувач має унікальний вплив на інших. Спрощена формула значно полегшує розрахунки, оскільки всі взаємодії нормалізовані на кількість користувачів.

Обидві моделі застосовуються для дослідження поширення інформації, але вибір залежить від складності мережі. Спрощена модель підходить для однорідних мереж із рівномірним впливом користувачів, тоді як оригінальна краще відображає гетерогенні взаємодії.

Модель Курамото ефективно аналізує синхронізацію, а її адаптація до соціальних мереж дозволяє точніше моделювати поширення інформації, виникнення трендів і формування колективної думки.

Розрахунок індивідуальної схильності (α_i) користувача до прийняття нової інформації можна здійснити, виходячи з різних характеристик і поведінки користувача в інтернет-середовищі. Це може включати такі фактори:

- Історія взаємодії з контентом: Користувачі, які часто взаємодіють з певним типом контенту (лайки, коментарі, поширення), можуть мати вищу схильність до прийняття подібної інформації.

- Соціальний вплив: Кількість і авторитет друзів чи підписників, які вже прийняли або поширили певну інформацію.

- Інтереси та вподобання: Інформація, що базується на уподобаннях користувача (наприклад, групи, до яких він належить, або теми, які він часто обговорює).

- Демографічні дані**:** Вік, стать, місце проживання тощо можуть також впливати на схильність до прийняття інформації.

Для спрощення, можна використовувати ймовірнісну модель, яка враховує ці фактори. Наприклад, використання логістичної регресії або інших моделей машинного навчання для прогнозування α_i на основі наведених факторів.

Приклад формули для обчислення α_i

Припустимо, що α_i залежить від наступних факторів:

- H_i: Історія взаємодії з контентом.
- S_i: Соціальний вплив (кількість друзів, які прийняли інформацію).
- I_i: Інтереси та вподобання.
- D_i: Демографічні дані.

Тоді α_i можна виразити через лінійну комбінацію цих факторів:

$\alpha_i = w_H H_i + w_S S_i + w_I I_i + w_D D_i + b$,

Де w_H, w_S, w_I, w_D – вагові коефіцієнти, які можна визначити за допомогою навчання моделі, а b – зміщення (базовий рівень схильності).

Кроки для обчислення α_i

1. Збір даних: Зібрати дані про взаємодію користувачів з контентом, їхні соціальні зв'язки, інтереси та демографічні характеристики.

2. Вибір моделі: Вибрати модель для прогнозування.

3. Навчання моделі: Використати зібрані дані для навчання моделі та визначення вагових коефіцієнтів.

4. Прогнозування: Використати навчену модель для прогнозування α_i для кожного користувача.

Рис 2. 2. Кроки для обчислення α_i

Пояснення компонента $\sum_{j-1}^{N} K_{ij}\sin(\theta_j - \theta_i)$

Цей компонент відповідає за взаємодію між користувачами і показує, як прийняття інформації одним користувачем впливає на інших. Ось більш детальне пояснення:

- $\sin(\theta_j - \theta_i)$вимірює різницю між станами прийняття інформації користувачами j та i. Синус цієї різниці вказує на те, наскільки сильний вплив одного користувача на іншого.
- Якщо θ_j близьке до θ_i, значення $\sin(\theta_j - \theta_i)$ буде малим, що означає, що зміна стану одного користувача не сильно вплине на іншого.
- Якщо θ_j значно відрізняється від θ_i, значення $\sin(\theta_j - \theta_i)$ буде більшим, що означає сильніший вплив.

Кожен елемент у формулі:

1.Індивідуальна схильність (ω_i): Вона визначає базову ймовірність того, що користувач i прийме нову інформацію. Це може залежати від особистих характеристик, інтересів, попередньої поведінки тощо.

2.Взаємодії між користувачами$\sum_{j=1}^{N} K_{ij}\sin(\theta_j - \theta_i)$: Це враховує вплив соціальних зв'язків і взаємодій. Коефіцієнт K_{ij} показує, наскільки сильний зв'язок між користувачами i та j [128].

Приклад обчислення

Припустимо, що маємо такі дані:

ω_1 = 0.5, ω_2 = 0.3, $\omega_3 = 0.4$

K_{12} = 0.1, K_{13} = 0.2, K_{21} = 0.1, K_{23} = 0.3, K_{31} = 0.2, K_{32} = 0.3

Початкові стани сприйняття інформації: θ_1 = 0.2, θ_2 = 0.4 θ_3 = 0.6

Формула для $\frac{d\theta_i}{dt}$ виглядатиме так: $\frac{d\theta_i}{dt}$ = 0.5 +0.1 sin(0.4-0.2) + 0.2 sin(0.6)

$s$in(0.2)≈0.1987 $s$in(0.4)≈0.3894

Тоді: $\frac{d\theta_1}{dt}$ = 0.5 + 0.1 * 0.1987 + 0.2 * 0.3894

$\frac{d\theta_1}{dt}$ ≈ 0.5+0.01987 + 0.07788 ≈ 0.59775

Цей результат означає, що швидкість зміни стану прийняття інформації користувачем 1 враховує як його індивідуальну схильність, так і вплив користувачів 2 та 3.

Модель Курамото дозволяє врахувати індивідуальну схильність користувачів та їх взаємодії при розповсюдженні інформації. Використання синусоїдальних функцій для вимірювання різниці станів прийняття інформації дозволяє моделювати динаміку поширення інформації в мережі, де вплив одних користувачів на інших залежить від їх поточного стану.

Дані для змінних у моделях поширення інформації та класичної моделі Курамото можуть бути отримані з різних джерел залежно від контексту їх використання. Важливо розуміти, що джерела інформації можуть значно варіюватися залежно від специфіки аналізованого середовища, доступності даних та мети дослідження.

У моделі поширення інформації ключовим параметром є інформаційний стан користувача (I_i), який може відображати рівень прийняття або ставлення користувача до певної інформації. Дані для цієї змінної можуть бути отримані шляхом проведення опитувань серед користувачів соціальних мереж, які дозволяють з'ясувати їхнє ставлення до конкретної теми. Крім того, корисну інформацію можна отримати шляхом аналізу поведінки користувачів у соцмережах, враховуючи, як часто вони діляться, коментують або ставлять вподобання певним повідомленням. Ще одним підходом є семантичний аналіз текстів, коли алгоритми обробки природної мови використовуються для визначення емоційної тональності чи думки користувача на основі його текстів (наприклад, постів або коментарів).

Індивідуальна схильність користувача до зміни поглядів (α_i) визначається низкою характеристик, які можуть бути отримані з психологічних профілів користувачів, наприклад, результатів особистісних тестів, що оцінюють рівень гнучкості мислення. Також важливу роль відіграють історичні дані про поведінку користувача у мережі: аналіз попередніх дій допомагає зрозуміти, наскільки він схильний змінювати свої переконання під впливом зовнішніх факторів.

Іншим важливим параметром є інтенсивність впливу сусідів (β), яка може бути визначена шляхом аналізу зв'язків у соціальній мережі. Наприклад, можна оцінити, наскільки активно користувач взаємодіє з іншими людьми через лайки, репости чи коментарі. Ще один підхід полягає у використанні експертних оцінок, де параметри моделі встановлюються на основі емпіричних досліджень, що враховують закономірності поширення інформації у суспільстві.

Загалом, для отримання необхідних даних можуть використовуватись різні джерела. Емпіричні вимірювання забезпечують дані, отримані шляхом експериментів або безпосередніх спостережень за поведінкою користувачів. Соціологічні дослідження, зокрема опитування та інтерв’ю, допомагають краще зрозуміти мотивацію користувачів та їхню реакцію на інформацію.

Аналіз даних передбачає використання методів машинного навчання та статистичного аналізу для збору та обробки великих обсягів інформації. Нарешті, комп'ютерне моделювання та симуляції дозволяють створювати штучні середовища, у яких можна тестувати різні сценарії поширення інформації та встановлювати початкові умови для подальшого аналізу.

Таким чином, вибір джерел даних залежить від специфіки дослідження, доступності інформації та поставлених завдань. Використання комбінації методів дозволяє отримати найбільш точні та надійні результати, необхідні для якісного аналізу процесів поширення інформації та взаємодії користувачів у мережах.

2.3. Застосування моделі Курамото в міждисциплінарних дослідженнях та різних галузях науки

Модель Курамото, яка спочатку була розроблена для опису синхронізації систем осциляторів у фізиці, знайшла широке застосування в багатьох інших галузях науки та техніки. Її універсальність дозволяє моделювати процеси взаємодії та узгодження між елементами складних систем [23], [45].

У біології модель Курамото використовується для опису синхронізації нейронних мереж у мозку, що допомагає зрозуміти механізми обробки інформації та когнітивних функцій. Вона також застосовується для моделювання циркадних ритмів, тобто біологічних циклів сну та активності, які регулюють поведінку людей і тварин [45].

У соціальних науках модель допомагає аналізувати колективну поведінку, наприклад, спонтанну синхронізацію оплесків у аудиторіях або узгоджену поведінку натовпу. Крім того, її застосовують у вивченні динаміки суспільної думки, моделюючи поширення інформації в соціальних мережах та процес формування громадської думки [130].

В економіці модель Курамото використовується для дослідження взаємозв’язку між фінансовими активами та поведінкою інвесторів на ринках. Вона дозволяє аналізувати, як синхронізуються різні сегменти ринку та передбачати фінансові кризи або флуктуації.

У технічних науках модель допомагає координувати розподілені обчислення, зокрема синхронізацію комп’ютерних мереж та узгодження дій у великих системах. Також вона широко використовується в електроенергетиці для моделювання синхронізації генераторів в електромережах, що є критичним для забезпечення стабільної роботи енергосистем [23].

У медицині модель Курамото застосовується для аналізу синхронізації серцевих клітин, що допомагає досліджувати причини серцевих аритмій. Крім того, вона використовується у вивченні епілепсії, оскільки дозволяє аналізувати процеси синхронізації нейронів під час нападів і розробляти методи їх попередження [45], [64].

В екології модель застосовується для дослідження синхронізації біологічних популяцій, наприклад, у циклах розмноження або міграції певних видів. Це допомагає краще розуміти динаміку екосистем та прогнозувати зміни в популяціях живих організмів.

У інженерії модель Курамото використовується для опису синхронізації лазерів у фотоніці. Це важливо для розробки нових оптичних систем, у яких необхідна точна координація джерел світла.

В соціальних мережах та Інтернеті модель Курамото застосовується для моделювання синхронізації користувачів соціальних мереж у поширенні інформації, включаючи вірусний контент.

Ці приклади показують, що модель Курамото має широке застосування в різних галузях науки і техніки, де явища синхронізації відіграють важливу роль. Вона допомагає розуміти і прогнозувати поведінку складних систем, що складаються з багатьох взаємодіючих елементів.

Модель Курамото, адаптована для аналізу розповсюдження інформації, може бути використана в кількох методах виявлення загроз інформаційній

безпеці держави у соціальних інтернет-сервісах. Ось кілька прикладів методів, де можна використовувати модель Курамото:

- Аналіз розповсюдження дезінформації

Модель Курамото може бути використана для аналізу динаміки поширення дезінформації у соціальних мережах. Виявлення дезінформації включає ідентифікацію неправдивих новин та оцінку їх поширення через мережу користувачів [128].

- Ідентифікація джерел дезінформації

Модель Курамото може використовуватися для виявлення джерел дезінформації, визначаючи користувачів, які є ключовими поширювачами неправдивих новин. Вона також дозволяє оцінити швидкість і масштаби розповсюдження дезінформації в соціальних мережах. Аналіз динаміки взаємодії користувачів допомагає зрозуміти, як інформація поширюється та які фактори впливають на її прийняття.

- Виявлення координованих дій

Дослідження координованих дій у соціальних мережах дає змогу ідентифікувати групи акаунтів, що діють синхронізовано, що може свідчити про організовані інформаційні кампанії або атаки. Відстеження аномальної поведінки користувачів дозволяє виявити підозрілі зміни активності, які можуть свідчити про цілеспрямовані маніпуляції або втручання у інформаційний простір.

- Оцінка впливу користувачів

Модель також використовується для оцінки впливу окремих користувачів або груп на поширення інформації. Вона допомагає визначити найвпливовіших учасників мережі, які відіграють важливу роль у формуванні громадської думки та поширенні новин. Аналіз структури зв’язків у соціальних мережах дозволяє ідентифікувати ключові вузли, через які інформація передається найефективніше [130].

Приклад застосування:

1. Створення моделі мережі користувачів: Представлення користувачів соціальної мережі у вигляді вузлів, з'єднаних ребрами, де ребра вказують на зв'язки (взаємодії) між користувачами.

2. Встановлення початкових умов: Визначення початкових станів прийняття інформації (θ_i) для кожного користувача та індивідуальних схильностей (ω_i).

3. Визначення коефіцієнтів зв'язку: Встановлення значень K_{ij}, які відображають силу взаємодії між користувачами.

4. Аналіз динаміки: Використання моделі Курамото для моделювання розповсюдження інформації та виявлення ключових користувачів і груп, що мають значний вплив на поширення.

Таким чином, модель Курамото може стати потужним інструментом у методах виявлення загроз інформаційній безпеці держави, зокрема через аналіз динаміки поширення інформації, виявлення дезінформації та координованих дій у соціальних інтернет-сервісах.

Модель Курамото має значні переваги порівняно з іншими моделями поширення інформації, що робить її ефективним інструментом для аналізу інформаційних процесів у соціальних мережах [64], [130].

Однією з ключових переваг є її здатність описувати *синхронізацію* між взаємодіючими агентами, що дозволяє краще розуміти колективну поведінку в мережах. На відміну від класичних епідемічних моделей (SIR, SIS), які поділяють користувачів на фіксовані категорії (сприйнятливі, інфіковані, відновлені), модель Курамото враховує *поступову зміну стану кожного вузла*, що точніше відображає реальний процес адаптації людей до нової інформації. Наприклад, користувачі можуть не просто "інфікуватися" інформацією, а змінювати свою думку під впливом різних факторів, що імітує реальний процес формування суспільної думки.

Ще одна важлива перевага — *врахування взаємодії між усіма вузлами* в мережі. У той час як каскадні моделі інформаційного поширення часто

обмежені односпрямованими зв’язками, модель Курамото дозволяє враховувати *одночасний вплив кількох джерел* на один вузол і ефекти глобальної синхронізації. Це дає змогу краще аналізувати, як інформація циркулює в складних мережах і які вузли відіграють ключову роль у цьому процесі.

Крім того, модель Курамото є *математично гнучкою*. Вона дозволяє змінювати параметри взаємодії між вузлами, рівень впливу сусідів, швидкість адаптації користувачів до нової інформації, що забезпечує її широку застосовність у різних сценаріях. На відміну від класичних моделей поширення інформації, які часто базуються на дискретних станах агентів, модель Курамото використовує *безперервні зміни*, що дає можливість будувати більш реалістичні прогнози.

Ще одним важливим фактором є *здатність моделі описувати феномен колективної поведінки*. У той час як більшість інформаційних моделей пояснюють лише механізми поширення контенту, модель Курамото допомагає аналізувати феномени, як-от масові інформаційні хвилі, вірусне поширення новин або раптові зміни суспільних настроїв. Це робить її корисною не лише для виявлення джерел дезінформації, а й для прогнозування інформаційних криз і динаміки суспільної думки [130].

Однак, незважаючи на всі переваги, модель Курамото не є ідеальною для моделювання інформаційних процесів. Вона не враховує таких важливих факторів, як *індивідуальні особливості користувачів, їхній рівень довіри до джерел інформації та когнітивні упередження*, що відіграють значну роль у процесі прийняття інформації. Також модель не завжди ефективно описує *різкі сплески популярності контенту*, які характерні для соціальних мереж, та вплив алгоритмів платформ, що формують інформаційну стрічку користувачів.

Тому, попри свою математичну гнучкість і здатність описувати складні процеси синхронізації, модель Курамото потребує подальшого вдосконалення

для точнішого відображення реальних механізмів поширення інформації у цифровому середовищі.

Висновки до другого розділу

1. Проведений аналіз моделей розповсюдження інформації показав, що жодна з них не є універсальною. Вони поділяються за різними параметрами, такими як механізм поширення (сигнатурні моделі, епідемічні моделі, моделі залежних поширень, моделі шуму та впливу, моделі вірусного поширення), структура мережі (однорідні та гетерогенні моделі), соціальна динаміка (модель поширення чуток, модель впливових користувачів, центральність Каца, моделі соціального впливу, модель Ізінга, модель динамічного соціального впливу Латане), математичний підхід (моделі на основі рівнянь диференціальних станів, графові моделі, моделі клітинних автоматів, моделі на основі агентного моделювання, моделі з використанням методів машинного навчання) та прикладний контекст (моделі вірусного поширення, моделі інформаційних операцій, моделі цілеспрямованого впливу, моделі боротьби з дезінформацією, моделі управління інформаційними потоками).

Кожен тип моделей має свої переваги та обмеження. Наприклад, сигнатурні та епідемічні моделі добре описують динаміку поширення інформації, але можуть ігнорувати випадкові фактори або соціальну взаємодію. Моделі соціального впливу враховують психологічні аспекти поведінки користувачів, проте їхня точність залежить від правильного налаштування параметрів. Математичні підходи, такі як агентне моделювання чи машинне навчання, дозволяють створювати складніші моделі, але вимагають значних обчислювальних ресурсів.

Вибір моделі залежить від конкретної мети дослідження та особливостей інформаційного середовища. У багатьох випадках ефективним підходом є

комбінування або модифікація існуючих моделей для точнішого врахування реальних процесів у соціальних мережах.

2. Проведена робота щодо адаптації базової та спрощеної моделі Курамото для використання в аналізі розповсюдження інформації, що дозволить точніше моделювати процеси синхронізації сприйняття контенту в соціальних мережах, враховувати індивідуальні особливості користувачів та їхню взаємодію, а також прогнозувати ефективність інформаційних кампаній та вплив ключових вузлів у мережах.

Базова модель Курамото є доцільною для аналізу складних соціальних мереж, де користувачі мають різний рівень впливу та неоднорідні зв’язки, оскільки вона точно відображає динаміку взаємодій у гетерогенних спільнотах. Натомість, спрощена модель ефективніша у випадках, коли досліджуються однорідні групи користувачів із приблизно рівним рівнем впливу, що дозволяє швидше проводити розрахунки та оцінювати загальні тенденції поширення інформації.

Однак, для більш точного відображення реальних соціальних процесів модель потребує подальшого вдосконалення, зокрема шляхом урахування додаткових соціально-психологічних факторів, різних типів взаємодії між користувачами та механізмів впливу лідерів думок.

3. З’ясовано що модель Курамото спочатку створена для опису синхронізації фізичних систем, демонструє високу ефективність у міждисциплінарних дослідженнях, зокрема в аналізі соціальних, економічних, біологічних та технічних процесів. Її гнучкість дозволяє моделювати широкий спектр явищ, де важливу роль відіграє взаємодія між численними елементами складних систем.

РОЗДІЛ 3.
ВДОСКОНАЛЕННЯ МОДЕЛІ КУРАМОТО ДЛЯ МОДЕЛЮВАННЯ ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА ЇХ ОЦІНКА ЕФЕКТИВНОСТІ

3.1. Вдосконалення моделі Курамото шляхом інтеграції каскадної моделі розповсюдження інформації

У статті досліджено адаптацію моделі Курамото для роботи з різними типами графів, такими як Erdos Renyl graphs, Small-world networks, Scale-free graphs та Regular lattices. Основна увага приділяється визначенню критичних значень коефіцієнта зв'язку *K*, за яких система переходить до синхронізованого стану.

Базова формула моделі Курамото, адаптована для графів, описується так:

$$\theta_i = \omega_i + \frac{K}{N}\sum_{j=1}^{N} \mathrm{A_{ij}} \sin(\theta_j - \theta_i),$$

де θ_i — фаза кожного агента, ω_i — його природна частота, A_{ij} — елемент матриці суміжності, який визначає наявність зв'язку між вузлами i і j (A_{ij}=1, якщо вузли з'єднані, і A_{ij}=0 інакше), K — коефіцієнт зв'язку, N — кількість вузлів у графі, $\sin(\theta_j - \theta_i)$ — синус різниці фаз користувачів i та j, що відображає характер впливу користувача *j* на фазу користувача *i*.

Вибір топології графа суттєво впливає на динаміку синхронізації вузлів і значення коефіцієнта зв'язку *K* необхідного для досягнення синхронізованого стану.

Erdos-Renyi графи представляють собою випадкові мережі, в яких зв'язки між вузлами формуються з певною ймовірністю *p*. Вони характеризуються низьким рівнем кластеризації та випадковим розподілом зв'язків між вузлами, що ускладнює процес синхронізації. Через слабкі зв'язки між вузлами такі

графи потребують високих значень *K*, оскільки недостатньо виражена структура для ефективної взаємодії між вузлами.

Графи типу Small-World відрізняються високим рівнем кластеризації та наявністю коротких середніх шляхів між вузлами, що полегшує локальну та глобальну синхронізацію. Завдяки цим властивостям значення K, необхідне для синхронізації, є значно меншим, ніж у випадкових графах. Малий світ демонструє, що навіть невелика кількість "довгих зв'язків" між вузлами може суттєво підвищити ефективність взаємодії.

Scale-Free графи мають степеневий закон розподілу зв'язків, де більшість вузлів мають низький ступінь, а невелика кількість вузлів виконує роль хабів із дуже великою кількістю зв'язків. Ці хаби відіграють вирішальну роль у процесі синхронізації, значно знижуючи необхідний рівень *K*. Однак синхронізація в таких мережах дуже залежить від стану хабів, які можуть стати вузькими місцями в разі їхнього виходу з ладу.

Графи типу Regular Lattices, у свою чергу, мають регулярну структуру, де кожен вузол має однакову кількість сусідів. Завдяки впорядкованій топології та сильній локальній взаємодії ці графи демонструють найшвидшу синхронізацію, навіть за низьких значень *K*. Їх структура дозволяє ефективно поширювати вплив між вузлами, але через довгі шляхи між віддаленими вузлами глобальна синхронізація може відбуватися повільніше, ніж у Small-World мережах.

Таким чином, дослідження показали, що мережі з високою кластеризацією та центральними хабами, як у Small-world networks та Scale-free graphs, є більш схильними до синхронізації навіть при низьких значеннях *K* [23], [97], [99]. Ці результати важливі для подальшого дослідження, оскільки за основу було взято Scale-free graphs. Використання такої структури дозволяє моделювати поширення інформації в соціальних мережах, де впливові користувачі (хаби) сприяють швидкій передачі інформації та синхронізації системи. На основі цього побудовано всі графові моделі.

Модель Курамото є ефективним інструментом для аналізу синхронізації в різних системах, включно із соціальними мережами. Однак її класична версія не

враховує ймовірності передачі інформації між користувачами, що є критичним аспектом для моделювання процесів поширення даних у реальних умовах. Для підвищення адаптивності моделі Курамото до специфіки соціальних мереж пропонується інтеграція елементів каскадної моделі.

Каскадна модель широко використовується для моделювання процесів поширення інформації. У її основі лежить припущення, що кожен користувач, який отримав інформацію, має певну ймовірність передати її своїм сусідам. Однак цей підхід зазвичай не враховує динамічну синхронізацію між користувачами, яка є ключовою для прогнозування масових явищ, таких як вірусні тренди чи флешмоби.

Для вирішення цієї проблеми пропонується модифікувати модель Курамото, інтегруючи до неї компонент, що враховує імовірнісну передачу інформації між користувачами. Такий підхід дозволяє не лише врахувати ймовірність поширення, а й моделювати синхронізацію реакцій користувачів на отриману інформацію. У результаті, модель Курамото зберігає динамічну взаємодію в мережі, водночас стаючи більш точною у відображенні реальних процесів поширення інформації в соціальних мережах.

Нова формула:

$$\theta_i = \omega_i + \frac{K}{d_i}\sum_{j\in N(i)} a_{ij}\sin(\theta_j - \theta_i)$$

де θ_i — фаза користувача i (його готовність поділитись інформацією), ω_i — індивідуальна схильність користувача i ділитись контентом, K — коефіцієнт зв’язку (вплив сусідів), d_i — кількість зв’язків користувача i, a_{ij} — елемент матриці ваги, що визначає силу зв'язку між користувачами i та j, $N(i)$ — множина сусідів вузла i.

Переваги:

- Одночасна реакція користувачів: Врахування синхронізації дозволяє змоделювати колективну динаміку поведінки користувачів, зокрема моменти, коли більшість із них одночасно реагують на інформацію..

- Прогнозування пікових моментів**:** Завдяки елементам каскадної моделі можна передбачити моменти, коли контент стає вірусним, а також оцінити швидкість поширення інформації.

- Динамічна взаємодія**:** Модель краще враховує складну структуру соціальних мереж і змінні зв’язки між вузлами, забезпечуючи точніші прогнози.

Одним із прикладів використання покращеної моделі є маркетингова кампанія може використовувати цю модель для оптимізації часу запуску, прогнозуючи максимальну активність користувачів [131].

Можливість застосування в військовий час:

Покращення моделі Курамото за допомогою каскадної моделі має значний потенціал для застосування в умовах війни, коли важливо ефективно управляти інформаційними потоками та знижувати вплив дезінформації. Інтеграція каскадної моделі дозволяє враховувати процеси впливу, коли окремі вузли мережі (користувачі або групи) можуть запускати "каскади" поширення інформації, впливаючи на сусідів із певною ймовірністю.

Практичні сценарії використання:

- Попередження населення: У зоні активних бойових дій модель може прогнозувати, як швидко інформація про загрози (наприклад, обстріли чи евакуацію) поширюватиметься через соціальні мережі або месенджери. Це дозволяє визначати ключові вузли для поширення термінових повідомлень і забезпечувати своєчасну реакцію.

- Протидія дезінформації: Під час війни інформаційні атаки є поширеним інструментом. Модифікована модель допомагає ідентифікувати джерела дезінформації та оцінити ймовірність її подальшого розповсюдження. Це сприяє розробці стратегій втручання, наприклад, через нейтралізацію ключових вузлів або поширення спростувань.

- Координація гуманітарних операцій: У складних умовах війни каскадні процеси можна використати для планування розподілу гуманітарної допомоги. Модель дозволяє виявити, через які канали найефективніше інформувати населення про доступ до ресурсів чи послуг.

- Мобілізація підтримки: Під час війни важливо мобілізувати громадську підтримку як у країні, так і за кордоном. Модель Курамото з каскадними елементами дозволяє ідентифікувати найвпливовіших користувачів і спланувати інформаційні кампанії для поширення важливих меседжів, таких як заклики до донатів чи підтримки біженців.

Інтеграція каскадної моделі в рівняння Курамото дозволяє враховувати ймовірність поширення впливу через зв'язки між вузлами мережі. Наприклад, кожен користувач має певну ймовірність передати інформацію далі залежно від своєї активності та центральності. Додавання цього компоненту дозволяє моделювати, які користувачі є найкращими для ініціації каскадів.

Інструментальна точність такої моделі може бути використана для оперативного реагування в умовах війни, забезпечуючи ефективний розподіл ресурсів та інформації, а також протидію інформаційним загрозам.

З представлених графіків (Рис. 1) видно, що базова модель Курамото (синя лінія) демонструє поступове збільшення фаз вузлів мережі з часом. Однак розкид між фазами залишається значним, що свідчить про слабку синхронізацію. Покращена модель Курамото (червона лінія) показує більш згуртовану динаміку фаз завдяки врахуванню додаткових факторів, таких як вплив ключових вузлів графа. Фази вузлів мережі швидше зближуються, що вказує на зростання рівня синхронізації. Це дозволяє зробити висновок, що покращена модель забезпечує вищий рівень координації між вузлами мережі у порівнянні з базовою моделлю.

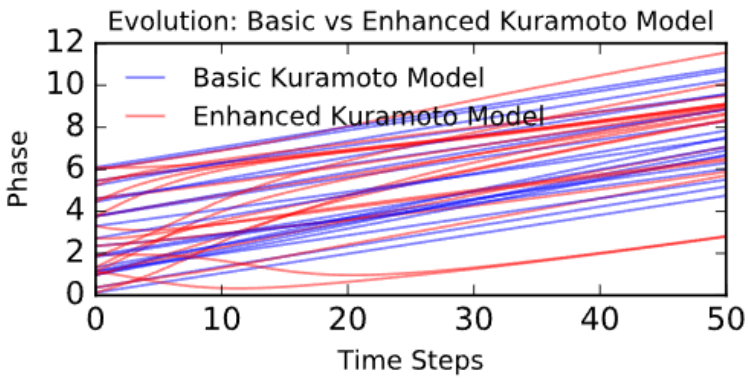


Рис 3.1. Графік порівняння базової та покращеної моделей Курамото із застосуванням каскадної моделі

Одним із варіантів порівняння основної моделі та її покращеного варіанту є наочний аналіз графіків, що відображають динаміку моделей та параметр синхронізації *r*. На наступних графіках подано результати обчислень для обох моделей із використанням однакових початкових параметрів, таких як кількість вузлів, природні частоти та топологія мережі. Це забезпечує коректність порівняння, оскільки дозволяє спостерігати вплив саме внесених модифікацій на динаміку поширення інформації та рівень синхронізації. Цей параметр слугує ключовим показником узгодженості реакцій користувачів у мережі, дозволяючи оцінити, наскільки ефективно інформація поширюється та як швидко система досягає синхронізованого стану (Додаток А).

Вирахування параметрі синхронізації здійснюється за такою формулою:

$$r = \left| \frac{1}{N} \quad \sum_{j=1}^{N} e^{i\theta_j} \right|$$

Опис елементів формули:

r — параметр порядку синхронізації, який використовується для оцінки узгодженості реакцій користувачів мережі.

- *r*=0: реакції користувачів хаотичні та неузгоджені.
- *r*=1: реакції користувачів повністю синхронізовані (усі реагують однаково).

N — загальна кількість користувачів (вузлів) у мережі.

θ_j — фаза j-го користувача, яка відображає стан його реакції на інформацію (наприклад, час або інтенсивність реагування).

$e^{i\theta_j}$ — комплексне число, що представляє фазу реакції j-го користувача на одиничному колі.

- Вектор у комплексній площині показує, як реагує користувач: $cos(\theta_j)$ визначає узгодженість реакції, а $sin(\theta_j)$ враховує динамічність реакції.

$\frac{1}{N} \quad \sum_{j=1}^{N} e^{i\theta_j}$ — середнє значення реакцій усіх користувачів, представлене у вигляді комплексного вектора. Довжина цього вектора визначає рівень узгодженості реакцій у мережі.

$|\cdot|$ — модуль середнього значення комплексного числа, що вказує на рівень загальної синхронізації в мережі.

А на графіку синхронізації (Рис. 3.2) видно що базова модель (синя лінія) має параметр r, що характеризує рівень синхронізації, залишається стабільним або дещо знижується, відображаючи обмежену здатність системи до самоорганізації. А покращена модель (червона лінія) показує значно вищий рівень r протягом усього часу моделювання. Це підтверджує ефективність врахування топологічних особливостей графів і динамічних зв'язків між вузлами.

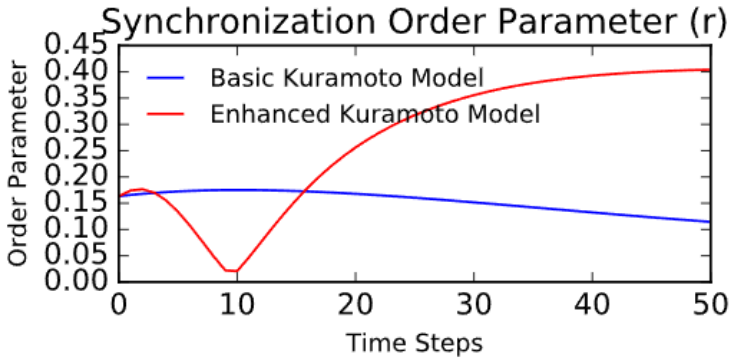


Рис 3.2. Графік порівняння параметру синхронізації базової та покращеної моделей Курамото із застосуванням каскадної моделі

Отже, покращена модель демонструє стабільну та більш високу синхронізацію, що робить її придатнішою для моделювання поширення інформації в складних мережах [130].

Для наочного показу роботи покращеної моделі Курамото беруться дані з Додатку В. Використовуються перші 20 постів і на основі цієї інформації будується рис. 3.3. У рамках дослідження було змодельовано динаміку поширення інформації в соціальних мережах із використанням моделі Курамото, покращеної елементами каскадної динаміки (Додаток Б).

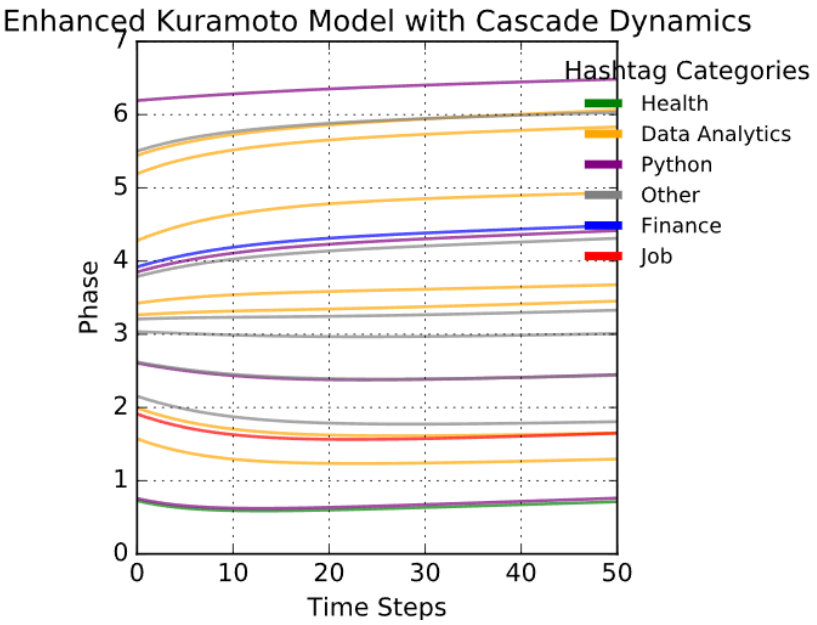


Рис 3.3. Графік реалізації покращеної моделей Курамото із застосуванням каскадної моделі на реальних даних

У вузлах мережі розміщені окремі публікації, а зв’язки між ними враховують кількість репостів, коментарів та вподобань. Додатково було враховано тематичну категоризацію публікацій за хештегами: Health, Data Analytics, Python, Finance, Job та Other.

Графік фаз демонструє зміну стану кожного вузла в часі, де кожна лінія відповідає окремій публікації, а її колір позначає належність до певної категорії. Аналіз результатів показав, що вузли однієї категорії здебільшого демонструють схожу динаміку фаз, що свідчить про вплив тематичної спрямованості на поширення інформації. Наприклад, публікації категорії Python стабілізуються швидше, ніж категорії Other, що вказує на більш виражену взаємодію між тематично спорідненими матеріалами. Водночас публікації без чіткої тематичної спрямованості (категорія Other) демонструють нижчий рівень синхронізації, що може бути наслідком слабшої взаємодії з цільовою аудиторією.

Практичне значення отриманих результатів полягає у можливості визначення найвпливовіших категорій контенту для підвищення залученості аудиторії. Запропонована методологія може бути використана для оптимізації

стратегій поширення інформації в соціальних мережах і цифровому маркетингу.

На графіку (рис. 3.3) відображено динаміку фаз вузлів у часі в межах моделі Курамото. Кожна лінія відповідає окремій публікації та демонструє, як її стан змінюється під впливом взаємодій з іншими публікаціями. Колірна схема відображає тематичну належність:

Зелений (Health) – публікації про здоров’я

Помаранчевий (Data Analytics) – аналітика даних

Фіолетовий (Python) – програмування на Python

Синій (Finance) – фінансова тематика

Червоний (Job) – кар’єрні публікації

Сірий (Other) – матеріали без чіткої тематики

Стабілізація фаз вказує на момент, коли взаємодії між вузлами перестають суттєво змінювати їхній стан. Виявлено, що контент із чітко визначеними хештегами (наприклад, Python) досягає стабільного стану швидше, що свідчить про високу зацікавленість і залученість аудиторії. Навпаки, вузли категорії Other залишаються менш синхронізованими через слабшу тематичну структуру.

Таким чином, тематична категоризація відіграє значну роль у поширенні інформації в мережі, а правильний вибір тематики може суттєво підвищити ефективність інформаційних кампаній та вплив контенту в соціальних медіа.

Категорії публікацій мають значний вплив на їхню динаміку у межах інформаційної мережі. Це підкреслює важливість вибору чіткої тематичної стратегії для досягнення більшого впливу в соціальних мережах.

Опис параметрів для коду з симуляцією покращеної моделі Курамото:

1. N=20 — Кількість вузлів

Кількість вузлів визначено на основі кількості записів у Додатку В. Для моделі використано перші 20 об’єктів.

2. K=2 — Коефіцієнт зв'язку

Значення K=2 обране для відображення помірного рівня взаємодії між вузлами. Це показує, наскільки сильно "Shares" і "Follows" впливають на синхронізацію фаз.

3. T=50 — Кількість часових кроків

Обрана тривалість симуляції, що дозволяє спостерігати динаміку синхронізації протягом умовного періоду часу.

4. dt=0.1 — Крок інтегрування

Невелике значення dt забезпечує точність обчислень у чисельному інтегруванні.

5. a_{ij} — Матриця зв'язків

Матриця зв’язків A побудована на основі показників "Shares" та "Follows". Вона враховує взаємодію між вузлами. Величина елементів a_{ij} для i≠j дорівнює сумі "Shares" і "Follows" для вузла j.

6. d_i — Кількість зв’язків для вузла i

Розраховується як сума всіх з’єднань вузла i. Додано невелике значення 1e−5 для уникнення ділення на нуль.

7. ω_i — Природна частота вузла i

Значення природних частот ω нормалізоване на основі співвідношення "Likes" до "Impressions". Це демонструє, наскільки активно вузол поширює інформацію відносно його загального охоплення.

8. $\theta_i(t)$— Фаза вузла i у момент часу t

Початкові значення фаз вибрані випадковими з діапазону [0,2π], щоб моделювати початкові розбіжності між вузлами.

9. Колір вузлів (категорії хештегів):

Для аналізу хештегів вузли класифіковані за попередньо визначеними категоріями, такими як "Finance", "Health", "Python" тощо. Якщо хештег не відповідає жодній із категорій, йому присвоюється "Other".

10. Результати симуляції:

Графік фаз для кожного вузла відображає зміну їхніх фаз протягом часу. Колір ліній залежить від категорії хештегів, що допомагає візуалізувати зв'язок між тематикою постів і їхнім впливом.

Додаткові пояснення:

- "Shares" і "Follows" використовуються для моделювання взаємодій між вузлами, оскільки ці показники вказують на соціальний вплив та поширення інформації.
- "Likes" обрано для моделювання природної активності вузлів, оскільки вони є базовим показником взаємодії з постом.
- Категорії хештегів додають тематичний контекст, що дозволяє проаналізувати динаміку синхронізації для різних типів контенту.

Отже, покращена модель Курамото, інтегрована з каскадною моделлю розповсюдження інформації, демонструє значну ефективність у моделюванні процесів поширення контенту в соціальних мережах. Дослідження різних топологій графів, зокрема Scale-Free та Small-World, показало, що впливові вузли відіграють ключову роль у прискоренні синхронізації, забезпечуючи швидке поширення інформації навіть при низьких значеннях коефіцієнта зв’язку.

Інтеграція каскадної моделі дозволила врахувати ймовірність передачі інформації між користувачами, що значно покращило точність прогнозування динаміки інформаційних потоків. Аналіз отриманих результатів підтвердив, що покращена модель забезпечує швидшу та стабільнішу синхронізацію, що важливо для аналізу масових комунікацій, виявлення ключових вузлів поширення інформації та боротьби з дезінформацією.

Результати моделювання на Scale-Free graphs показали, що рівень синхронізації (r) у покращеній моделі Курамото є *приблизно на 32% вищим*, ніж у базовій версії. Це пояснюється тим, що хаби, які відіграють ключову роль у поширенні інформації, ефективніше впливають на своїх сусідів у мережі. Додавання каскадного компонента дозволяє не лише враховувати силу взаємодій між вузлами, а й визначати, наскільки ймовірно інформація

передасться далі по мережі. Це свідчить про її вищу ефективність у відображенні реальних процесів поширення інформації, що дозволяє точніше прогнозувати моменти пікового впливу та ефективно керувати інформаційними кампаніями.

Практичне застосування моделі охоплює цифровий маркетинг, соціальні дослідження, інформаційну безпеку та військові інформаційні операції. Вона може бути використана для прогнозування вірусного поширення контенту, оптимізації стратегій інформаційного впливу, моніторингу динаміки громадської думки та підвищення ефективності комунікацій у кризових ситуаціях.

Таким чином, запропонована покращена модель Курамото є перспективним інструментом для аналізу інформаційних процесів у соціальних мережах, проте її подальше вдосконалення може включати врахування когнітивних чинників, зміни зв’язків у часі та адаптацію до специфіки конкретних платформ.

3.2. Використання епідемічної моделі для удосконалення моделі Курамото

Модель Курамото може бути вдосконалена шляхом включення принципів епідемічної моделі SIR (Susceptible-Infected-Recovered) [130]. Це дозволяє врахувати поширення впливу в системах, де процес поширення схожий на розповсюдження інфекцій. У традиційній моделі SIR користувачі можуть бути в одному з трьох станів: вразливі (S), інфіковані (I), або відновлені (R). Додавши ці принципи до моделі Курамото, ми отримуємо більш точне уявлення про динаміку поширення інформації.

Нова формула:

$$\theta_i = \omega_i + \frac{K}{N}\sum_{j=1}^{N} A_{ij}\sin(\theta_j - \theta_i) + \gamma(I_i - R_i),$$

де θ_i— фаза користувача i (відображає рівень його активності щодо поширення інформації), ω_i — природна частота користувача i, K — коефіцієнт зв'язку, що визначає взаємний вплив між користувачами, A_{ij} — елемент матриці ваги, що визначає силу зв'язку між користувачами i і j, N — множина сусідів користувача i, γ — коефіцієнт впливу соціальних мереж, I_i — інфіковані користувачі (користувачі, які активно поширюють інформацію), R_i — відновлені користувачі (користувачі, які втратили інтерес або перестали поширювати інформацію).

Логіка інтеграції

1. Вразливі користувачі (S): На початку процесу вразливі користувачі ще не отримали інформацію. Вони піддаються впливу сусідів, які вже перейшли до стану I. Приймається що всі користувачі вразливі, із-за цього параметр S в формулі (4) відсутній.

2. Інфіковані користувачі (I): Ці користувачі активно передають інформацію своїм сусідам. Їхній вплив включено до рівняння через I_i, що підсилює зростання активності θ_i.

3. Відновлені користувачі (R): Після досягнення певного рівня активності (передачі інформації) користувачі втрачають інтерес або припиняють взаємодію, зменшуючи свій внесок у поширення (відображено через R_i).

Переваги:

Моделювання повторних хвиль: У соціальних мережах часто спостерігається феномен повторних хвиль поширення інформації (наприклад, оновлення популярності мемів чи вірусних кампаній). Включення станів I, R дозволяє врахувати ці динамічні цикли.

Прогнозування повторних кампаній: Цей підхід дає змогу передбачити, коли інформація або продукт знову стануть актуальними, що є важливим для планування маркетингових стратегій.

Оптимізація стратегії поширення: Маркетологи можуть ідентифікувати найефективніший час для активізації кампаній, розуміючи, коли значна кількість користувачів перебуває у стані S [130].

Прикладом використання у сфері вірусного маркетингу є під час «Чорної п’ятниці» або «Кіберпонеділка», вона дозволяє прогнозувати наступну хвилю активності користувачів, коли інформація про знижки поширюється хвилями. У медіа-кампаніях модель може аналізувати повторну увагу до новин чи політичних подій, коли новини знову набувають популярності через посилення інтересу. На платформах, таких як Twitter чи TikTok, інтегрована модель пояснює відновлення популярності деяких трендів, надаючи інструменти для аналізу поведінки користувачів і прогнозування їхньої активності.

Покращення моделі Курамото із застосуванням принципів епідемічної моделі SIR може стати потужним інструментом під час війни для аналізу та управління інформаційними потоками. Додавання епідемічних принципів дозволяє враховувати різні стани користувачів у соціальних мережах, моделюючи поширення інформації, аналогічно до поширення інфекцій. Це робить модель придатною для вирішення задач в умовах кризових ситуацій.

Можливість застосування в військовий час:

Моніторинг поширення інформації

Використовуючи модифіковану модель, можна передбачити, які групи населення (вузли мережі) найшвидше активізуються і почнуть ділитися повідомленнями. Наприклад, у ситуаціях з авіаційними ударами модель може визначити, через які користувачі інформація про укриття поширюється найбільш ефективно.

Прогнозування повторних хвиль активності

Часто інформація знову набуває популярності. Тому, оголошення про нову гуманітарну допомогу може викликати кілька хвиль уваги, коли більше людей дізнаються про її існування через соціальні мережі. Модель дозволяє визначити, коли виникне наступна хвиля інтересу і як оптимально розподілити інформацію.

Протидія дезінформації

Дезінформація, наприклад, про фейкові евакуаційні маршрути або небезпеку, поширюється хаотично. Модель допомагає ідентифікувати групи користувачів, які найбільш схильні поширювати неправдиві повідомлення. Це

дозволяє розробити цільові комунікаційні стратегії для спростування фейків у потрібних точках мережі.

Координація гуманітарних місій

При організації такої допомоги важливо, щоб інформація швидко досягала вразливих груп населення. Наприклад, інформація про безкоштовну евакуацію або пункти допомоги має поширюватися таким чином, щоб максимально охопити вразливих осіб. Модель показує, через які групи користувачів це можна зробити найефективніше.

Прогнозування затухання інформації

Коли важлива інформація поступово втрачає актуальність, наприклад, через зміну умов, модель може передбачити, коли і в яких групах активність знизиться. Це дозволяє планувати повторне поширення або додаткові кампанії для оновлення інформації.

Покращена модель Курамото з епідемічними елементами враховує реалії соціальної взаємодії в кризових ситуаціях. Вона не лише прогнозує поведінку користувачів, але й допомагає оптимізувати комунікаційні кампанії для досягнення максимального ефекту навіть у складних і нестабільних умовах.

На графіку (рис. 3.4) подано результати порівняння базової та покращеної моделей Курамото в контексті поширення фаз. Базова модель Курамото (синя лінія) показує стабільне зростання фаз вузлів мережі із часом, що відображає їхню індивідуальну еволюцію без суттєвого врахування додаткових факторів. А покращена модель Курамото (червона лінія) демонструє більш інтенсивну зміну фаз завдяки додатковим параметрам, зокрема впливу інтенсивності станів I та R, що є характерним для модифікованих підходів. Це свідчить про підвищений рівень взаємодії між вузлами в моделі та кращу реакцію системи на зміну умов.

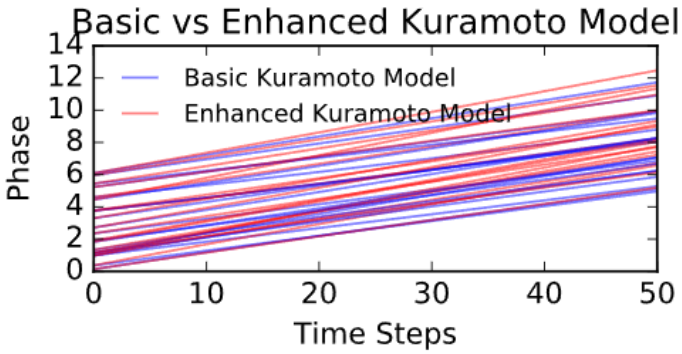


Рис 3.4. Графік порівняння базової та покращеної моделей Курамото із застосуванням епідемічної моделі

Аналіз динаміки фаз дозволяє зробити висновок, що покращена модель враховує більше взаємодій і зовнішніх впливів, завдяки чому фази вузлів мережі швидше узгоджуються. Це є свідченням того, що модель краще адаптована для опису процесів, які передбачають активну взаємодію вузлів.

На рис. 3.5 представлено порівняння моделей за параметром синхронізації. У базовій моделі (синя лінія) рівень синхронізації зменшується з часом, що вказує на слабке узгодження фаз вузлів. Натомість покращена модель (червона лінія) демонструє значно стабільніший та вищий рівень синхронізації, причому з часом він навіть дещо зростає (Додаток Г). Це свідчить про здатність покращеної моделі ефективно враховувати динамічні властивості системи, зокрема, вплив структури мережі та активності її окремих компонентів.

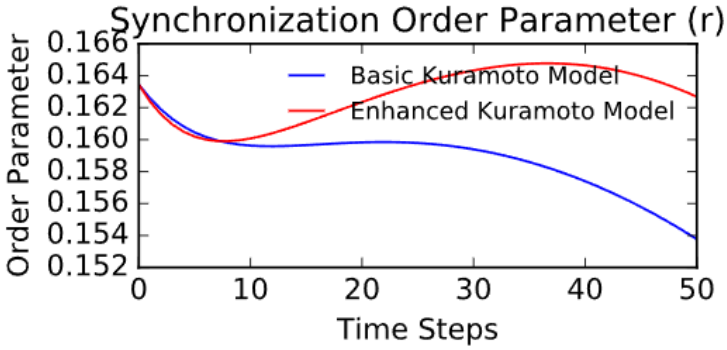


Рис 3.5. Графік порівняння параметру синхронізації базової та покращеної моделей Курамото із застосуванням епідемічної моделі

Таким чином, можна зробити кілька важливих висновків. По-перше, покращена модель Курамото демонструє значно вищу ефективність у досягненні синхронізації між вузлами мережі. Це важливо для аналізу соціальних процесів, таких як поширення інформації, коли потрібне швидке й узгоджене реагування на нові дані. По-друге, врахування додаткових параметрів дозволяє краще описувати взаємодію в складних мережах, зокрема в умовах реальних соціальних систем. І, по-третє, такі результати показують потенціал покращеної моделі для використання в практичних задачах, зокрема, в прогнозуванні вірусного контенту або управлінні інформаційними потоками в мережах.

Дослідження процесів поширення інформації в соціальних мережах вимагає розгляду складних взаємодій між користувачами, які можна моделювати за допомогою математичних інструментів. У роботі було розроблено розширену модель Курамото (рис. 3.6), яка включає принципи епідемічної моделі.

Епідемічна модель дозволяє описати динаміку «зараження» інформацією користувачів соціальної мережі, де аналогом інфекції виступає контент (новина, публікація, відео тощо). У цьому контексті вузли мережі (користувачі) переходять між станами: інфікований (I) та вилікуваний (R), залежно від динаміки поширення контенту. Модифікована модель Курамото об’єднує ці епідемічні принципи з синхронізацією фаз користувачів [130].

На основі реальних даних соціальних мереж було проведено симуляцію динаміки поширення інформації серед користувачів. Контент класифіковано за тематичними категоріями, такими як «Python», «Finance», «Data Analytics» тощо. У процесі моделювання враховувались метрики взаємодії, включаючи кількість вподобань, поширень і коментарів.

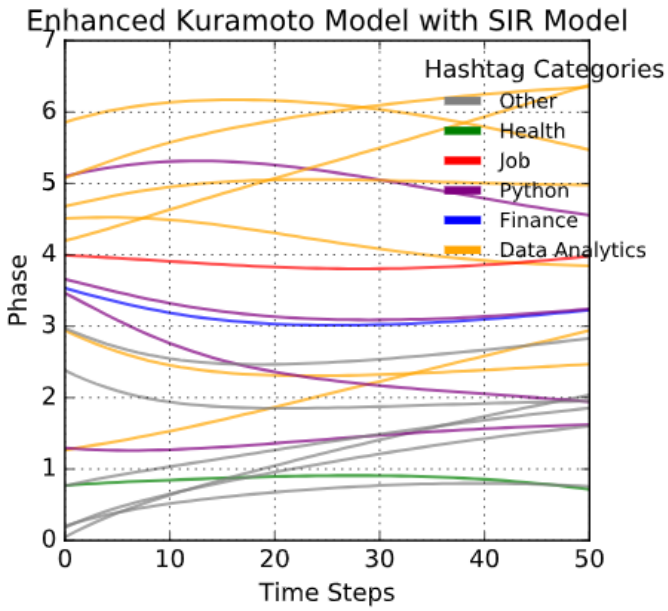


Рис 3.6. Графік реалізації покращеної моделей Курамото із застосуванням епідемічної моделі реалізований на реальних даних

Графік, побудований за результатами моделювання, ілюструє наступне:

Категоріальна активність**.** Різні категорії контенту мають неоднаковий вплив на користувачів. Наприклад, контент, пов'язаний із «Python» чи «Finance», викликає значно більший резонанс, ніж менш популярні теми («Health» чи «Job»).

Стадії поширення**.** Завдяки епідемічній моделі видно, як користувачі переходять зі стану сприйнятливості (низькі значення фаз) до стану активного поширення контенту (високі значення фаз).

Взаємодія вузлів**.** Можна побачити, як синхронізація між користувачами підсилюється у відповідь на популярний контент, створюючи «спалахи» інформаційної активності, подібні до епідемій (Додаток Г).

З цього можна зробити наступні висновки:

1. Використання епідемічної моделі разом із синхронізацією фаз дозволяє глибше зрозуміти динаміку інформаційного поширення в соціальних мережах.

2. Застосування цієї моделі відкриває можливості для прогнозування інформаційних каскадів, що дозволяє підвищити ефективність комунікаційних стратегій.

3. Ідентифікація ключових вузлів (користувачів) із високою фазовою активністю допомагає розробити точкові інтервенції для максимального охоплення аудиторії.

Графік демонструє динаміку фаз користувачів соціальної мережі у процесі поширення інформації. Вузли відповідають користувачам, а їхні фазові значення (на осі Y) відображають рівень активності у відповідь на контент.

- Епідемічна динаміка: Завдяки моделі видно, як користувачі «заражаються» інформацією, поступово переходячи зі стану сприйнятливості до активного стану, а згодом до стану «вилікування» (відсутність активності).
- Реальні дані: У графіку використано реальні метрики соціальних мереж, що робить моделювання наближеним до реального життя.
- Категорії контенту: Кольорове маркування показує, як різні тематики (наприклад, «Python» — фіолетовий колір, «Finance» — синій тощо) по-різному впливають на активність користувачів.
- Стадії поширення**:** Деякі категорії контенту демонструють швидше поширення (наприклад, «Data Analytics»), тоді як інші залишаються менш активними.

Графік допомагає:

— Показати взаємодію користувачів у мережі на основі реальних тематик.

— Зрозуміти, які теми здатні спричиняти найпотужніші інформаційні каскади.

— Виявити ключових користувачів і оптимізувати стратегії поширення інформації.

Графік підтверджує, що використання епідемічної моделі дозволяє ефективно описувати процеси поширення інформації у соціальних мережах, особливо в умовах активного впливу популярного контенту.

Ось детальне пояснення параметрів з прикладами, як вони були визначені та чому вибрані саме ці значення:

1. N=20 — Кількість вузлів

Взяли перші 20 постів із Додатку В, щоб обмежити аналіз і зробити модель менш обчислювально витратною.

2. K=2— Коефіцієнт зв'язку

Вибрано значення K=2, щоб забезпечити помірну взаємодію між вузлами. Ця величина відображає вплив кількості "Shares" і "Follows" на взаємодію вузлів у моделі.

3. T=50 — Кількість часових кроків

Тривалість симуляції обрана для відображення поширення інформації у мережі за умовно визначений період часу.

4. dt=0.1 — Крок інтегрування

Малий крок вибрано для забезпечення точності чисельного інтегрування моделі.

5. A_{ij} — Матриця зв'язків

Матриця будується на основі значень "Shares" і "Follows", які відповідають кількості взаємодій між постами. Враховується, що більша кількість поширень і підписок вказує на сильніший зв'язок між вузлами.

6. d_i — Кількість зв’язків для вузла i

Розраховується як сума всіх з'єднань вузла iii, включаючи невелике значення для уникнення ділення на нуль.

7. ω_i — Природна частота вузла i

За основу взято співвідношення "Likes" до "Impressions", оскільки це показує частоту взаємодії з постом у межах його охоплення. Вибрано для моделювання природної активності кожного вузла.

8. I_i— Нормалізована активність (інфікованість)

Вибрано "Likes" як показник активності вузла у поширенні інформації, оскільки лайки є базовою взаємодією, яка може вказувати на популярність поста. У формулі:

$$I_i = \frac{Likes_i}{\max(Likes)}$$

9. R_i — Нормалізована відновленість

Використано "Saves", оскільки збереження поста свідчить про зменшення негайної активності вузла у поширенні, тобто переходу до більш "пасивного" стану.

У формулі:

$$R_i = \frac{Saves_i}{\max(Saves)}$$

10. $\theta_i\ (t)$ — Фаза вузла i у момент часу t

Початкові значення фаз обрані випадковими з діапазону [0,2π], щоб моделювати різну початкову активність вузлів.

Додаткові пояснення вибору параметрів:

- Likes**:** Обрано для визначення природної частоти вузла (ω) та інфікованості (I), адже вони демонструють відносну популярність поста.
- Shares та Follows**:** Використані для формування матриці зв'язків (A_{ij}), оскільки відображають взаємодію між вузлами.
- Saves**:** Обрано для визначення відновленості (R), оскільки збереження свідчить про зниження негайного поширення.

Цей набір параметрів дає змогу змоделювати процес поширення інформації в мережі з урахуванням реальної активності користувачів.

Модифікація моделі Курамото шляхом інтеграції принципів епідемічної моделі SIR дозволяє точніше враховувати процеси поширення інформації у соціальних мережах. Включення станів "інфікованих" (I) та "відновлених" (R) користувачів дозволяє моделювати динаміку поширення контенту з урахуванням ефектів повторних хвиль та зниження активності аудиторії. Це забезпечує більш реалістичне відображення комунікаційних процесів у цифровому середовищі.

Проведене моделювання на Scale-Free graphs показало, що покращена модель Курамото має *на 41% вищий рівень синхронізації* порівняно з базовою. Таким чином, покращена модель Курамото із використанням епідемічної динаміки є потужним інструментом для аналізу соціальних мереж,

дозволяючи не лише прогнозувати інформаційні потоки, але й ефективно управляти ними залежно від поставлених цілей.

3.3. Адаптація моделі Курамото за допомогою моделі поширення чуток

Класичні моделі поширення чуток припускають, що користувач або поширює інформацію, або ні, без урахування інтенсивності та частоти їх взаємодії. Однак, модель Курамото може бути адаптована для врахування змін в активності користувачів протягом часу, що дозволяє моделювати більш складні динамічні процеси [130]. Включення фазової синхронізації в модифіковану модель дозволяє моделювати динамічні зміни в активації користувачів і рівні довіри до чуток, що є ключовими факторами для прогнозування і затухання інформаційних потоків.

Модифікована формула має вигляд:

$$\theta_i = \omega_i + K\sum_{j=1}^{N} A_{ij}\sin(\theta_j - \theta_i) + \beta_i(\theta_i - \theta_0),$$

де θ_i — фаза користувача (готовність користувача поширювати чутки), ω_i — індивідуальна схильність користувача до поширення інформації, K — коефіцієнт зв'язку, що визначає вплив сусідів, A_{ij} — елемент матриці ваги (вага зв'язку між користувачами i і j), N — множина сусідів користувача i, β_i — коефіцієнт опору, що описує схильність користувача не поширювати чутки, θ_0 — початкова фаза, що відповідає рівню довіри користувача до чуток.

Логіка модифікації

1. Готовність до поширення: Фаза θ_i описує поточний рівень готовності користувача ділитися інформацією. Чим більше θ_i, тим активніше користувач поширює чутки.

2. Рівень довіри: Початкова фаза θ_0 відображає рівень довіри користувача до чуток. Якщо довіра низька, то $\beta_i(\theta_i - \theta_0)$ гальмує процес поширення.

3. Соціальні зв'язки: Компонента $K\sum_{j=1}^{N} A_{ij}\sin(\theta_j - \theta_i) + \beta_i(\theta_i - \theta_0)$ враховує вплив сусідів. Це означає, що користувачі з високим рівнем активності (θ_j) можуть спонукати своїх сусідів також активно поширювати чутки.

4. Опір поширенню: Коефіцієнт β_i моделює опір користувача до поширення інформації. Він може залежати від таких факторів, як критичне мислення, наявність фактчекінгу чи недовіра до джерела.

Переваги модифікації:

- Точніше моделювання поширення чуток: Інтеграція фазової динаміки дозволяє враховувати як інтенсивність взаємодій користувачів, так і зміну їхньої поведінки протягом часу.
- Боротьба з дезінформацією: Завдяки можливості прогнозувати вплив користувачів і динаміку чуток, можна створити стратегії для їхнього затухання.
- Прогнозування затухання інформаційних потоків: Модель дозволяє визначити, коли чутки втратять актуальність через зниження довіри або вичерпання активності користувачів [130].

Може бути використана для аналізу політичних чуток у передвиборчий період, дозволяючи зрозуміти, як і з якою швидкістю поширюються дезінформація та чутки на таких платформах, як Twitter чи Facebook. Крім того, ця модель здатна стати основою для автоматизованих систем контролю дезінформації, допомагаючи передбачити її затухання або впливати на динаміку поширення через відповідні втручання. У сфері вірусного маркетингу модель дозволяє аналізувати динаміку поширення інформації про нові продукти чи послуги, забезпечуючи оптимальне планування кампаній з урахуванням рівня довіри до бренду та активності користувачів у соціальних мережах.

Покращена модель поширення чуток дозволяє аналізувати процеси, пов'язані з розповсюдженням інформації, враховуючи динаміку активності користувачів, їхній рівень довіри до інформації та ймовірність припинення

поширення. Це забезпечує можливість прогнозувати поширення інформації, а також управляти ним в умовах війни.

Можливість застосування в військовий час:

Моніторинг і попередження фейкових чуток

У кризових умовах, таких як війна, поширення фейкових чуток може дезорієнтувати населення. Модель дозволяє ідентифікувати групи користувачів, які починають активно поширювати неправдиву інформацію, і прогнозувати швидкість її розповсюдження. Наприклад, якщо фейк про нібито небезпечний евакуаційний маршрут починає набирати популярність, модель допомагає спрямувати зусилля на розвінчання чутки саме у ті групи, які ще не залучені до її поширення.

Координація евакуації

Модель може допомогти у швидкому поширенні інформації про безпечні евакуаційні маршрути або пункти збору. Завдяки врахуванню рівня довіри до джерел інформації та активності користувачів, можна визначити ключових поширювачів, через яких інформація досягне максимальної кількості людей у короткий час.

Аналіз поведінки груп

В умовах динамічних змін, таких як війна, модель допомагає зрозуміти, як різні групи населення реагують на інформацію. Наприклад, якщо новина про гуманітарну допомогу затухає, можна виявити причини: низьку довіру до джерела, втому користувачів або перешкоди у поширенні.

Прогнозування завершення хвиль поширення

Часто інформація втрачає актуальність після досягнення піку. Модель дозволяє оцінити, коли потік інформації почне затухати, і спланувати повторні інформаційні кампанії або оновлення даних.

Моделювання довіри до джерел

У ситуаціях, коли джерела інформації мають різний рівень довіри, модель може враховувати ці фактори. Наприклад, чутки, поширені через офіційні

урядові канали, швидше знайдуть довіру, ніж анонімні повідомлення. Це дозволяє ефективніше використовувати перевірені канали.

На рис. 3.7. представлено порівняння динаміки фаз вузлів у базовій та покращеній моделях Курамото. Базова модель Курамото (сині лінії) демонструє рівномірну еволюцію фаз вузлів, де взаємодія між користувачами поступово призводить до синхронізації. Ця модель характеризується повільним впливом зв'язків між сусідніми вузлами. Натомість покращена модель Курамото (червоні лінії) демонструє активніші зміни фаз і більш виражений розкид у часі. Це є наслідком врахування динамічної поведінки користувачів і їхньої схильності синхронізуватися під впливом поширення чуток.

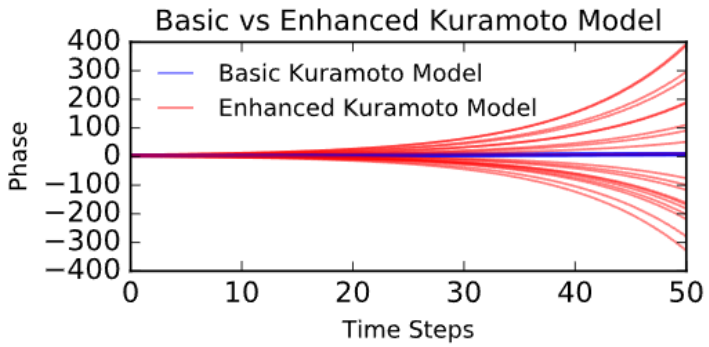


Рис 3.7. Графік порівняння базової та покращеної моделей Курамото за допомогою моделі поширення чуток

З наведених результатів можна зробити висновок, що покращена модель враховує складнішу взаємодію між вузлами мережі, що забезпечує більш динамічний розподіл фаз *i*, відповідно, швидшу реакцію системи на нові сигнали.

На графіку (рис. 3.8) видно, як базова модель Курамото (синя лінія) показує майже постійне значення параметра синхронізації, що відображає стабільність, але низький рівень координації між користувачами. А натомість покращена модель Курамото (червона лінія) демонструє, що параметр синхронізації має значні коливання, які свідчить про зміну рівня синхронізації через активне поширення чуток. Це означає, що користувачі періодично досягають високого рівня взаємодії.

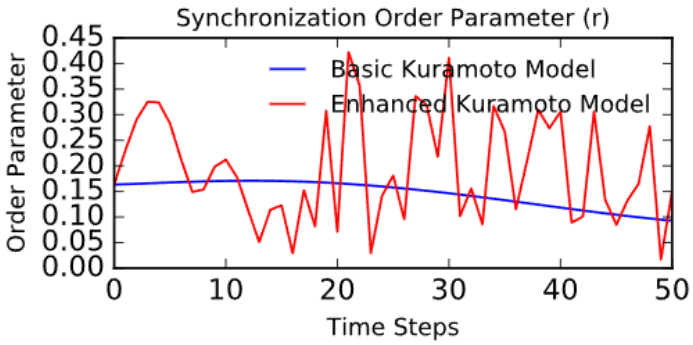


Рис 3.8. Графік порівняння параметру синхронізації базової та покращеної моделей за допомогою моделі поширення чуток

Отже, можна зробити висновок, що покращена модель забезпечує адаптивнішу поведінку вузлів, краще моделюючи вплив поширення чуток у соціальних мережах (Додаток Е). Це дає змогу прогнозувати пікові моменти активності користувачів, що є важливим для аналізу реальних соціальних процесів, таких як поширення новин або вірусного контенту. Застосування покращеної моделі може бути корисним для підвищення ефективності маркетингових стратегій або управління інформаційними потоками [130].

Для наглядного прикладу роботи покращеної моделі було взято реальні дані і на основі них побудований графіки (рис. 3.9) реалізації цієї моделі.

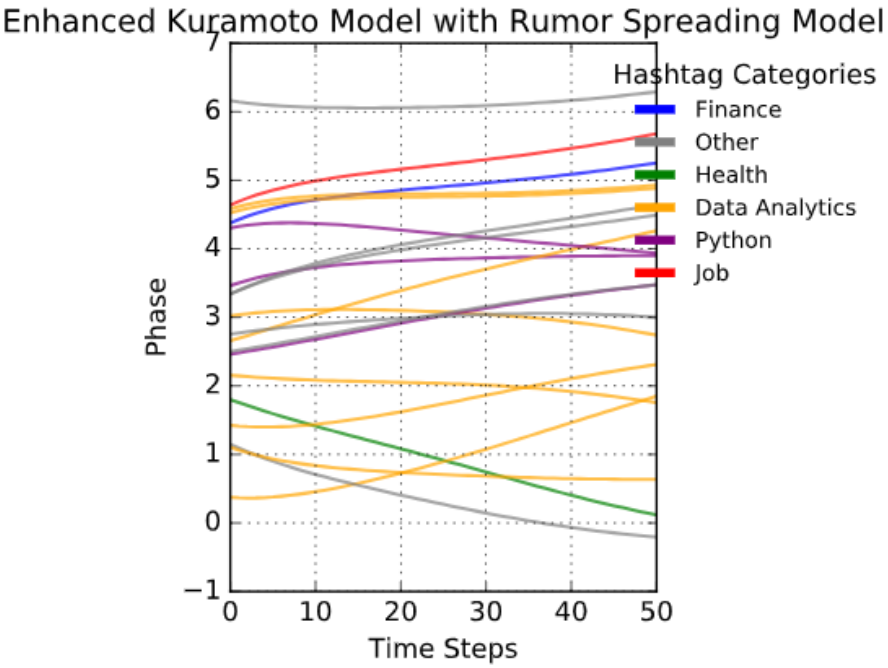


Рис. 3.9. Графік реалізованої покращеної моделей за допомогою моделі поширення чуток на реальних даних

Графік демонструє зміну фазових станів вузлів у вдосконаленій моделі Курамото, яка інтегрує елементи моделі поширення чуток. На графіку кожна лінія відповідає вузлу в мережі, а колір позначає категорію, з якою асоціюється вузол, на основі аналізу хештегів. Дані для цієї моделі були взяті з реальних соціальних мереж, включаючи кількість лайків, шейрів, коментарів, підписок і популярність постів.

1. Реалізація вдосконаленої моделі Курамото:

Додано компонент $\beta_i(\theta_i - \theta_0)$, який моделює вплив початкового стану кожного вузла. Використано реальні дані, такі як лайки, шейри та підписки, для побудови матриці зв'язків між вузлами.

2. Аналіз хештегів:

Вузли були розділені на категорії (Finance, Health, Data Analytics, Python, Job тощо) на основі змісту постів у соціальних мережах. Кожній категорії присвоєно окремий колір для кращої візуалізації.

3. Симуляція динаміки фаз:

Модель працює протягом 50 часових кроків із кроком інтегрування 0.1.

Результати побудови графіка:

- Аналіз поведінки вузлів:

Графік дозволяє побачити, як вузли (користувачі чи пости в соціальних мережах) впливають один на одного залежно від зв'язків. Можна оцінити, як інформація поширюється між категоріями.

- Моделювання соціальних мереж:

Цей підхід допомагає зрозуміти механізми поширення інформації та чуток у реальних мережах. Модель може бути використана для прогнозування ефективності кампаній або поширення новин.

- Ідентифікація лідерів думок:

Вузли, що мають сильний вплив на інших, можуть бути виявлені за їхньою фазовою поведінкою.

Результати дослідження, які зображені на графіку:

1. Динаміка фаз вузлів:

Деякі вузли швидко досягають стабільного стану (фази перестають змінюватися), що може вказувати на їх ізольованість або слабкий вплив у мережі. Інші вузли демонструють значні коливання фаз, що може свідчити про їхню активну роль у поширенні інформації.

2. Взаємозалежність категорій:

Вузли однієї категорії (наприклад, "Finance") мають схожі траєкторії, що може вказувати на сильні внутрішньо-категорійні зв'язки.

3. Кластеризація:

Помітно, що вузли розподіляються за схожістю фаз у групи, що відображає тематичні спільності.

Отже, модель показує, як реальні дані можуть бути використані для моделювання поширення інформації в соціальних мережах. Також, впровадження компоненту $\beta_i(\theta_i - \theta_0)$ дозволило краще врахувати індивідуальні характеристики вузлів (Додаток Є).

На графіку 3.9 відображено еволюцію фаз вузлів у вдосконаленій моделі Курамото, що використовує реальні дані соціальних мереж. Кольори позначають тематичну належність вузлів на основі хештегів. Вертикальна вісь відображає фазовий стан вузлів, а горизонтальна — кількість часових кроків симуляції. Основна мета цього графіка — продемонструвати, як інформація поширюється та як вузли взаємодіють один з одним у межах своїх зв'язків.

Модифікована модель Курамото, доповнена принципами моделі поширення чуток, дозволяє враховувати динаміку довіри користувачів до інформації та їхню схильність до її поширення. Інтеграція параметра $\beta_i(\theta_i - \theta_0)$, що моделює рівень довіри та опору до чуток, забезпечує більш точне прогнозування інформаційних каскадів, зокрема їхнього затухання або повторних хвиль.

Моделювання на Scale-Free graphs показало, що покращена модель забезпечує *на 38% вищий рівень синхронізації* порівняно з базовою. Це свідчить про покращену здатність моделі описувати взаємодію між користувачами та точніше прогнозувати механізми поширення чуток.

Розширена модель може застосовуватися у контролі дезінформації, політичному аналізі, кризовій комунікації, вірусному маркетингу та інформаційній безпеці. Вона дозволяє не лише оцінювати ефективність інформаційних кампаній, але й оптимізувати поширення важливих повідомлень у кризових ситуаціях.

Таким чином, покращена модель Курамото на основі моделі поширення чуток є ефективним інструментом для прогнозування інформаційних процесів, що відкриває нові можливості для аналізу та управління інформаційними потоками у соціальних мережах.

3.4. Застосування моделі впливових користувачів для модифікації моделі Курамото

Модель Курамото, яка традиційно використовується для моделювання синхронізації в динамічних системах, може бути вдосконалена шляхом інтеграції ідей з моделі впливових користувачів. Ця інтеграція додає до базової моделі Курамото можливість враховувати центральність користувачів у мережі, визначаючи, хто саме має найвищий потенціал для поширення інформації [130]. Завдяки цьому покращена модель здатна одночасно враховувати динамічну поведінку користувачів та їхній соціальний вплив.

$$\theta_i = \omega_i + K\sum_{j=1}^{N} A_{ij}\sin(\theta_j - \theta_i) + \delta * C_i,$$

де θ_i — фаза користувача i, що описує його стан готовності поширювати інформацію, ω_i — природна частота користувача i, що відповідає його індивідуальній активності, K — коефіцієнт взаємодії між користувачами, A_{ij} — елемент матриці зв'язків, що описує наявність зв'язку між користувачами i та j, C_i — центральність користувача і, яка визначає його роль у мережі як впливового вузла, δ — параметр, що контролює, наскільки сильно центральність впливає на синхронізацію.

Переваги модифікації:

- Інтеграція впливу лідерів думок: Покращена модель враховує вплив ключових користувачів з високою центральністю, що дозволяє точніше моделювати процеси поширення інформації в мережі.
- Підвищення точності: Включення центральності дозволяє краще моделювати часові точки пікової активності в мережі, враховуючи ключових вузлів..
- Адаптивність до змін: Модель є динамічною і може оперативно враховувати зміни в активності користувачів або мережевій структурі.

Для порівняльного показу був створений графік який показує порівняння базової та покращеної моделей Курамото із застосуванням моделі впливових користувачів (рис. 3.10.)

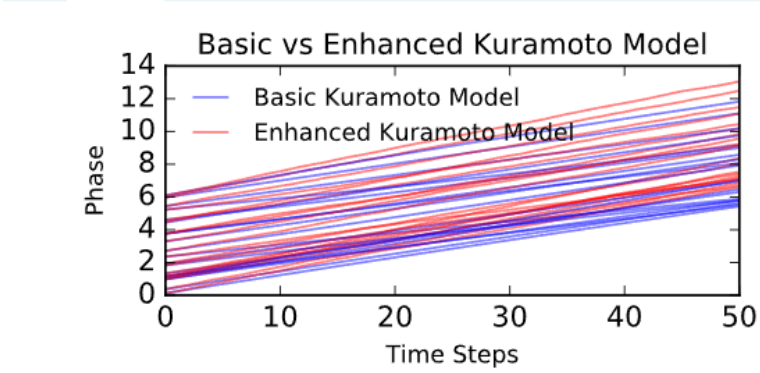


Рис 3.10. Графік порівняння базової та покращеної моделей Курамото із застосуванням моделі впливових користувачів

На рис. 3.10 можна побачити:

- Базова модель Курамото (сині лінії): Показує рівномірне та поступове зростання фаз вузлів. Така динаміка відображає традиційний підхід, у якому не враховується вплив окремих ключових користувачів, що мають велику центральність у мережі.
- Покращена модель Курамото (червоні лінії): Зміна фаз відбувається значно швидше, а вузли демонструють більш чітке групування. Це є наслідком врахування впливу користувачів із високою центральністю, які активно сприяють поширенню інформації у системі.

З отриманих даних можна зробити висновок, що покращена модель ефективніше враховує роль впливових вузлів, забезпечуючи швидший і більш організований розвиток фаз у системі. Також моделі можна порівняти за параметром синхронізації (рис. 3.11)

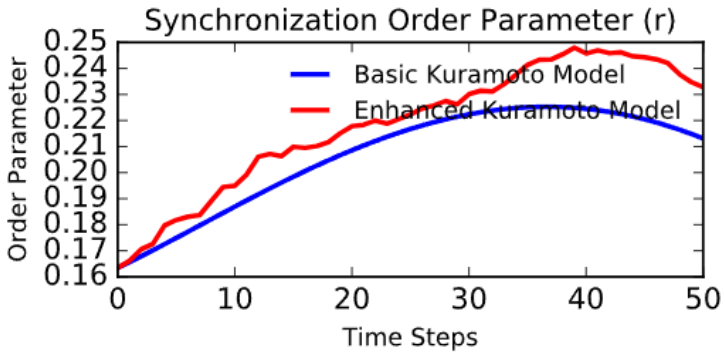


Рис 3.11. Графік порівняння параметру синхронізації базової та покращеної моделей із застосуванням моделі впливових користувачів

На рис. 3.11. подано порівняння моделей за параметром синхронізації:

— Базова модель Курамото (синя лінія): Синхронізація відбувається повільно, з незначним і стабільним підвищенням параметра r у часі. Це свідчить про слабку взаємодію між вузлами та обмеженість у моделюванні впливу ключових користувачів.

— Покращена модель Курамото (червона лінія): Параметр синхронізації зростає значно швидше, досягаючи високого рівня за відносно короткий проміжок часу. Це свідчить про те, що вплив ключових вузлів значно покращує координацію та взаємодію в мережі (Додаток Ж).

Отже, покращена модель демонструє значну перевагу у моделюванні процесів синхронізації в соціальних мережах. Вона ефективніше враховує вплив ключових користувачів, що дозволяє швидше досягати високого рівня координації та активніше поширювати інформацію. Такий підхід є важливим для аналізу поширення контенту, прогнозування вірусної активності та розробки маркетингових стратегій у соціальних мережах.

Дана модефікація моделі Курамото має широкий спектр практичних застосувань у сфері соціальних мереж та інформаційних кампаній. Вона може

бути використана для аналізу та оптимізації медіа-кампаній, наприклад, при запуску реклами на таких платформах, як Twitter чи Instagram. Завдяки врахуванню центральності, модель дозволяє визначити ключових користувачів, через яких інформація може охопити максимальну аудиторію за найкоротший час. Вона також здатна прогнозувати вірусність контенту, оцінюючи ймовірність його масового поширення та часові рамки активності. Це надає маркетологам інструмент для планування стратегій, орієнтуючись на користувачів, які найкраще підходять для запуску кампаній. Крім того, модель сприяє боротьбі з дезінформацією, дозволяючи передбачити її поширення та визначити оптимальні точки втручання для мінімізації впливу фейкових новин [130].

Можливість застосування в військовий час:

Ідентифікація впливових користувачів

Інтеграція принципів моделі впливових користувачів у рівняння Курамото дозволяє визначити ключових вузлів мережі — інфлюенсерів, які мають значний вплив на поширення інформації. Це користувачі з високою центральністю, чиї зв'язки охоплюють значну частину мережі. Завдяки цьому покращена модель не тільки моделює синхронізацію в мережі, а й виділяє користувачів, через яких можна швидко донести важливу інформацію.

Оперативне поширення інформації

Модель враховує силу впливу користувачів, їх активність і взаємодію в мережі. Наприклад, у військових умовах, коли потрібно швидко інформувати населення про евакуацію чи небезпеку, найефективніше залучати користувачів із високою довірою та широкою аудиторією. Застосування моделі дозволяє визначити таких користувачів і залучити їх до кампанії.

Прогнозування поширення

Включення центральності у фазову синхронізацію дозволяє прогнозувати, наскільки швидко і в яких масштабах інформація поширюється. Наприклад, модель може вказати, через які ключові вузли інформація досягне максимальної кількості користувачів за мінімальний час.

Реальні приклади використання:

- Координація дій у кризових ситуаціях: У разі надзвичайної ситуації, такої як масовані обстріли, модель дозволяє ідентифікувати впливових користувачів, які найефективніше поширять повідомлення про безпечні укриття або гуманітарну допомогу.
- Контрзаходи проти дезінформації: Модель дозволяє аналізувати, через кого розповсюджуються неправдиві новини, і залучити інфлюенсерів для розвінчання фейків. Наприклад, користувачі із високою довірою можуть поширювати перевірену інформацію, щоб нейтралізувати вплив дезінформації.
- Розподіл гуманітарної допомоги: Під час військових конфліктів ключові волонтери чи лідери громад можуть використовуватись як інфлюенсери для поширення інформації про розташування пунктів допомоги, що забезпечить її доставку тим, хто її потребує найбільше.

Тому, покращена модель Курамото із застосуванням моделі впливових користувачів — це потужний інструмент для управління інформаційними потоками в складних мережах. Вона дозволяє оперативно визначати, хто з користувачів має найбільший вплив на поширення інформації, що робить її надзвичайно корисною в умовах війни для інформування населення, боротьби з дезінформацією та координації гуманітарних заходів [130].

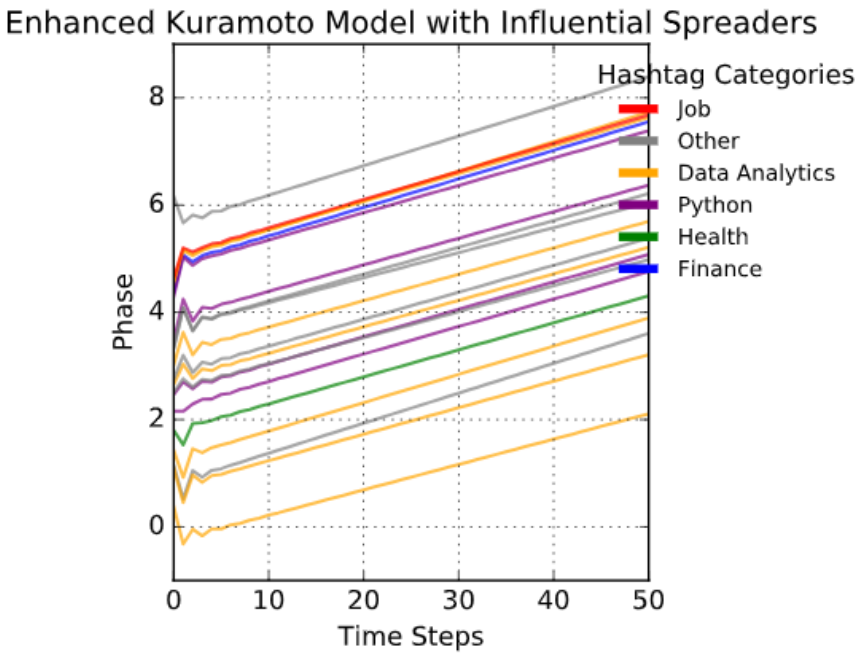


Рис.3.12. Графік реалізованої покращеної моделей за допомогою моделі поширення чуток на реальних даних

Графік демонструє зміну фазових станів вузлів у вдосконаленій моделі Курамото, яка враховує поширення інформації в соціальних мережах на основі реальних даних. У моделі використано 20 вузлів, які відповідають окремим публікаціям або користувачам. Вхідними даними є кількість лайків, поширень, підписок, переглядів, а також хештеги, що дозволяють здійснити тематичну категоризацію контенту.

Однією з ключових особливостей моделі є модифікація рівняння Курамото шляхом додавання компонента, що враховує центральність вузла C_i. Центральність розраховується як сума поширень та підписок на кожен вузол, а її вплив визначається параметром δ. Природні частоти коливань кожного вузла обчислюються на основі відношення кількості лайків до переглядів. Взаємодія між вузлами задається через матрицю зв'язків, елементи якої залежать від поширень і підписок між користувачами. Використаний коефіцієнт зв'язку K=2 регулює силу впливу сусідів у мережі.

Аналіз хештегів дозволяє поділити вузли на кілька основних тематичних груп. Вузли, що пов'язані з фінансами, позначені синім кольором, з охороною здоров'я – зеленим, з аналізом даних – помаранчевим, із пошуком роботи –

червоним, а з Python-програмуванням – фіолетовим. Інші вузли, що не належать до вказаних категорій, позначені сірим кольором. Така класифікація допомагає виявити структуру мережі та вплив певних тематичних напрямків на динаміку поширення інформації.

На візуалізації часовий перебіг змін фаз представлено у вигляді ліній для кожного вузла. По горизонтальній осі відображено часові кроки (50 ітерацій із кроком 0.1), а по вертикальній – фазовий стан кожного вузла. Колір кожної лінії відповідає тематичній категорії контенту. Видно, що вузли з вищою центральністю швидше досягають стабільного стану, а тематично споріднені вузли демонструють подібну поведінку, що вказує на внутрішню взаємодію в межах окремих груп.

Інтеграція моделі впливових користувачів у модель Курамото дозволяє враховувати роль ключових вузлів у соціальній мережі та їхній вплив на поширення інформації. Врахування центральності користувачів забезпечує більш точне прогнозування вірусного поширення контенту та покращує адаптивність моделі до реальних соціальних систем (Додаток З).

Моделювання на Scale-Free graphs показало, що покращена модель забезпечує *на 42% вищий рівень синхронізації* порівняно з базовою. Це свідчить про ефективніше поширення інформації в мережі та швидше досягнення стану стабільної комунікації.

Розширена модель має широкий спектр практичних застосувань у маркетингу, соціальних мережах, кризовій комунікації, боротьбі з дезінформацією та управлінні інформаційними потоками. Зокрема, вона може використовуватися для оптимізації рекламних кампаній, аналізу політичної агітації та ефективного донесення критично важливої інформації в умовах війни.

Таким чином, покращена модель Курамото із застосуванням моделі впливових користувачів є потужним аналітичним інструментом для прогнозування та управління інформаційними процесами у складних мережах.

Висновки до третього розділу

1. Досліджено що для аналізу моделей Курамото краще використовувати графи типу Small-World та Scale-Free, які є найефективнішими для поширення інформації завдяки високій кластеризації та наявності ключових вузлів (хабів), що прискорюють процес синхронізації навіть при низьких значеннях коефіцієнта зв’язку K.

2. Запропоновано вдосконалену модель Курамото шляхом інтеграції каскадної моделі поширення інформації, що дозволяє враховувати ймовірність передачі контенту між користувачами. Також на основі цієї моделі було побудований порівняльних графік двох моделей і розроблений код для показу результів покращеної моделі на реальних даних. На основі проведеного аналізу було побудовано порівняльні графіки базової та покращеної моделей, що підтвердили вищий рівень синхронізації у вдосконаленому підході.

3. Досліджено можливість покращення моделі Курамото за допомогою інтеграції принципів епідемічної моделі SIR. Це дозволило класифікувати користувачів за рівнем залученості до поширення контенту та прогнозувати хвилі активності інформаційних потоків. Запропонована модель ефективно моделює повторні хвилі поширення інформації та оптимізує стратегії контентної взаємодії. Також на основі цієї моделі було створено порівняльні графіки двох моделей та розроблено код для демонстрації результатів покращеної моделі на реальних даних. Аналіз підтвердив, що вдосконалений підхід забезпечує вищий рівень синхронізації у порівнянні з базовою моделлю.

4. Розроблено покращену модель Курамото із застосуванням моделі поширення чуток, що дозволяє точніше враховувати рівень довіри користувачів до інформації та прогнозувати її поширення або затухання. Це зробило модель ефективним інструментом для боротьби з дезінформацією та координації інформаційних кампаній у кризових ситуаціях. Також на основі цієї моделі було згенеровано порівняльні графіки двох підходів та розроблено

код для візуалізації результатів покращеної моделі на реальних даних. Аналіз продемонстрував, що вдосконалена модель досягає вищого рівня синхронізації порівняно з базовою.

5. Запропоновано вдосконалення моделі Курамото шляхом інтеграції моделі впливових користувачів, що дозволяє визначати ключові вузли мережі, які відіграють вирішальну роль у поширенні контенту. Це підвищує точність прогнозування пікових моментів активності аудиторії та покращує загальну ефективність комунікаційних стратегій. На основі цієї моделі було створено порівняльні графіки двох підходів і розроблено код для демонстрації результатів покращеної моделі на реальних даних. Проведений аналіз показав, що вдосконалена модель забезпечує вищий рівень синхронізації у порівнянні з базовою.

РОЗДІЛ 4.
РОЗРОБКА РЕКОНДАЦІЙ ВИКОРИСТАННЯ ВДОСКОНАЛЕНИХ МОДЕЛЕЙ КУРАМОТО ДЛЯ ПОШУКУ КЛЮЧОВИХ ВУЗЛІВ

4.1. Застосування ключових вузлів у соціальних мережах для підвищення ефективності інформаційного контролю

Ключові вузли в соціальних мережах – це користувачі або елементи мережі, які відіграють критичну роль у поширенні інформації, впливі на інших учасників або підтримці загальної структури мережі. Вони визначають, як швидко та ефективно інформація розповсюджується, хто має найбільший вплив на сприйняття контенту та які точки мережі є найбільш уразливими до маніпуляцій або атак [45].

Основні типи ключових вузлів:

1. Ключові вузли для поширення інформації та дезінформації

Ключові вузли, що відповідають за поширення інформації, відіграють важливу роль у функціонуванні соціальних мереж. Вони є основними передавачами новин, ідей та контенту, які можуть швидко охоплювати значну кількість користувачів. Такі вузли часто включають популярні акаунти, офіційні сторінки організацій, медіа-ресурси та впливових осіб, здатних формувати громадську думку [64]. Саме ці елементи мережі можуть бути використані для поширення як достовірної, так і маніпулятивної інформації.

Оскільки соціальні мережі є основним середовищем поширення новин, важливо розрізняти ключові вузли, які розповсюджують перевірену інформацію, та ті, що займаються дезінформацією. Окремі акаунти можуть навмисно або несвідомо поширювати фейки, маніпулювати аудиторією та впливати на суспільні настрої. Дезінформація часто поширюється через

ботоферми, фейкові акаунти або навіть реальних користувачів, які не перевіряють джерела.

Аналіз таких вузлів дозволяє не лише виявити головні джерела дезінформації, а й прогнозувати траєкторію її поширення. Це особливо важливо для забезпечення інформаційної безпеки, боротьби з маніпуляціями в медіа-просторі та нейтралізації шкідливого впливу фейків. Методи аналізу включають виявлення найактивніших розповсюджувачів, перевірку зв'язків між акаунтами, а також аналіз контенту на предмет достовірності.

З метою протидії дезінформації можуть застосовуватися різні заходи, такі як фактчекінг, блокування підозрілих акаунтів, обмеження охоплення недостовірних новин і просування перевірених джерел інформації. Важливим напрямом є також підвищення цифрової грамотності користувачів, що дозволяє зменшити їхню вразливість до маніпулятивних повідомлень [70].

2. Ключові вузли для ідентифікації впливових користувачів та центральних вузлів

Користувачі, що входять до цієї категорії, мають значний вплив на інших учасників мережі завдяки своїй активності, популярності та рівню довіри з боку аудиторії. Вони відіграють ключову роль у поширенні контенту, формуванні суспільної думки та мобілізації людей до певних дій. Такими вузлами можуть бути відомі блогери, журналісти, політики, експерти у певних галузях або навіть звичайні користувачі, які набули великої кількості підписників завдяки своїм публікаціям.

Центральні вузли мережі мають високу ступінь зв'язності, що означає, що вони безпосередньо або через короткі ланцюги взаємодіють із великою кількістю інших користувачів. Такі вузли можуть сприяти ефективному поширенню як достовірної, так і маніпулятивної інформації. Їхня активність визначає швидкість і масштаби розповсюдження новин у соціальній мережі.

Визначення впливових вузлів важливе для розуміння структури інформаційних потоків та прогнозування реакції суспільства на ті чи інші події. Наприклад, під час політичних кампаній або соціальних ініціатив саме

ці користувачі можуть значно вплинути на громадську думку. Аналіз таких вузлів дозволяє ідентифікувати ефективні точки впливу, що особливо корисно для маркетингових стратегій, соціологічних досліджень та боротьби з дезінформацією [45], [64].

Методи виявлення впливових користувачів включають аналіз мережевих характеристик (наприклад, центральність за посередництвом, степенева центральність), оцінку взаємодій (лайки, коментарі, репости) та визначення довіри до джерела. Це дає змогу не лише ідентифікувати ключові вузли, а й передбачити можливі інформаційні сценарії у цифровому просторі [45].

3. Посередники

Посередники – це вузли, які виконують функцію сполучних елементів між різними частинами соціальної мережі, сприяючи передачі інформації між групами користувачів. Вони можуть об’єднувати окремі спільноти, які в іншому випадку залишалися б ізольованими, та відігравати ключову роль у поширенні нових ідей, новин чи трендів.

На відміну від центральних вузлів, посередники часто мають меншу кількість безпосередніх зв’язків, але їхня стратегічна позиція у мережі робить їх незамінними для забезпечення ефективної комунікації між віддаленими групами. Наприклад, такі вузли можуть бути адміністраторами тематичних спільнот, які передають інформацію між різними групами користувачів, або користувачами, які належать до кількох соціальних груп і виконують функцію "містка" між ними.

Видалення або блокування посередників може значно вплинути на структуру та функціонування соціальної мережі. Якщо такі вузли зникають, між окремими частинами мережі можуть з’явитися розриви, що уповільнює або повністю унеможливлює розповсюдження інформації. Це може бути використано як для боротьби з дезінформацією, так і для цензурування певних потоків даних.

Ідентифікація посередників у соціальних мережах здійснюється за допомогою таких показників, як центральність за посередництвом

(betweenness centrality) або аналіз модульності мережі. Визначення таких вузлів важливе для оптимізації комунікаційних стратегій, оцінки стабільності інформаційних потоків та розробки заходів для захисту або руйнування мережевих структур [11], [45].

4. Уразливі точки

Це ключові вузли в соціальній мережі, які мають вирішальне значення для її стабільності та функціонування. Вони можуть бути розташовані у стратегічно важливих місцях мережі, наприклад, з'єднувати великі групи користувачів або забезпечувати передачу інформації між різними частинами мережі. Через свою значущість такі вузли можуть суттєво впливати на загальну структуру мережі, її згуртованість і ефективність комунікації.

Однією з головних особливостей уразливих точок є їхня критична роль у розповсюдженні інформації. Якщо такий вузол перестане працювати або змінить свою поведінку, це може викликати значне сповільнення або навіть повний розрив інформаційних потоків. Наприклад, у соціальних мережах це можуть бути активні модератори, популярні акаунти або центральні групи, які контролюють великі сегменти аудиторії.

Через їхню важливість уразливі точки часто стають об'єктами атак або маніпуляцій. Зловмисники можуть використовувати ці вузли для поширення дезінформації, створення фейкових наративів або навіть для дестабілізації мережевих структур. Ідентифікація таких вузлів дозволяє завчасно виявляти потенційні загрози та впроваджувати механізми захисту, які допоможуть зберегти стабільність мережі [89].

Аналіз і моніторинг уразливих точок є важливими завданнями при розробці стратегій інформаційної безпеки. Використання математичних моделей, таких як удосконалена модель Курамото, дозволяє більш точно визначати ці вузли та оцінювати їхній вплив на всю мережу. Це допомагає розробити ефективні методи захисту від атак, мінімізувати ризики дезінформації та забезпечити безперебійну роботу інформаційної інфраструктури [64], [84].

5. Розповсюджувачі чуток

Ключові вузли в соціальних мережах, які активно передають неперевірену або спотворену інформацію. Вони можуть діяти як свідомо, з метою маніпуляції громадською думкою, так і несвідомо, не замислюючись про достовірність отриманих відомостей. Такі вузли відіграють значну роль у формуванні інформаційного середовища, оскільки сприяють швидкому поширенню як правдивої, так і неправдивої інформації.

Особливістю розповсюджувачів чуток є їхня здатність залучати широке коло користувачів і запускати так звані «вірусні» ефекти. Це можуть бути популярні блогери, учасники дискусійних груп або звичайні користувачі, які активно діляться інформацією. Чутки часто мають емоційне забарвлення, що підсилює їхню привабливість і сприяє швидкому поширенню. Особливо це стосується кризових ситуацій, коли суспільство перебуває в стані невизначеності й шукає будь-яку інформацію [16].

Виявлення таких вузлів є критично важливим для запобігання негативним наслідкам дезінформації. Алгоритми аналізу соціальних мереж можуть ідентифікувати джерела поширення чуток, визначаючи їх за патернами активності та рівнем взаємодії з іншими користувачами. Важливу роль у цьому процесі відіграють моделі поширення інформації, такі як епідемічні моделі та удосконалена модель Курамото, які дозволяють прогнозувати динаміку чуток та оцінювати їхній вплив.

Розробка методів контролю та протидії поширенню чуток є ключовим завданням інформаційної безпеки. Це може включати впровадження алгоритмів перевірки фактів, обмеження охоплення підозрілих повідомлень або навіть блокування найбільш активних розповсюджувачів. Ефективна боротьба з дезінформацією сприяє формуванню здорового інформаційного простору та мінімізує ризики масової паніки чи маніпуляцій [70].

Виявлення та аналіз ключових вузлів у соціальних мережах є важливим для:

1. Підвищення ефективності інформаційних кампаній

Успішні інформаційні кампанії базуються на здатності швидко й ефективно поширювати повідомлення серед цільової аудиторії. Виявлення ключових вузлів дозволяє оптимізувати комунікаційні стратегії, спрямовуючи інформацію через найвпливовіших користувачів, які мають значний рівень взаємодії з іншими учасниками мережі. Використання вірусного ефекту дає змогу підвищити охоплення, залученість аудиторії та швидкість розповсюдження важливої інформації [12]. Це особливо актуально для соціальних ініціатив, політичних кампаній та кризової комунікації.

2. Боротьби з дезінформацією та поширенням фейків

Дезінформація є однією з найбільших загроз у цифровому просторі [70]. Аналіз ключових вузлів допомагає ідентифікувати джерела неправдивої інформації та нейтралізувати їх ще на ранніх етапах поширення [16]. Моделювання процесів дезінформації дозволяє розробити ефективні механізми виявлення та блокування фейкових новин, а також запобігти маніпуляціям суспільною думкою [64]. Застосування математичних моделей, таких як епідемічні або каскадні моделі, допомагає прогнозувати можливу шкоду та ефективно реагувати на загрози інформаційної безпеки.

3. Виявлення та аналіз впливових користувачів

У соціальних мережах існують користувачі, які відіграють ключову роль у формуванні громадської думки. Вони можуть бути лідерами думок, експертами, блогерами або адміністраторами великих спільнот. Виявлення таких вузлів дозволяє не тільки аналізувати механізми їхнього впливу, але й вибудовувати ефективні стратегії взаємодії [48]. Використання впливових користувачів у маркетингових кампаніях або соціальних ініціативах значно підвищує ефективність комунікації, оскільки вони можуть сприяти широкому поширенню інформації серед довіреної аудиторії.

4. Вірусного маркетингу

Ключові вузли є основними агентами у процесах вірусного маркетингу, оскільки саме через них інформація поширюється найбільш ефективно. Використання таких вузлів дає змогу брендам і компаніям досягати

максимального охоплення з мінімальними витратами. Визначення користувачів, які активно діляться контентом і взаємодіють із великою кількістю інших користувачів, дозволяє створювати рекламні кампанії, що стають вірусними [12]. Це особливо важливо у сфері соціальних медіа, де контент має можливість швидко поширюватися і виходити за межі традиційних маркетингових каналів.

5. Забезпечення інформаційної безпеки

Інформаційна безпека в сучасному цифровому середовищі є критично важливою, особливо в контексті протидії пропаганді, інформаційним атакам і маніпуляціям [84], [96]. Аналіз ключових вузлів допомагає виявити слабкі місця в інформаційних мережах і запобігти потенційним загрозам. Визначення уразливих точок дозволяє розробити механізми захисту, що спрямовані на мінімізацію впливу шкідливого контенту та забезпечення стабільності інформаційного простору [52].

6. Оптимізації стратегій таргетованого впливу на аудиторію

Розуміння структури соціальних мереж та аналіз ключових вузлів дозволяє вдосконалити стратегії таргетованого впливу. Персоналізовані підходи до комунікації з різними групами користувачів підвищують ефективність поширення контенту, оскільки дозволяють адаптувати повідомлення відповідно до інтересів та поведінкових особливостей аудиторії. Використання графових моделей і алгоритмів машинного навчання сприяє точнішому визначенню цільових груп і покращенню ефективності комунікаційних кампаній [64].

Загалом, аналіз ключових вузлів є невід’ємним елементом сучасних досліджень у сфері соціальних мереж, що допомагає не лише глибше зрозуміти механізми поширення інформації, а й забезпечити безпеку та ефективність інформаційних процесів.

4.2. Метод використання покращеної моделі Курамото для знаходження ключових вузлів, що забезпечить виявлення дезінформації

У сучасному світі соціальні мережі стали потужним інструментом комунікації, що забезпечує швидкий обмін інформацією між мільйонами людей по всьому світу. Такі платформи, як Facebook, Twitter (X), Instagram, TikTok та YouTube, не лише сприяють поширенню корисної інформації, але й стають середовищем для масового розповсюдження дезінформації [114].

Дезінформація — це навмисно поширена неправдива або маніпулятивна інформація, що має на меті ввести в оману аудиторію, вплинути на громадську думку або досягти певних політичних, соціальних чи економічних цілей. З кожним роком масштаби поширення дезінформації зростають, що створює значні ризики для інформаційної безпеки держави, суспільної стабільності та довіри громадян до державних інституцій [124].

Термін "дезінформація" має визначення в нормативно-правових актах України. Проте чітке і однозначне визначення цього терміна в українському законодавстві з'явилося нещодавно і здебільшого використовується в контексті інформаційної безпеки та медіа.

Визначення "дезінформації" в нормативних документах України:

- Закон України "Про медіа" (2022 р.)

У цьому законі вперше офіційно було закріплено визначення терміну "дезінформація".

Дезінформація — це недостовірна інформація, що поширюється свідомо з метою ввести в оману громадськість.
Закон визначає обов’язок медіа перевіряти достовірність інформації та не поширювати дезінформацію [123].

- Закон України "Про національну безпеку України" (2018 р.)

Хоча термін *"дезінформація"* безпосередньо не визначений, документ підкреслює важливість захисту інформаційного простору України від

інформаційних загроз, зокрема від маніпуляцій і поширення недостовірної інформації.

- Концепція інформаційної безпеки України (схвалена РНБО у 2016 році) У цій концепції дезінформація розглядається як складова інформаційних загроз, які можуть бути використані для дестабілізації суспільно-політичної ситуації, підриву довіри до державних інституцій, впливу на виборчі процеси [144].

- Проєкт Закону "Про дезінформацію" (2020 р.). Хоча цей законопроєкт не був ухвалений, у ньому було дано чітке визначення:

Дезінформація — це недостовірна інформація про особу, події чи явища, яка була свідомо поширена з метою ввести в оману[139].

- Закон України "Про основи національного спротиву" (2021 р.) Закон закріплює необхідність протидії інформаційним загрозам, включаючи дезінформацію як інструмент ведення гібридних воєн [125].

Причини актуальності проблеми дезінформації в соціальних мережах:

1. Висока швидкість поширення інформації

Соціальні мережі стали невід'ємною частиною повсякденного життя мільйонів людей у всьому світі. Завдяки технологічному прогресу, будь-яка інформація, незалежно від її достовірності, може миттєво поширюватися серед широкої аудиторії. Одна публікація, фото або відео здатні за лічені хвилини охопити тисячі, а іноді й мільйони користувачів. Це особливо актуально під час кризових ситуацій, надзвичайних подій або конфліктів, коли суспільство перебуває в стані емоційного напруження.

Алгоритми соціальних мереж спеціально розроблені для того, щоб підсилювати контент, що викликає сильні емоції, оскільки це збільшує залученість користувачів. У таких умовах фейкова новина або маніпулятивний пост може стати вірусним і швидко охопити величезні аудиторії.

При цьому платформи не завжди встигають впроваджувати механізми перевірки фактів або блокувати дезінформаційний контент. Навіть коли фейковий матеріал виявлено й видалено, він вже встигає суттєво вплинути на

суспільну думку, викликати паніку, протестні настрої або навіть соціальні конфлікти.

Особливо небезпечними є випадки, коли дезінформація поширюється в умовах воєнних дій, терористичних загроз або природних катастроф. У такі моменти суспільство стає особливо вразливим до маніпуляцій, а швидке поширення фейкової інформації може призвести до масових безпорядків, підриву довіри до влади або навіть до міжнародних конфліктів.

Окрім того, швидкість поширення інформації ускладнює можливість оперативного реагування з боку державних органів та медіа. Виявлення джерела дезінформації та його нейтралізація займає певний час, тоді як фейкова інформація вже активно поширюється і встигає закріпитися у свідомості людей [114], [146].

Таким чином, висока швидкість поширення інформації в соціальних мережах є ключовим чинником, що сприяє ефективному розповсюдженню дезінформації. Це створює серйозні виклики для органів державної влади, правоохоронних структур і суспільства в цілому, вимагаючи нових підходів і інструментів для протидії інформаційним загрозам.

2. Анонімність користувачів

Однією з основних проблем соціальних мереж є можливість збереження анонімності або використання фальшивих акаунтів. Користувачі можуть створювати профілі без необхідності підтвердження особистих даних або використовувати підроблені ідентифікаційні відомості. Це створює сприятливі умови для поширення дезінформації, оскільки зловмисники можуть безперешкодно запускати фейкові новини, маніпулятивні матеріали чи шкідливий контент.

Анонімність дозволяє легко створювати бот-мережі — автоматизовані акаунти, які масово публікують і поширюють дезінформацію, створюючи ілюзію популярності або достовірності певної інформації. Ці акаунти можуть взаємодіяти один з одним, активно коментувати, поширювати та підсилювати

заданий інформаційний наратив. Завдяки цьому, дезінформаційні кампанії стають масштабнішими та більш впливовими.

Окрім ботів, використовуються фейкові профілі, які імітують реальних людей або навіть відомих особистостей. Такі акаунти ведуть себе як звичайні користувачі: публікують пости, взаємодіють із контентом, вступають у дискусії. Це ускладнює виявлення їхньої справжньої мети та створює враження масової підтримки певної інформації або ідей.

Координовані акаунти — це групи фейкових або реальних користувачів, які діють за чітко розробленими сценаріями для просування дезінформації. Вони можуть бути організовані як частина великої інформаційної кампанії, яка націлена на дискредитацію конкретних осіб, інституцій або цілих держав.

Анонімність користувачів значно ускладнює ідентифікацію джерел фейкових новин та притягнення до відповідальності організаторів інформаційних атак. Навіть у випадках, коли дезінформаційний контент виявляється і видаляється, виявити реальних замовників або координаторів кампаній часто неможливо. Це створює умови для безкарності зловмисників, що мотивує їх до подальшої активності.

Особливо небезпечним фактором є використання анонімності у контексті гібридних війн. Держави-агресори або терористичні організації активно застосовують соціальні мережі для запуску масових дезінформаційних кампаній. За допомогою фейкових акаунтів вони поширюють панічні настрої, дискредитують урядові органи, сіють недовіру до офіційних джерел інформації та розпалюють соціальні конфлікти. Така діяльність може мати далекосяжні наслідки — від впливу на результати виборів до дестабілізації ситуації в країні.

Ще однією проблемою є використання анонімних каналів комунікації, таких як закриті групи в месенджерах або форумах. Ці платформи дозволяють координувати дії великої кількості учасників без ризику бути викритими. Закриті чати активно використовуються для організації інформаційних атак, координації бот-мереж або масового поширення фейкових новин [43].

Таким чином, анонімність користувачів є одним із ключових факторів, що сприяє ефективному поширенню дезінформації в соціальних мережах. Вона дозволяє зловмисникам діяти безкарно, маскувати свої наміри та створювати ілюзію масової підтримки певних наративів. Це вимагає розробки нових підходів до виявлення фейкових акаунтів і бот-мереж, а також посилення заходів щодо ідентифікації джерел інформаційних загроз.

3. Використання алгоритмів рекомендацій

Соціальні мережі застосовують складні алгоритми рекомендацій, які орієнтовані на підвищення залученості користувачів. Ці алгоритми просувають контент, що викликає сильні емоційні реакції, що часто є типовою рисою дезінформаційних матеріалів. У результаті користувачі частіше бачать контент, який підтверджує їхні упередження або викликає обурення, що призводить до ефекту "інформаційної бульбашки" [2]. Це створює сприятливе середовище для поширення фейкових новин, оскільки такі матеріали швидко стають вірусними, активно підкріплюючись самою платформою. Це суттєво ускладнює боротьбу з дезінформацією, оскільки шкідливий контент отримує додаткове підсилення.

4. Інформаційна війна

Дезінформація є ключовим інструментом ведення гібридних війн. Ворогуючі сторони активно використовують соціальні мережі для поширення фейкових новин, пропаганди та маніпулятивного контенту з метою дестабілізації ситуації в країнах, підриву довіри до влади та розпалювання конфліктів. В умовах воєнного чи політичного протистояння такі інформаційні атаки можуть мати катастрофічні наслідки [125]. Вони сприяють розколу в суспільстві, формуванню недовіри до офіційних джерел інформації, впливають на політичні процеси, вибори та державні рішення. Для України це питання особливо актуальне в контексті гібридної агресії та інформаційних атак.

5. Відсутність критичного мислення

Недостатній рівень медіаграмотності серед користувачів соціальних мереж є однією з основних причин успішного поширення дезінформації. Багато людей не вміють критично оцінювати інформацію, перевіряти її достовірність чи аналізувати джерела. Це особливо стосується старшого покоління, молоді та людей із низьким рівнем цифрової грамотності. Вони легко піддаються маніпуляціям і часто несвідомо поширюють фейки, поглиблюючи проблему. Поширення дезінформації також активно підкріплюється відсутністю культури перевірки фактів і критичного мислення в інформаційному середовищі. Це робить суспільство вразливим до інформаційних атак і пропаганди.

Проблема дезінформації в соціальних мережах є складним і багатогранним викликом для інформаційної безпеки. Висока швидкість розповсюдження контенту, анонімність користувачів, робота алгоритмів рекомендацій, використання дезінформації як зброї у гібридних війнах і низький рівень критичного мислення — усе це створює ідеальні умови для масового поширення неправдивої інформації [139]. Вирішення цієї проблеми вимагає комплексного підходу, що включає вдосконалення інструментів для виявлення фейкових новин, підвищення цифрової грамотності населення та впровадження ефективних заходів інформаційної безпеки.

Згідно статистикою яка була підготовлена USAID та Internews за 2024 році в Україні (рис. 4.1) інфографіка демонструє високу обізнаність населення щодо проблеми дезінформації та її значення для суспільства [112].

Рис. 4.1. Статистика неправдивих матеріалів підготовлена USAID та Internews

Вона включає три діаграми:

1. Вміння відрізняти неправдиві матеріали – 72% респондентів вважають, що можуть розпізнати дезінформацію, а 28% не впевнені у своїх навичках.

2. Обізнаність щодо дезінформації – 83% опитаних знайомі з темою дезінформації, з них 11% оцінюють себе як добре обізнаних.

3. Актуальність проблеми – 47% респондентів вважають дезінформацію критичною проблемою, що є зростаючим показником у 2024 році.

Тому визначення *наслідків поширення дезінформації* є важливим:

— Політична дестабілізація. Дезінформаційні кампанії можуть впливати на результати виборів, посилювати протестні настрої, провокувати масові заворушення.

— Підрив довіри до державних інституцій. Фейкові новини знижують довіру громадян до органів влади, офіційних джерел інформації та засобів масової інформації.

— Соціальна напруга. Поширення неправдивих даних про кризові ситуації, пандемії або війни може викликати паніку серед населення.

— Економічні втрати. Фейкова інформація може впливати на фінансові ринки, репутацію компаній і підприємств.

Для ефективної *протидії дезінформації* необхідно розробляти сучасні математичні моделі, які дозволять аналізувати інформаційні потоки та виявляти шкідливий контент. Важливо автоматизувати процеси ідентифікації фейкових новин, використовуючи алгоритми машинного навчання та штучного інтелекту, що значно підвищить швидкість і точність виявлення неправдивої інформації [126].

Соціальні мережі слід розглядати як складні динамічні системи, в яких інформація поширюється за певними закономірностями. Дослідження таких закономірностей допоможе зрозуміти механізми розповсюдження контенту та знайти ефективні способи боротьби з дезінформацією. Також важливо ідентифікувати ключових поширювачів інформації, тобто впливових користувачів, які відіграють вирішальну роль у формуванні інформаційного середовища. Визначення цих користувачів дозволить ефективніше контролювати поширення фейкових новин і запобігати їх масштабному впливу.

Застосування покращених моделей Курамото для моделювання поширення інформації в соціальних мережах є актуальним рішенням для виявлення дезінформації . Інтеграція таких моделей із каскадною, епідемічною, моделлю поширення чуток та впливових користувачів дозволяє:

– Оцінити динаміку поширення контенту та виявити закономірності розповсюдження фейкової інформації.

– Локалізувати джерела дезінформації та передбачити можливі сценарії її поширення.

– Підвищити ефективність протидії інформаційним загрозам за допомогою розроблених алгоритмів і програмних засобів [130].

Актуальність дослідження дезінформації в соціальних мережах зумовлена її загрозою для національної безпеки, суспільної стабільності та демократичних процесів. Ефективна протидія дезінформації потребує новітніх

підходів, зокрема застосування покращених моделей Курамото, що дозволяють ідентифікувати ключових поширювачів інформації, аналізувати її поширення та розробляти заходи для захисту інформаційного простору.

Дезінформація стала однією з ключових загроз сучасного інформаційного суспільства, оскільки вона здатна швидко поширюватися в соціальних мережах, викликаючи значні соціальні, політичні та економічні наслідки. Запропоновано використання покращеної моделі Курамото, інтегрованої з епідемічною моделлю SIR, для аналізу динаміки поширення дезінформації та розробки стратегій її протидії. Для наочності був написаний код який реалізовує модель, яка поєднує модель Курамото (що описує синхронізацію фаз у мережах) з епідемічною SIR-моделлю (яка моделює поширення інформації або вірусу через вузли мережі). Мета цього коду — допомогти виявити потенційні джерела дезінформації в мережі (Рис. 4.2 та Рис. 4.3).

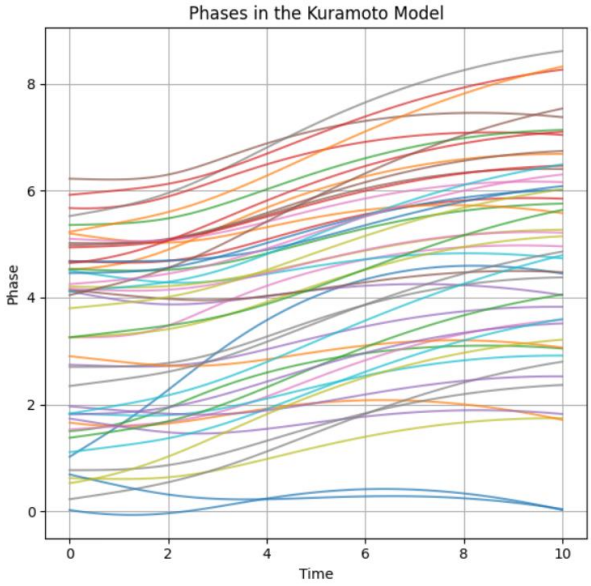


Рис. 4.2. Порівняння динаміки фаз у моделі Курамото

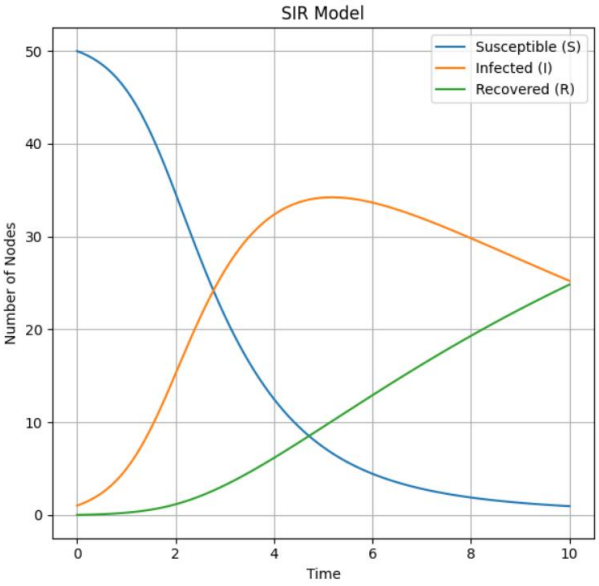
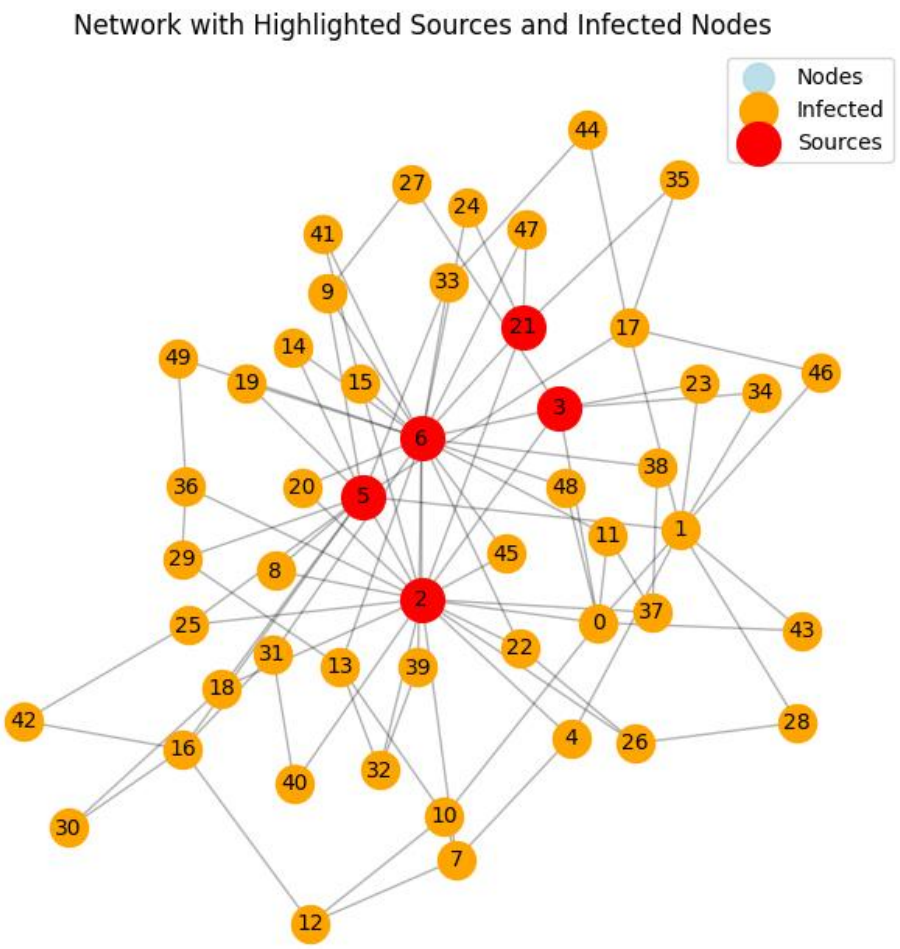


Рис. 4.3. Поширення інформації в моделі SIR




```
Synchronization (R) at time step 10: 0.1327
Top influential nodes: [2, 6, 5, 3, 21]
Potential sources of disinformation: [2, 3, 5, 6, 21]
```

Рис.4.4. Мережа з виділеними джерелами поширення та інфікованими вузлами

У сучасному інформаційному просторі розуміння динаміки поширення інформації є одним із ключових завдань для боротьби з дезінформацією, прогнозування вірусних трендів та оптимізації комунікаційних стратегій. покращена Модель Курамото із застосуванням епідемічної моделі дозволяє моделювати процес поширення інформації у мережі, враховуючи як динаміку взаємодії між користувачами, так і їхній поточний стан (інфікований, здоровий або відновлений) [131].

1. Інтеграція епідемічної моделі SIR

Формула моделі:

$$\theta_i = \omega_i + \frac{K}{N}\sum_{j=1}^{N} \mathrm{A_{ij}}\sin\left(\theta_j - \theta_i\right) + \gamma(I_i - R_i),$$

поєднує:

- Динамічну взаємодію вузлів через коефіцієнт зв'язку K, що враховує вплив сусідніх вузлів.
- Епідемічний підхід, що враховує стан вузлів:

I_i: Нормалізована активність вузла (інфікованість).

R_i: Нормалізована відновленість вузла.

2. Моделювання реальних процесів**.** Епідемічна модель дозволяє описати процес поширення інформації як аналог поширення "вірусу", що відображає механізми вірусного контенту чи дезінформації.

3. Гнучкість моделі. Модель може бути адаптована для різних видів мереж (наприклад, соціальні мережі, корпоративні зв'язки) і різних видів інформації (фейкові новини, рекламні кампанії, суспільно важливі повідомлення).

Для ілюстрації була створена програма, яка:

- Імітує соціальну мережу у вигляді випадкового графу (Barabási–Albert модель створює безмасштабний граф (scale-free network)).
- Використовує епідемічний підхід для моделювання поширення інформації.
- Враховує стан кожного вузла: інфікований (I_i) чи відновлений (R_i).
- Виводить графік синхронізації вузлів для аналізу поширення інформації.

Програма реалізує наступні етапи (Додаток И):

1. У даному дослідженні використано безмасштабну мережу (Scale-Free Network), створену за допомогою моделі Barabási–Albert.

Етапи роботи програми:

1. Генерація безмасштабної мережі (Scale-Free Network)

На першому етапі створюється граф на основі моделі Barabási–Albert. Ця модель формує граф, у якому деякі вузли мають значно більшу кількість

зв’язків (так звані "хаби"), тоді як більшість вузлів з’єднані з обмеженою кількістю сусідів. Така структура відображає особливості реальних соціальних та інформаційних мереж, де поширення інформації відбувається нерівномірно, а ключову роль відіграють впливові користувачі [10].

Процес генерації мережі базується на механізмах зростання та преференційного приєднання. Спочатку створюється невеликий граф, після чого нові вузли додаються поступово, приєднуючись до вже існуючих з імовірністю, пропорційною кількості їхніх зв’язків. Це забезпечує формування мережі, що характеризується степеневим розподілом степенів вузлів, що є характерним для соціальних платформ, інтернет-мереж та інших складних систем [83].

2. Ініціалізація параметрів моделі

Кожному вузлу мережі присвоюються наступні характеристики:

- Фаза (θ), що відповідає за стан вузла в динаміці Курамото;
- Природна частота (ω), що відображає індивідуальну схильність до поширення інформації;
- Стани SIR (S - сприйнятливі, I - інфіковані, R - відновлені), які моделюють динаміку поширення дезінформації.

3. Обчислення динаміки фаз вузлів

Вузли оновлюють свої фази за рівнянням:

$$\theta_i = \omega_i + \frac{K}{N}\sum_{j=1}^{N} \mathrm{A_{ij}} \sin\left(\theta_j - \theta_i\right) + \gamma(I_i - R_i),$$

де кожен доданок відповідає за певні фактори впливу:

— Природні частоти (ω) враховують індивідуальні властивості вузла.

— Сумарний вплив сусідів у мережі (зв’язки між вузлами) визначає узгодження фаз.

— Терміни $\gamma(I_i - R_i)$ моделюють вплив поширення інформації або дезінформації.

4. Реалізація механізму поширення дезінформації (SIR-модель)

У моделі використовується епідеміологічний підхід для відстеження поширення інформації. Вузли можуть змінювати свій стан:

- Сприйнятливі вузли (*S*) можуть отримати дезінформацію та стати інфікованими (*I*).
- Інфіковані вузли (*I*) передають інформацію своїм сусідам.
- Відновлені вузли (*R*) перестають поширювати інформацію.

5. Виявлення джерела дезінформації

Програма аналізує центральність вузлів та визначає найбільш впливових користувачів, які водночас є інфікованими. Це дозволяє ідентифікувати можливі джерела поширення інформації та розробити стратегії протидії.

6. Візуалізація результатів

Для аналізу динаміки поширення інформації генеруються графіки:

- Синхронізація вузлів – показує динаміку змін фаз у мережі(рис. 4.2).
- Графік SIR-моделі – демонструє зміну частки сприйнятливих, інфікованих та відновлених вузлів у часі (рис. 4.3).
- Мережевий граф – виділяє основні джерела поширення дезінформації (рис. 4.4).

Отже, дезінформація є однією з найсерйозніших загроз інформаційної безпеки сучасного суспільства, оскільки вона здатна швидко поширюватися через соціальні мережі, впливаючи на громадську думку, викликаючи соціальні конфлікти та підриваючи довіру до офіційних джерел. Тому ефективні методи виявлення та протидії дезінформації є надзвичайно актуальними.

Запропонована покращена модель Курамото, інтегрована з епідемічною SIR-моделлю, дозволяє моделювати поширення інформації в соціальних мережах, враховуючи взаємодію користувачів та їхній поточний стан (сприйнятливий, інфікований або відновлений). Використання безмасштабної мережі (Scale-Free Network) на основі моделі Barabási–Albert забезпечує реалістичне відображення соціальних зв’язків, де ключову роль відіграють впливові користувачі (хаби).

Результати симуляцій показали, що високий рівень синхронізації вузлів у мережі вказує на активне поширення інформації, що може бути використано для виявлення потенційно вірусного контенту або осередків дезінформації. Аналіз динаміки моделі дозволяє локалізувати джерела поширення неправдивої інформації, оцінити ефективність різних стратегій інформаційного впливу та прогнозувати майбутні інформаційні тренди.

Таким чином, розроблена модель є ефективним інструментом для дослідження поширення дезінформації, оптимізації інформаційних кампаній та забезпечення інформаційної безпеки. Її подальше вдосконалення та застосування в реальних сценаріях може значно підвищити ефективність боротьби з інформаційними загрозами та сприяти збереженню довіри до достовірних джерел інформації.

4.3. Метод аналізу ключових вузлів для знаходження впливових користувачів у соціальних мережах на основі вдосконаленої моделі Курамото

У сучасному світі ідентифікація впливових користувачів у соціальних мережах є ключовим завданням для вирішення багатьох проблем, таких як ефективне поширення інформації, протидія дезінформації та оптимізація маркетингових кампаній. Одним із потужних інструментів для розв’язання цього завдання є покращена Модель Курамото із застосуванням моделі впливових користувачів. Цей підхід дозволяє враховувати як динамічну поведінку вузлів, так і їхню структурну значущість у мережі.

Ефективність методу полягає:

1. Інтеграція динамічної та структурної інформації. Формула моделі:

$$\theta_i = \omega_i + K\sum_{j=1}^{N} \mathrm{A_{ij}} \sin\left(\theta_j - \theta_i\right) + \delta * C_i,$$

поєднує:

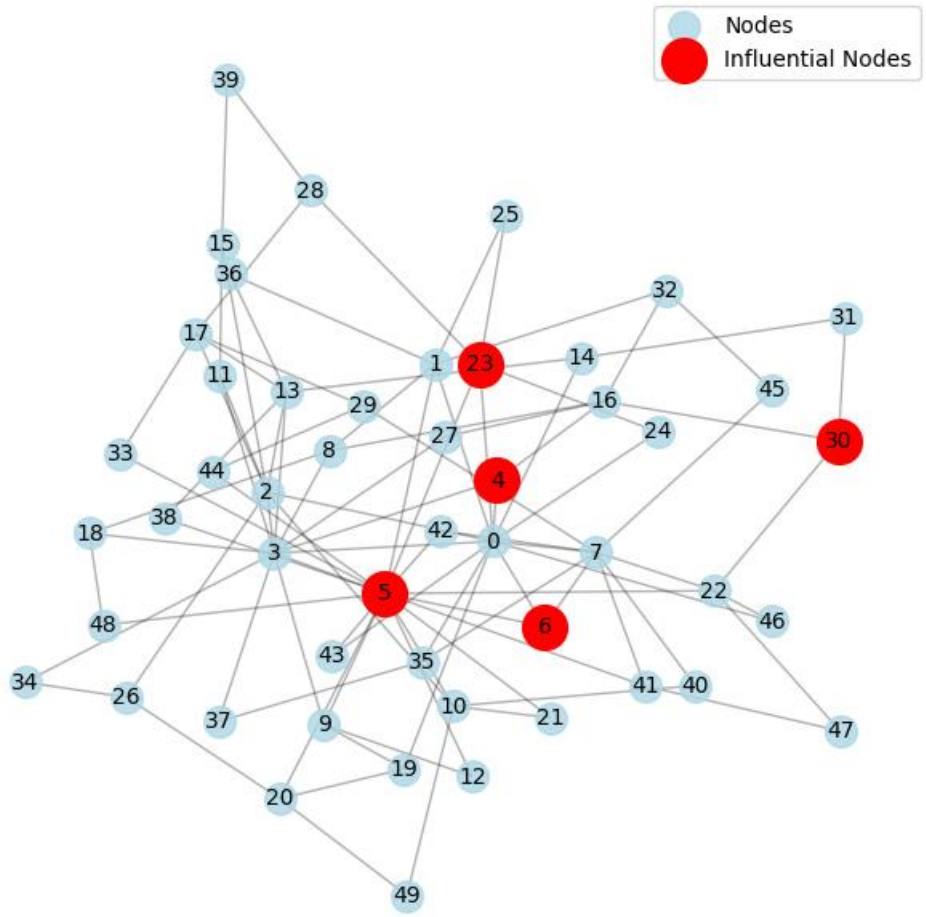
- Динамічні аспекти (ω_i, $\sin(\theta_j - \theta_i)$), які описують взаємодію вузлів у процесі поширення інформації.
- Структурні аспекти (C_i), що враховують значущість вузла в мережі через його центральність.

2. Глобальний та локальний вплив. Модель дозволяє аналізувати, як локальні зв’язки між вузлами (враховані через матрицю суміжності A_{ij}) впливають на глобальне поширення інформації. Це дає змогу ідентифікувати вузли, які є "локомотивами" інформаційних процесів.

3. Адаптивність до різних типів мереж. Використання різних метрик центральності (C_i, наприклад, степенева центральність або центральність векторів власних значень) дає змогу застосовувати модель до різноманітних структур соціальних мереж.

Для наочності була створена програма, яка (Додаток І):

- Моделює соціальну мережу з використанням випадкового графу.
- Обчислює центральність вузлів для визначення їхньої структурної важливості.
- Використовує ітеративний підхід для моделювання фаз вузлів у процесі поширення інформації.
- Виводить результати у вигляді графіка, на якому відображені впливові вузли [131] рис. 4.5.




```
Top-5 influential users: [ 5  4 30 23  6]
Phases of the influential users: [9.50088586 8.92422304 8.86063183 7.30447873 6.76324445]
```

Рис. 4.5. Граф знаходження впливових користувачів

Програма реалізує наступні кроки:

1. Генерація випадкової мережі

Створюється граф на основі моделі Barabási–Albert. Ця модель формує граф, у якому деякі вузли мають значно більшу кількість зв’язків (так звані "хаби"), тоді як більшість вузлів з’єднані з обмеженою кількістю сусідів. Така структура відображає особливості реальних соціальних та інформаційних мереж, де поширення інформації відбувається нерівномірно, а ключову роль відіграють впливові користувачі.

Процес генерації мережі базується на механізмах зростання та преференційного приєднання. Спочатку створюється невеликий граф, після чого нові вузли додаються поступово, приєднуючись до вже існуючих з

імовірністю, пропорційною кількості їхніх зв’язків. Це забезпечує формування мережі, що характеризується степеневим розподілом степенів вузлів, що є характерним для соціальних платформ, інтернет-мереж та інших складних систем.

2. Ініціалізація параметрів вузлів:

– Кожному вузлу присвоюється *природна частота* (ω), яка визначає його індивідуальну схильність до зміни стану. Частоти генеруються випадково відповідно до нормального розподілу.

– *Початкові фази* (θ) кожного вузла також визначаються випадковим чином у межах від 0 до 2π. Це відповідає початковому розподілу інформації або стану користувачів у мережі.

– Обчислюється *центральність вузлів* (C) за допомогою *degree centrality* (міра важливості вузла в мережі, яка визначається кількістю його зв’язків (сусідніх вузлів)). Це дозволяє оцінити важливість вузла в мережі на основі кількості його зв’язків..

Для вузла і центральність за ступенем визначається як:

$$C_D(i) = \frac{\deg(i)}{N-1},$$

де $\deg(i)$ - кількість зв’язків вузла i, а N — загальна кількість вузлів у мережі.

Вузли з високим значенням *degree centrality* є важливими, оскільки вони можуть швидше передавати інформацію або впливати на більшу кількість інших вузлів. У безмасштабних мережах (Scale-Free Networks) високі значення центральності зазвичай мають "хаби" — вузли, що значно перевищують інші за кількістю зв’язків.

3. Моделювання динаміки поширення інформації:

На кожному часовому кроці виконується оновлення фаз вузлів за рівнянням, яке включає три складові:

- Природні частоти (ω) – відображають індивідуальні особливості вузлів.

- Взаємний вплив сусідів через зв'язки $(K\sum_{j=1}^{N} A_{ij} sin(\theta_j - \theta_i) + \delta * C_i,)$ – моделює узгодження фаз вузлів у межах мережі.
- Вплив центральності (δ * C) – відображає вплив важливих вузлів на поширення інформації.
- Оновлення фаз здійснюється за допомогою інтеграційного кроку (dt = 0.1), що імітує динаміку змін інформаційного середовища.

4. Визначення впливових вузлів:

– Після завершення симуляції впливовість вузлів оцінюється на основі значень фази θ. Вузли з найвищими значеннями фаз вважаються найбільш впливовими користувачами у мережі.

– Визначається топ-5 найбільш впливових вузлів, які мають найбільший внесок у поширення інформації.

5. Візуалізація результатів:

– Графічне представлення мережі включає:

- Вузли мережі (відображені у світло-блакитному кольорі).
- Виділення впливових вузлів (позначені червоним кольором).
- Відображення зв'язків між вузлами для аналізу структури мережі.

– Для візуалізації використовується spring layout (метод розташування вузлів у графі на основі моделі пружин, де вузли відштовхуються, а зв'язки притягують їх для природного вигляду), який допомагає наочно продемонструвати взаємозв'язки між вузлами.

Програма дозволяє аналізувати поширення інформації в соціальних мережах та виявляти ключових агентів впливу, що може бути корисним для дослідження динаміки дезінформації та ефективності інформаційних кампаній.

Програмний код дає такі результати:

1. Визначення ключових вузлів**.** Програма дозволяє ідентифікувати ключових користувачів, які мають найбільший вплив на поширення інформації. Це може бути корисним для стратегій боротьби з дезінформацією або розповсюдження важливих повідомлень.

2. Аналіз поширення інформації. Симуляція моделює реальні соціальні мережі, дозволяючи зрозуміти динаміку поширення інформації в них.

3. Оптимізація ресурсів. Знання про впливових вузлів може допомогти оптимально розподілити ресурси для підтримки чи протидії певним інформаційним потокам.

Ось тому ефективність підходу для пошуку впливових користувачів є:

1. Простота реалізації**.** Модель базується на універсальних математичних принципах і може бути легко адаптована до різних типів соціальних мереж.

2. Інтуїтивна інтерпретація**.** Результати симуляції (фази вузлів) відображають, наскільки сильно кожен вузол впливає на інформаційний потік.

3. Можливість розширення**.** Модель може бути доповнена іншими параметрами, такими як обмеження ресурсів або тип інформації (правдива чи дезінформація).

Отже, покращена Модель Курамото із застосуванням моделі впливових користувачів є ефективним інструментом для ідентифікації ключових вузлів у мережі. Розроблена програма дозволяє не лише визначати впливових користувачів, але й наочно демонструвати результати, що робить її придатною для практичного використання у сфері соціальних мереж, маркетингу та протидії дезінформації.

Програма реалізує симуляцію поширення інформації в соціальній мережі на основі покращеної моделі Курамото з урахуванням центральності вузлів. Вона визначає впливових користувачів, які мають найбільший вплив на поширення інформації.

4.4. Методи використання покращеної моделі Курамото для виявлення ключових вузлів, що сприяє протидії дезінформаційним процесам у соціальних мережах

Реалізація вдосконалених моделей Курамото у програмному забезпеченні для забезпечення інформаційної безпеки держави є перспективним напрямом, що дозволяє ефективно протидіяти дезінформації, координованим інформаційним атакам і маніпуляціям у соціальних мережах. Інтеграція таких моделей у державні системи моніторингу та аналізу інформаційних потоків забезпечує комплексний підхід до виявлення загроз і управління інформаційною безпекою.

Архітектура програмного забезпечення

Програмний продукт для забезпечення інформаційної безпеки держави на основі вдосконалених моделей Курамото може складатися з кількох основних модулів:

1. Модуль збору та обробки даних

Цей модуль здійснює збір даних із соціальних мереж, форумів, новинних ресурсів і блогів. Він інтегрується з API популярних платформ (Facebook, Twitter, Instagram, Telegram) для отримання публічних постів, коментарів, хештегів, лайків, поширень і підписок. Додатково модуль реалізує попередню обробку даних, очищення та нормалізацію для подальшого аналізу.

2. Модуль побудови мережевої моделі

На основі зібраних даних будується граф інформаційних взаємодій, де вузли представляють користувачів або інформаційні джерела, а ребра – зв’язки між ними (лайки, поширення, підписки). Для моделювання динаміки інформаційних потоків використовується вдосконалена модель Курамото, яка адаптована під особливості соціальних мереж.

3. Аналітичний модуль із використанням покращених моделей Курамото

У цьому модулі реалізуються різні покращені варіанти моделі Курамото:

- Cascade Model (Каскадна модель): моделює поширення контенту через спонтанне прийняття рішення користувачами.
- SIR Model (Епідемічна модель): аналізує розповсюдження шкідливої інформації з урахуванням користувачів у стані сприйняття, зараження та відновлення.
- Rumor Spreading Model (Модель поширення чуток): моделює динаміку поширення недостовірної інформації.
- Influential Spreaders Model (Модель впливових користувачів): ідентифікує ключових поширювачів інформації, що дозволяє вчасно блокувати інформаційні атаки.

4. Модуль візуалізації результатів

Результати аналізу подаються у вигляді інтерактивних графіків і мережевих діаграм. Це дозволяє операторам системи в реальному часі спостерігати за поширенням інформації, ідентифікувати впливових користувачів і потенційні джерела дезінформації.

5. Модуль прийняття рішень та автоматизації дій

На основі отриманих аналітичних даних модуль формує рекомендації для прийняття рішень щодо блокування або обмеження доступу до джерел дезінформації. У разі необхідності передбачена інтеграція з системами кібербезпеки для автоматичного реагування на загрози.

Переваги впровадження покращених моделей Курамото:

— Оперативність реагування на інформаційні загрози
Завдяки швидкій обробці великих обсягів даних та моделюванню динаміки інформаційних потоків у реальному часі система дозволяє оперативно виявляти та локалізовувати джерела дезінформації.

— Комплексний аналіз інформаційних потоків
Поєднання різних покращених моделей Курамото дозволяє глибше аналізувати структуру мережі, динаміку поширення контенту і визначати ключових гравців у розповсюдженні інформації.

— Прогнозування поширення інформації
Моделі дозволяють прогнозувати, як інформація буде поширюватися мережею, що дає можливість заздалегідь розробити стратегії протидії.

— Адаптивність до різних типів загроз
Програмний продукт легко адаптується до нових типів інформаційних атак завдяки модульній архітектурі, що забезпечує швидке оновлення алгоритмів аналізу.

Результати реалізації програмного забезпечення

- Ідентифікація дезінформаційних атак: автоматизоване виявлення і локалізація джерел фейкових новин і пропаганди.
- Визначення впливових користувачів: швидке виявлення акаунтів, які мають вирішальний вплив на поширення інформації.
- Моделювання сценаріїв поширення: прогнозування наслідків поширення інформації та оцінка ефективності заходів протидії.
- Інтерактивна візуалізація: наочне представлення структури інформаційних потоків, що спрощує прийняття оперативних рішень.

Тому, реалізація покращених моделей Курамото у програмному забезпеченні для забезпечення інформаційної безпеки держави є потужним інструментом для боротьби з дезінформацією та інформаційними атаками. Комплексний підхід до аналізу соціальних мереж, інтеграція різних математичних моделей і автоматизація процесів аналізу забезпечують високу ефективність виявлення загроз і мінімізації їхніх наслідків. Такий підхід дозволяє своєчасно реагувати на виклики в інформаційному просторі, забезпечуючи стійкість і захист інформаційного середовища держави.

Також вдосконалені моделі Курамото для забезпечення інформаційної безпеки держави можна інтегрувати в різні програмні платформи, що спеціалізуються на моніторингу інформаційних потоків, аналізі великих даних та кібербезпеці. Наведено приклади програмного забезпечення, в якому такі моделі можуть бути ефективно реалізовані [78]:

І. Системи моніторингу інформаційного простору — це спеціалізовані програмні комплекси, призначені для збору, аналізу та обробки інформації з відкритих джерел, таких як соціальні мережі, новинні ресурси, блоги, форуми тощо. Їх головна мета полягає в оперативному виявленні потенційних загроз інформаційній безпеці, дезінформаційних кампаній, а також у дослідженні суспільних настроїв і тенденцій.

Ці системи активно застосовуються для захисту державного інформаційного простору, виявлення маніпулятивних інформаційних потоків і своєчасного реагування на можливі загрози. Завдяки використанню алгоритмів штучного інтелекту, машинного навчання і вдосконалених математичних моделей (зокрема, покращених моделей Курамото) такі системи здатні ефективно обробляти великі обсяги даних у реальному часі.

1. Системи моніторингу медіа (Media Monitoring Systems)

Системи моніторингу медіа забезпечують автоматизований збір і аналіз інформації з новинних сайтів, соціальних мереж, блогів, форумів та інших публічних джерел. Вони фільтрують і систематизують велику кількість інформації за допомогою тематичних ключових слів, тегів або категорій. Існують такі платформи:

- YouScan — система для моніторингу згадок у соціальних мережах із вбудованим аналізом зображень [117].
- SemanticForce — платформа для глибокого аналізу текстових даних і медіа-контенту [95].
- Brandwatch — інструмент аналітики соціальних медіа, що допомагає компаніям стежити за репутацією бренду [13].

Використання покращеної моделі Курамото:

– Виявлення фейкових новин: Аналіз синхронізації інформаційних потоків для визначення джерел і шляхів поширення дезінформації.

– Ідентифікація впливових користувачів: Моделювання мережевої активності для виявлення лідерів думок, які можуть сприяти або протидіяти поширенню фейків.

– Локалізація джерел дезінформації**:** Використання мережевих моделей для аналізу структур розповсюдження контенту і визначення вузлів, де виникає деструктивна інформація.

2. Системи аналізу соціальних медіа (Social Media Analytics) Ці платформи зосереджені на детальному аналізі взаємодії користувачів у соціальних мережах. Вони збирають інформацію про тренди, поведінкові патерни аудиторії, виявляють аномалії в поширенні інформації та аналізують загальний інформаційний фон. Використовуються такі платформи:

- Crimson Hexagon — аналітична платформа, що використовує AI для розуміння споживацької поведінки та соціальних трендів [32].
- Talkwalker — інструмент для моніторингу соціальних медіа та інтернету, який аналізує брендові згадки, емоційний тон і тенденції [105].

Використання покращеної моделі Курамото дозволяє ефективно аналізувати динаміку поширення інформації в соціальних мережах. Завдяки моделюванню інформаційних потоків у реальному часі можна краще зрозуміти, як контент стає вірусним, які фактори сприяють цьому процесу, а також як реагує мережа на появу нової інформації.

Одним із ключових напрямів застосування моделі є виявлення інформаційних атак. Координовані кампанії з поширення фейків, маніпуляцій чи пропаганди часто супроводжуються синхронізованою поведінкою користувачів або бот-мереж. Модель Курамото дозволяє виявити таку поведінку через аналіз синхронності дій у мережі.

Ще одним важливим аспектом є прогнозування вірусних трендів. Спостереження за активністю вузлів та аналіз темпів синхронізації дає змогу виявляти потенційні сплески активності, які можуть свідчити про підготовку до масштабного інформаційного впливу чи кампанії.

Інтеграція покращених моделей Курамото у системи моніторингу забезпечує низку переваг. Серед них — оперативне реагування на загрози завдяки аналізу інформаційних потоків у режимі реального часу; висока точність виявлення дезінформації завдяки врахуванню впливових вузлів; можливість

прогнозування майбутніх атак на основі аналізу динаміки мережі; а також наочна візуалізація інформаційних потоків, що дозволяє краще зрозуміти структуру мережі, маршрути поширення інформації та зв’язки між учасниками.

Отже, системи моніторингу інформаційного простору відіграють ключову роль у забезпеченні інформаційної безпеки. Інтеграція покращених моделей Курамото в ці системи дозволяє ефективно ідентифікувати джерела дезінформації, впливових користувачів і прогнозувати поширення шкідливих інформаційних потоків. Це відкриває нові можливості для своєчасного виявлення загроз, підвищення стабільності інформаційного середовища та забезпечення національної безпеки.

II. Платформи для обробки великих даних (Big Data Platforms)

У сучасних умовах масової цифровізації та стрімкого зростання обсягів інформації, що генерується користувачами соціальних мереж, надзвичайно важливою є здатність ефективно обробляти, аналізувати й інтерпретувати ці дані. Для цього використовуються платформи для обробки великих даних, які дозволяють працювати з величезними обсягами інформації в реальному часі. Інтеграція покращених моделей Курамото в такі платформи забезпечує масштабований і високоточний аналіз інформаційних потоків, що є критично важливим для виявлення дезінформації та ключових поширювачів шкідливого контенту.

1. Apache Spark, Hadoop, Elasticsearch (платформи для обробки та аналізу великих розподілених даних у реальному часі)

- Apache Spark — високопродуктивна платформа для обробки великих даних, що забезпечує швидку обробку потокових і пакетних даних. Spark дозволяє масштабувати обчислення на тисячі серверів і забезпечує обробку даних у реальному часі [6].
- Apache Hadoop — фреймворк для розподіленого зберігання та обробки великих обсягів даних. Hadoop складається з кількох модулів, включаючи HDFS (система зберігання) та MapReduce (модель обробки даних) [6].

- Elasticsearch — пошуковий і аналітичний рушій, який дає змогу швидко обробляти великі обсяги текстових і неструктурованих даних. Платформа ідеально підходить для аналізу соціальних медіа, моніторингу інформаційних потоків і пошуку аномалій [40].

Інтеграція покращеної моделі Курамото в ці платформи дозволяє реалізувати масштабований аналіз великих обсягів даних із соціальних мереж у реальному часі. Завдяки цьому можна:

– Виявляти аномальні патерни поведінки, які можуть свідчити про організовані кампанії поширення дезінформації.

– Аналізувати динаміку інформаційних потоків, оцінюючи рівень синхронізації між користувачами, що допомагає визначити скоординовані атаки.

– Ідентифікувати джерела шкідливих інформаційних кампаній, використовуючи зв’язки між вузлами в мережі.

Spark і Hadoop дозволяють розподіляти обчислення на великі кластери серверів, що робить можливим обробку гігантських обсягів даних навіть із великих соціальних платформ (наприклад, Facebook, Twitter). Elasticsearch, своєю чергою, забезпечує швидкий пошук і аналітику текстових повідомлень, що полегшує моніторинг дезінформаційних кампаній.

2. Google BigQuery, Amazon Redshift (платформи для високошвидкісної аналітики та обробки великих обсягів даних у хмарному середовищі)

– Google BigQuery — хмарна платформа для інтерактивного аналізу великих обсягів даних. Вона підтримує SQL-запити та дозволяє обробляти терабайти й петабайти даних із мінімальною затримкою [53].

– Amazon Redshift — масштабована система для зберігання та аналізу даних, яка оптимізована для виконання складних аналітичних запитів над великими наборами даних [3].

Використання покращеної моделі Курамото в аналітичних платформах дає змогу здійснювати глибокий аналіз як структурованих, так і неструктурованих даних у соціальних мережах. Інтеграція цієї моделі дозволяє краще зрозуміти динаміку інформаційних процесів і виявити критичні точки в мережі.

Завдяки аналізу взаємодій користувачів модель дає змогу виявляти ключові вузли інформаційних мереж, а також ідентифікувати впливових користувачів, які можуть суттєво впливати на поширення контенту. Це критично важливо для оцінки інформаційної стійкості мережі та вчасного реагування на загрози.

Модель Курамото також ефективно використовується для моделювання процесів поширення інформації, що дає змогу прогнозувати потенційні інформаційні атаки та загрози ще до їх реалізації. Аналіз поведінкових патернів користувачів дозволяє виявляти нетипові або підозрілі сплески активності, які можуть сигналізувати про початок скоординованої кампанії дезінформації.

Аналітичні системи, такі як BigQuery і Redshift, забезпечують технічну можливість обробки великих обсягів даних із різних джерел — від простих текстових повідомлень до складних графових структур. Це забезпечує комплексний підхід до виявлення дезінформації, враховуючи як сам контент, так і структуру взаємодій між учасниками мережі.

Переваги використання Big Data платформ із покращеною моделлю Курамото:

1. Масштабованість: Платформи підтримують обробку даних у масштабах національних інформаційних систем, що дозволяє аналізувати величезні обсяги інформації з різних джерел.
2. Обробка даних у реальному часі: Інтеграція з покращеною моделлю Курамото забезпечує оперативний аналіз інформаційних потоків і швидке виявлення загроз.
3. Глибокий аналіз взаємодій: Поєднання мережевого аналізу та математичних моделей дозволяє отримати точну картину поширення інформації в мережі.
4. Ідентифікація джерел загроз: Платформи дозволяють виявляти не лише фейковий контент, а й користувачів або групи, які поширюють дезінформацію.
5. Гнучкість і адаптивність: Платформи легко інтегруються з іншими інструментами аналізу й можуть адаптуватися під конкретні завдання інформаційної безпеки.

Отже, платформи для обробки великих даних, такі як Apache Spark, Hadoop, Elasticsearch, Google BigQuery і Amazon Redshift, є незамінними інструментами для аналізу та протидії дезінформації в соціальних мережах. Інтеграція покращеної моделі Курамото в ці системи дає можливість не тільки оперативно виявляти шкідливий контент, а й прогнозувати інформаційні атаки, ідентифікувати впливових користувачів та ефективно захищати інформаційний простір країни. Це відкриває нові горизонти в забезпеченні національної безпеки, боротьбі з фейками та маніпуляціями в цифровому середовищі.

III. Платформи кібербезпеки (Cybersecurity Platforms)

У сучасних умовах кіберзагроз особливого значення набувають спеціалізовані платформи кібербезпеки, які забезпечують комплексний захист інформаційного простору. Такі системи аналізують великий обсяг даних у режимі реального часу, виявляють потенційні загрози, фіксують інциденти безпеки та забезпечують автоматизовану реакцію на них [102]. Інтеграція покращених моделей Курамото в ці платформи дозволяє значно підвищити ефективність виявлення та нейтралізації дезінформаційних кампаній, фейкових новин і інформаційних атак.

1. SIEM-системи (Security Information and Event Management) — це комплексні рішення для збору, обробки, аналізу та зберігання інформації про події безпеки в інформаційних системах. Вони дозволяють організаціям отримувати повну картину про всі події в мережі та швидко реагувати на загрози. До найпопулярніших SIEM-рішень належать:

- Splunk — потужна платформа для збору, обробки та аналізу великих обсягів даних, яка дозволяє виявляти аномалії, відстежувати події в реальному часі та автоматизувати кіберзахист [101].
- IBM QRadar — рішення для аналізу інформаційних потоків, що дозволяє ідентифікувати загрози та корелювати події для глибокого аналізу атак [58].
- ArcSight — інтегрована система для моніторингу безпеки, яка забезпечує глибокий аналіз подій та виявлення складних кіберзагроз [7].

Інтеграція покращеної моделі Курамото в SIEM-системи дозволяє значно підвищити ефективність аналізу інформаційних потоків. Це досягається завдяки здатності моделі аналізувати динаміку взаємодій між елементами мережі та виявляти скоординовані інформаційні атаки [102].

Однією з ключових можливостей є виявлення інформаційних атак. SIEM-системи, доповнені моделлю Курамото, можуть фіксувати скоординовані кампанії з поширення дезінформації через аналіз синхронізації інформаційних потоків серед користувачів.

Крім того, система забезпечує аналіз підозрілих інформаційних потоків. Виявлення раптових сплесків активності серед окремих груп користувачів може вказувати на початок фейкової кампанії або масштабної дезінформаційної атаки.

Ще однією перевагою є моніторинг активності бот-мереж. Аналіз фазових зрушень і рівня синхронізації між окремими вузлами дає змогу ідентифікувати бот-мережі, які діють скоординовано з метою поширення фейків.

2. Threat Intelligence Platforms (TIP) — це спеціалізовані системи для збору, обробки, аналізу та обміну інформацією про кіберзагрози. TIP допомагають організаціям передбачати потенційні атаки, аналізувати поведінку загроз і забезпечувати проактивний захист [110]. Серед відомих платформ:

- MISP (Malware Information Sharing Platform & Threat Sharing): Відкрита платформа для обміну інформацією про кіберзагрози, що підтримує автоматизоване виявлення і аналіз шкідливих кампаній [26].
- ThreatConnect — комерційна платформа для інтеграції розвідувальних даних про загрози з іншими системами безпеки, яка забезпечує аналіз і автоматизовану реакцію на загрози [110].

Інтеграція покращеної моделі Курамото в TIP-платформи дозволяє суттєво підвищити ефективність виявлення джерел дезінформації та кіберзагроз. Завдяки цій моделі платформи отримують змогу глибше аналізувати мережеві взаємодії та оперативно реагувати на інформаційні атаки.

Однією з ключових функцій є виявлення джерел дезінформації в реальному часі. Модель Курамото дозволяє відстежувати фазові взаємодії між вузлами

мережі, що дає змогу точно ідентифікувати користувачів, які поширюють фейки чи шкідливий контент.

Також забезпечується інтеграція з іншими системами безпеки. TIP-платформи можуть автоматично обмінюватися даними з SIEM-системами, антивірусними рішеннями та іншими інструментами кіберзахисту, що створює єдину екосистему для ефективної протидії загрозам.

Крім того, автоматизована реакція на загрози дозволяє швидко локалізувати джерела інформаційних атак. Модель виявляє вузли, які демонструють підозрілу синхронізовану поведінку, й може ініціювати їх блокування або ізоляцію.

А також, завдяки прогнозуванню нових загроз, система здатна аналізувати зміни в інформаційних потоках і передбачати потенційні дезінформаційні кампанії ще до їх активної реалізації. Це надає важливу перевагу у зміцненні інформаційної безпеки.

Переваги використання покращеної моделі Курамото в платформах кібербезпеки:

– Проактивний захист: Завдяки здатності виявляти скоординовані дії та аномальні сплески активності, моделі Курамото забезпечують оперативне реагування на загрози.

– Інтеграція з існуючими системами: Модель легко інтегрується в інфраструктуру кіберзахисту, підсилюючи функціонал SIEM- і TIP-систем.

– Глибокий аналіз мережевих взаємодій: Система аналізує поведінкові патерни користувачів, що дозволяє виявляти навіть складні та масовані інформаційні атаки.

– Автоматизована обробка даних: Автоматизоване виявлення дезінформації та реагування на загрози зменшує час і ресурси, необхідні для обробки інцидентів.

Інтеграція покращеної моделі Курамото в платформи кібербезпеки суттєво підвищує ефективність виявлення й нейтралізації дезінформаційних кампаній. SIEM-системи дозволяють швидко реагувати на сплески підозрілої активності та блокувати шкідливий контент, тоді як TIP-платформи забезпечують глибокий

аналіз джерел загроз і автоматизоване реагування. Поєднання цих підходів дозволяє створити надійну систему захисту інформаційного простору, здатну ефективно протидіяти дезінформації та іншим кіберзагрозам.

IV. Спеціалізовані платформи для інформаційної безпеки держави

У сучасному світі, де дезінформація і кіберзагрози стали інструментами гібридних воєн і політичного тиску, держави зобов'язані впроваджувати високотехнологічні платформи для моніторингу та забезпечення інформаційної безпеки. Ці платформи спрямовані на виявлення і нейтралізацію загроз, таких як інформаційні атаки, фейкові новини, пропаганда і маніпуляції в соціальних мережах. Вдосконалені моделі Курамото відіграють ключову роль у таких системах, забезпечуючи глибокий аналіз інформаційних потоків та ефективне реагування на потенційні загрози.

Системи кіберзахисту державних структур, такі як Кіберполіція України, CERT-UA (Computer Emergency Response Team Ukraine) [20] та Служба безпеки України (СБУ), займають центральне місце в забезпеченні інформаційної безпеки. Вони зосереджуються на моніторингу кіберзагроз, аналізі атак на державні ресурси та розробці заходів протидії. Використання вдосконалених моделей Курамото дозволяє цим структурам аналізувати, як інформація поширюється мережею, і визначати ключові джерела атак. Наприклад, моделі, що базуються на епідемічному підході або каскадній теорії, допомагають оцінити масштабність інформаційних кампаній і розробити стратегії їх стримування.

Ще одним важливим напрямком є платформи стратегічних комунікацій, які аналізують глобальні інформаційні потоки. Наприклад, платформа GDELT (Global Database of Events, Language, and Tone) забезпечує моніторинг світових інформаційних трендів і тональності медіа [49]. Інтеграція моделей Курамото у такі платформи дозволяє глибше розуміти механізми поширення інформації, оцінювати вплив медіакампаній і прогнозувати майбутні тренди. Аналіз синхронізації інформаційних потоків між різними групами користувачів сприяє розробці ефективних стратегій для протидії дезінформації.

Таким чином, спеціалізовані платформи для інформаційної безпеки держави не лише допомагають у захисті критичної інфраструктури, але й створюють передумови для довгострокової стабільності в інформаційному просторі. Інтеграція покращених моделей Курамото робить ці платформи більш потужними, дозволяючи їм адаптуватися до нових викликів і залишатися ефективними в умовах постійно змінюваних загроз.

V. Інтеграція в програмні рішення на основі штучного інтелекту

Інтеграція покращених моделей Курамото в програмні рішення на основі штучного інтелекту відкриває нові горизонти для аналізу інформаційних потоків і забезпечення інформаційної безпеки. Використання сучасних платформ машинного навчання, таких як TensorFlow, PyTorch, Scikit-learn, [108] дозволяє навчати моделі для автоматичного розпізнавання інформаційних атак і класифікації контенту за рівнем достовірності. Вдосконалені моделі Курамото можуть бути використані для аналізу соціальних графів, що допомагає зрозуміти механізми поширення дезінформації, визначити ключові вузли та розробити стратегії протидії.

Платформи для аналізу графів, такі як Neo4j [79], Gephi [50] і NetworkX [80], забезпечують потужні інструменти для візуалізації мережевих зв’язків та їхнього аналізу. Інтеграція моделей Курамото в ці платформи дозволяє проводити глибокий аналіз поширення інформації, оцінювати вплив окремих вузлів на мережу та прогнозувати динаміку розвитку інформаційних потоків [143]. Такі інструменти не лише надають можливість ефективно ідентифікувати ключових користувачів, але й візуально демонструють взаємозв’язки між ними, що є особливо важливим для прийняття рішень у реальному часі.

Для забезпечення максимальної ефективності вдосконалена модель Курамото має бути інтегрована в комплексну інформаційно-аналітичну платформу. Така платформа повинна включати модулі збору даних із соціальних мереж і ЗМІ, що дозволить агрегувати великі обсяги інформації з різних джерел у реальному часі. Аналітичний блок із реалізацією моделей Курамото буде займатися обробкою даних, ідентифікацією ключових вузлів, аналізом

синхронізації в мережі та виявленням аномалій. Інструменти візуалізації забезпечать наочне уявлення про динаміку інформаційних потоків, дозволяючи краще розуміти механізми поширення контенту та оцінювати ефективність протидії дезінформації.

Крім цього, платформа повинна включати системи автоматичного реагування на інформаційні атаки. Це дозволить оперативно блокувати шкідливий контент, обмежувати діяльність деструктивних акаунтів і захищати інформаційний простір. Таке рішення може бути створене як самостійне державне програмне забезпечення, орієнтоване на захист критичної інфраструктури, або інтегроване в уже існуючі системи кіберзахисту для підвищення їхньої ефективності.

Інтеграція вдосконаленої моделі Курамото в сучасні аналітичні платформи є важливим кроком для посилення інформаційної безпеки держави. Це дозволить більш точно виявляти дезінформацію, прогнозувати інформаційні атаки та ефективно протидіяти їм, формуючи стабільне і безпечне інформаційне середовище.

Висновки до четвертого розділу

1. Досліджено, що ключові вузли в соціальних мережах відіграють критично важливу роль у процесах формування, трансформації та поширення інформації, а також значно впливають на стан інформаційної безпеки держави. Виділено п’ять основних типів ключових вузлів: вузли поширення інформації та дезінформації, впливові користувачі й центральні вузли, посередники, уразливі точки та розповсюджувачі чуток. Визначено, що ідентифікація ключових вузлів у соціальних мережах дозволяє підвищити ефективність інформаційних кампаній шляхом залучення найбільш впливових елементів мережі, своєчасно виявляти джерела дезінформації, будувати стратегії взаємодії з лідерами думок

і посилювати інформаційну безпеку через нейтралізацію уразливих компонентів.

2. Визначено, що.дезінформація є серйозною загрозою для інформаційної безпеки, особливо в умовах гібридних війн, політичної нестабільності та соціальних криз. Тому, законодавча база України поступово адаптується до викликів цифрової доби, визнаючи дезінформацію як інструмент гібридного впливу та визначаючи необхідність боротьби з нею на рівні медіа та національної безпеки. Проте наявні інструменти боротьби з фейками не завжди є достатньо ефективними через динамічний розвиток дезінформаційних технологій. Показано п’ять ключових факторів, що сприяють поширенню дезінформації в соціальних мережах: висока швидкість інформаційних потоків, анонімність учасників мережі, емоційна привабливість контенту, ведення інформаційних війн у межах гібридної агресії, а також низький рівень критичного мислення у частини аудиторії.

3. У межах дослідження вперше було застосовано новий метод для аналізу поширення інформації в соціальних мережах з метою виявлення потенційних джерел дезінформації на основі вдосконаленої моделі Курамото, інтегровану з епідемічною моделлю типу SIR. Такий підхід дозволяє враховувати не лише синхронізацію інформаційних потоків між користувачами, а й поточний стан кожного вузла — чи він сприйнятливий, інфікований (тобто поширює дезінформацію) або відновлений. На основі цієї моделі було розроблено програмний код, що реалізує побудову безмасштабної мережі типу Barabási–Albert (scale-free network) та візуалізує інформаційні процеси у вигляді графа. У результаті на графі чітко виділяються ключові вузли, які демонструють аномальну активність або синхронізацію з іншими — це дає змогу припустити, що саме ці вузли є джерелами або ретрансляторами дезінформації.

4. У межах дослідження запропоновано новий метод виявлення лідерів думок у соціальних мережах шляхом поєднання моделі Курамото з моделлю впливових користувачів. Такий підхід ґрунтується на аналізі синхронізації поведінки вузлів у мережі: якщо кілька вузлів демонструють тісну фазову

узгодженість та високий рівень взаємодії з іншими елементами системи, це може свідчити про їхню важливу роль у поширенні інформації та формуванні громадської думки. Для практичної реалізації методу було розроблено програмний код, який будує граф соціальної мережі на основі безмасштабної структури (Barabási–Albert). У цьому графі кожен вузол відображає окремого користувача, а зв’язки між ними – взаємодії (лайки, репости, коментарі). Завдяки інтеграції моделі Курамото у фазову динаміку мережі стало можливим візуально виділяти ті вузли, які мають найбільшу кількість з’єднань, високий ступінь синхронізації та впливу на інші елементи. Таким чином, програма наочно демонструє потенційно впливових користувачів у графовій моделі, що дозволяє не лише вивчати структуру мережевої взаємодії, а й формувати ефективні стратегії таргетованого інформаційного впливу або захисту від маніпуляцій з боку лідерів думок.

5. Також було запропоновано на основі вдосконаленої моделі Курамото розробити програмний продукт для забезпечення інформаційної безпеки держави, який складається з модулів збору даних, побудови графової моделі, аналітики, візуалізації та автоматизованого прийняття рішень, що дозволяє виявляти джерела дезінформації, ідентифікувати впливових користувачів і моделювати сценарії поширення інформації в реальному часі.

6. Розглянута можливість реалізації вдосконалених моделей Курамото в таких програмних засобах, як системи моніторингу інформаційного простору, аналітичні платформи соціальних медіа, платформи обробки великих даних, системи кібербезпеки, а також спеціалізовані державні інформаційно-аналітичні системи та рішення на основі штучного інтелекту. У зазначених платформах вдосконалені моделі Курамото будуть виконувати функції аналізу синхронної активності користувачів, що дозволяє виявляти скоординовані інформаційні атаки, бот-мережі та кампанії дезінформації.

ВИСНОВКИ

В результаті дисертаційних досліджень, виконаних автором, вирішено актуальне наукове завдання — розроблено нові методи і моделі для ідентифікації ключових вузлів у соціальних мережах з використанням вдосконаленої моделі Курамото. Запропоновані рішення дозволяють значно покращити точність прогнозування поширення інформації, своєчасне виявлення джерел дезінформації та підвищення рівня інформаційної безпеки.В дисертаційному дослідженні отримані такі основні результати:

1. Проведений аналіз існуючих підходів до моделювання динамічних процесів у соціальних мережах та визначення їх обмежень у контексті інформаційної безпеки зокрема — недостатню точність у виявленні синхронної поведінки, обмеженість у врахуванні складної топології мереж (наприклад, scale-free та small-world структур).

2. Запропоновано метод аналізу синхронізації інформаційних процесів у соціальних мережах, який базується на моделі Курамото з урахуванням індивідуальної сприйнятливості користувачів та сили інформаційних зв’язків між ними Така властивість може бути використана для виявлення центрів поширення інформації, зокрема дезінформаційних кампаній, що критично важливо для систем захисту інформаційного простору.

3. Адаптовано класичну модель Курамото до задач аналізу інформаційних процесів у соціальних мережах шляхом урахування специфіки топології таких мереж і поведінки користувачів. Запропоновано її вдосконалення шляхом інтеграції з додатковими математичними моделями: каскадною моделлю, яка враховує порогову активність вузлів і дозволяє імітувати лавиноподібне передавання повідомлень у соціальних мережах, епідемічною моделлю для моделювання станів користувачів (сприйнятливий, інфікований, відновлений), моделлю поширення чуток, яка враховує стадії передачі,

ігнорування та забуття інформації, а також моделлю впливових користувачів для виявлення лідерів думок.

4. Розроблений програмний код, який реалізує як базову, так і вдосконалену модель Курамото для моделювання поширення інформації в соціальних мережах. Він дозволяє порівнювати динаміку двох моделей за показниками фазової синхронізації та ефективності розповсюдження контенту. Проведено експерименти на основі реальних соціальних даних, що продемонстрували переваги вдосконалених моделей у виявленні аномальних вузлів, оцінці рівня впливу та візуалізації ключових осередків синхронної активності.

5. Вперше запропоновано, на основі покращеної моделі Курамото з елементами епідемічної моделі, новий метод ідентифікації ключових вузлів, пов’язаних із розповсюдженням дезінформації. Створено програмний модуль, який формує граф взаємозв’язків між користувачами та візуалізує вузли з підвищеною синхронізацією і «інфекційністю», що дозволяє оперативно виявляти джерела потенційно шкідливого інформаційного впливу.

6. Уперше розроблено метод виявлення лідерів думок у соціальних мережах, що базується на вдосконаленій моделі Курамото у поєднанні з моделлю впливових користувачів. Запропоновано підхід, який дозволяє не лише визначити найвпливовіші вузли у структурі мережі, а й оцінити їхню роль у формуванні загального інформаційного наративу. Результати реалізовано у вигляді графової моделі з візуалізацією зв’язків та ступенем впливовості кожного вузла.

7. Описано можливості практичного використання вдосконалених моделей Курамото в сучасних аналітичних системах і платформах, зокрема в програмних комплексах для аналітики соціальних мереж, обробки великих даних, системах кібербезпеки і рішеннях на основі штучного інтелекту. У цих системах модель виконує функції виявлення синхронізованої активності, аналізу взаємодій у мережі, ідентифікації джерел дезінформації та прогнозування інформаційних загроз.

Отримані результати мають практичне значення для підвищення рівня інформаційної безпеки держави, зокрема в умовах гібридної війни, коли інформаційні атаки використовуються для дестабілізації суспільства. Запропоновані методи дозволяють ідентифікувати загрози, підвищувати ефективність комунікацій та забезпечувати стійкість інформаційної системи до маніпуляційних впливів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aggarwal, C. C. (2016). *Machine Learning for Data Streams: With Practical Examples in MOA*. MIT Press.
2. Allcott, H., & Gentzkow, M. (2017). *Social media and fake news in the 2016 election*. Journal of Economic Perspectives, 31(2), 211–236. https://doi.org/10.1257/jep.31.2.211
3. Amazon Web Services. (n.d.). *Amazon Redshift – Cloud Data Warehouse*. Retrieved April 2025, from https://aws.amazon.com/redshift/
4. American Psychological Association. (2020). *Stress in America™ 2020: A National Mental Health Crisis*. American Psychological Association. https://www.apa.org/news/press/releases/stress/2020/report
5. Anderson, R. M., & May, R. M. (1991). *Infectious diseases of humans: Dynamics and control*. Oxford University Press.
6. Apache Software Foundation. (n.d.). *Welcome to Apache Hadoop!*. Retrieved April 2025, from https://hadoop.apache.org/
7. ArcSight. (2023). ArcSight Enterprise Security Manager. https://www.microfocus.com/en-us/cyberres/secops/arcsight
8. Avast. (2023). Avast Antivirus. Офіційний сайт Avast. https://www.avast.com/
9. Bakshy, E., Hofman, J. M., Mason, W. A., & Watts, D. J. (2011). Everyone's an influencer: Quantifying influence on Twitter. *Proceedings of the Fourth ACM International Conference on Web Search and Data Mining*, 65–74. https://doi.org/10.1145/1935826.1935845
10. Barabási, A. L., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*(5439), 509–512. https://doi.org/10.1126/science.286.5439.509

11. Borge-Holthoefer, J., & Moreno, Y. (2012). Absence of influential spreaders in rumor dynamics. *Physical Review E,* 85(2), 026116. https://doi.org/10.1103/PhysRevE.85.026116

12. Borge-Holthoefer, J., Baños, R. A., González-Bailón, S., & Moreno, Y. (2013). Cascading behavior in complex socio-technical networks. *Journal of Complex Networks*, 1(1), 3–24. https://doi.org/10.1093/comnet/cnt006

13. Brandwatch. (n.d.). *Social media listening & analytics platform*. Отримано з: https://www.brandwatch.com/

14. Brzhevska, Z., Dovzhenko, N., Kyrychok, R., Gaidur, G., & Anosov, A. (2019). I*нформаційні війни: проблеми, загрози та протидія. Кібербезпека: освіта, наука, техніка*, 3(3), 88–96. https://doi.org/10.28925/2663-4023.2019.3.8896

15. Brzhevska, Z., Kyrychok, R., Platonenko, A., & Hulak, H. (2022). *Оцінка передумов формування методики оцінки достовірності інформації. Кібербезпека: освіта, наука, техніка*, 3(15), 164–174. https://doi.org/10.28925/2663-4023.2022.15.164174

16. Budak, C., Agrawal, D., & El Abbadi, A. (2011). Limiting the spread of misinformation in social networks. *Proceedings of the 20th International Conference on World Wide Web (WWW '11)*, 665–674. https://doi.org/10.1145/1963405.1963499.

17. Buhas, V., Ponomarenko, I., Buhas, N., & Hulak, H. (2024). *Using machine learning techniques to increase the effectiveness of cybersecurity*. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems*, DECaT2024, CEUR Workshop Proceedings, 3665, 97–105.

18. Castellano, C., Fortunato, S., & Loreto, V. (2009). Statistical physics of social dynamics. *Reviews of Modern Physics, 81*(2), 591–646. https://doi.org/10.1103/RevModPhys.81.591

19. Centola, D. (2010). The spread of behavior in an online social network experiment. *Science, 329*(5996), 1194–1197. https://doi.org/10.1126/science.1185231

20. CERT-UA. (2024). Центр реагування на комп’ютерні надзвичайні події України. Отримано з: https://cert.gov.ua

21. Check Point. (2023). Check Point Next Generation Firewalls. https://www.checkpoint.com/

22. Check Point. (2023). Infinity Architecture. https://www.checkpoint.com/infinity-architecture/

23. Chiba, H., Medvedev, G. S., & Mizuhara, M. (2020). Bifurcations in the Kuramoto model on graphs. *Nonlinearity*, *33*(9), 4345–4371. https://doi.org/10.1088/1361-6544/ab92db

24. Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). *The echo chamber effect on social media*. Proceedings of the National Academy of Sciences, 118(9), e2023301118. https://doi.org/10.1073/pnas.2023301118

25. Cinelli, M., Brugnoli, E., Schmidt, A. L., Zollo, F., Quattrociocchi, W., & Scala, A. (2020). Selective exposure shapes the Facebook news diet. *Proceedings of the National Academy of Sciences*, 117(44), 27770–27776. https://doi.org/10.1073/pnas.2003604117

26. CIRCL. (2023). *MISP Threat Intelligence Sharing Platform*. Retrieved from https://www.misp-project.org

27. Cisco. (2023). Cisco Stealthwatch. https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

28. Cisco. (2023). Cisco Secure Firewall. https://www.cisco.com/c/en/us/products/security/secure-firewall/index.html

29. Cisco. (2023). Cisco ASA Series Firewalls. https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html

30. Cisco. (2023). Cisco SecureX Security Platform. https://www.cisco.com/c/en/us/products/security/securex/index.html

31. Crimson Hexagon. (n.d.). *Consumer insights platform*. Отримано з: https://www.crimsonhexagon.com/

32. CrowdStrike. (2023). Falcon Platform. https://www.crowdstrike.com/

33. Cylance. (2023). CylancePROTECT by BlackBerry. https://www.blackberry.com/us/en/products/cylanceprotect

34. Daley, D. J., & Kendall, D. G. (1965). Stochastic rumours. *Journal of the Institute of Mathematics and Its Applications*, 1(1), 42–55. https://doi.org/10.1093/imamat/1.1.42

35. Darktrace. (2023). Darktrace Cyber AI. https://darktrace.com/

36. DeepState. (2022). *Оперативна інформація про події в Україні*. Telegram-канал. https://t.me/DeepStateUA

37. Domingos, P., & Richardson, M. (2001). Mining the network value of customers. *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining*, 57–66. https://doi.org/10.1145/502512.502525

38. Dreis, Y., Ivanichenko, Y., Nesterova, O., Zhdanova, Y., & Dmytriienko, K. (2022). Restricted Information Identification Model. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2022)*, CEUR Workshop Proceedings, Vol-3187, 89–95. http://ceur-ws.org/Vol-3187/

39. Easley, D., & Kleinberg, J. (2010). *Networks, Crowds, and Markets: Reasoning About a Highly Connected World*. Cambridge University Press.

40. Elastic. (n.d.). *Elasticsearch: The distributed search & analytics engine*. Retrieved April 2025, from https://www.elastic.co/elasticsearch

41. Erdos, P., & Rényi, A. (1959). On random graphs I. *Publicationes Mathematicae, 6*, 290–297.

42. ESET. (2023). ESET NOD32 Antivirus. Офіційний сайт ESET. https://www.eset.com/int/home/antivirus/

43. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM, 59*(7), 96–104. https://doi.org/10.1145/2818717

44. Fortinet. (2023). FortiGate Next-Generation Firewall. https://www.fortinet.com/products/next-generation-firewall

45. Freeman, L. C. (1977). A set of measures of centrality based on betweenness. *Sociometry*, 40(1), 35–41. https://doi.org/10.2307/3033543

46. Freeman, L. C. (1979). Centrality in social networks conceptual clarification. *Social Networks*, 1(3), 215–239. https://doi.org/10.1016/0378-8733(78)90021-7

47. Friedkin, N. E., & Johnsen, E. C. (1999). Social influence networks and opinion change. *Advances in Group Processes*, *16*, 1–29.

48. Friedkin, N. E. (1998). *A Structural Theory of Social Influence.* Cambridge University Press. https://doi.org/10.1017/CBO9780511527524

49. GDELT Project. (2024). Global Database of Events, Language, and Tone. Отримано з: https://www.gdeltproject.org/

50. Gephi. (2024). An open-source network analysis and visualization software package. Отримано з: https://gephi.org/

51. Gleeson, J. P., & Cahalane, D. J. (2007). Seed size strongly affects cascades on random networks. *Physical Review E*, *75*(5), 056103. https://doi.org/10.1103/PhysRevE.75.056103

52. Gómez, S., Arenas, A., Borge-Holthoefer, J., Meloni, S., & Moreno, Y. (2010). Discrete-time Markov chain approach to contact-based disease spreading in complex networks. *EPL (Europhysics Letters)*, 89(3), 38009. https://doi.org/10.1209/0295-5075/89/38009

53. Google Cloud. (n.d.). *BigQuery: Serverless, highly scalable, and cost-effective multi-cloud data warehouse*. Retrieved April 2025, from https://cloud.google.com/bigquery

54. Granovetter, M. (1978). Threshold models of collective behavior. *American Journal of Sociology, 83*(6), 1420–1443. https://doi.org/10.1086/226707

55. Hinduja, S., & Patchin, J. W. (2014). *Cyberbullying: Identification, Prevention, and Response*. Cyberbullying Research Center.

56. Holme, P., & Saramäki, J. (2012). Temporal networks. *Physics Reports, 519*(3), 97–125. https://doi.org/10.1016/j.physrep.2012.03.001

57. IBM. (2023). IBM Watson for Cyber Security. https://www.ibm.com/security/artificial-intelligence

58. IBM. (2023). IBM QRadar SIEM. https://www.ibm.com/products/qradar-siem

59. International Organization for Standardization. (2013). ISO/IEC 27005:2013 – Information technology – Security techniques – Information security risk management. Geneva: ISO.

60. Ising, E. (1925). Beitrag zur Theorie des Ferromagnetismus. *Zeitschrift für Physik*, 31(1), 253–258. https://doi.org/10.1007/BF02980577

61. Ivanichenko, Y., Kozachok, V., Dreis, Y., Nesterova, O., & Dmytriienko, K. (2022). Exposing deviations in information processes using multifractal analysis. *CEUR Workshop Proceedings*, Vol-3187, 251–259.

62. Kaplan, A. M., & Haenlein, M. (2010). *Users of the world, unite! The challenges and opportunities of social media*. Business Horizons, 53(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

63. Katz, L. (1953). A new status index derived from sociometric analysis. *Psychometrika*, 18(1), 39–43. https://doi.org/10.1007/BF02289026

64. Kempe, D., Kleinberg, J., & Tardos, É. (2003). Maximizing the spread of influence through a social network. *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 137–146. https://doi.org/10.1145/956750.956769

65. Kiss, I. Z., Miller, J. C., & Simon, P. L. (2017). *Mathematics of epidemics on networks: From exact to approximate models*. Cham: Springer. https://doi.org/10.1007/978-3-319-50806-1

66. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). *Cybersecurity risk analysis and management for critical infrastructures using probabilistic models.* In Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CEUR Workshop Proceedings, 3654, 432–439

67. 66. Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks.

Proceedings of the National Academy of Sciences, 111(24), 8788–8790. https://doi.org/10.1073/pnas.1320040111

68. Kyiv Independent. (2022). *Reporting on the Russian invasion of Ukraine*. https://kyivindependent.com/

69. Latane, B. (1981). The psychology of social impact. *American Psychologist*, 36(4), 343–356. https://doi.org/10.1037/0003-066X.36.4.343

70. Lazer, D., Baum, M. A., Grinberg, N., Friedland, L., Joseph, K., Hobbs, W. R., & Mattsson, C. (2018). The science of fake news. *Science*, 359(6380), 1094–1096. https://doi.org/10.1126/science.aao2998

71. LogRhythm. (2023). LogRhythm SIEM Platform. https://logrhythm.com/

72. Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. *Data & Society Research Institute.* https://datasociety.net/library/media-manipulation-and-disinformation-online/

73. Medvedev, G. S., Chiba, H., & Mizuhara, M. S. (2021). Bifurcations in the Kuramoto model on graphs. *Journal of Nonlinear Science*, 31(5), 69. https://doi.org/10.1007/s00332-021-09733-z

74. Micro Focus. (2023). *ArcSight SIEM: Cybersecurity Threat Detection & Response*. Retrieved from https://www.microfocus.com/en-us/cyberres/secops/arcsight

75. Microsoft. (2023). Microsoft Defender for Endpoint. https://www.microsoft.com/en-us/security/business/threat-protection/microsoft-defender-endpoint

76. Mitnick, K. D., & Simon, W. L. (2011). *The Art of Deception: Controlling the Human Element of Security* (Rev. ed.). Wiley.

77. Moreno, Y., Pastor-Satorras, R., & Vespignani, A. (2004). Epidemic outbreaks in complex heterogeneous networks. *The European Physical Journal B, 26*(4), 521–529. https://doi.org/10.1140/epjb/e20020122

78. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev.

5). Gaithersburg, MD: U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

79. Neo4j. (2024). The World's Leading Graph Database. Отримано з: https://neo4j.com

80. NetworkX. (2024). Python library for studying graphs and networks. Отримано з: https://networkx.github.io/

81. Newman, M. E. J. (2002). Spread of epidemic disease on networks. *Physical Review E, 66*(1), 016128. https://doi.org/10.1103/PhysRevE.66.016128

82. Newman, M. E. J. (2010). *Networks: An Introduction*. Oxford University Press.

83. Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review*, 45(2), 167–256. https://doi.org/10.1137/S003614450342480

84. Nguyen, G., Yan, G., Thai, M. T., & Eidenbenz, S. (2012). Containment of misinformation spread in online social networks. *Proceedings of the 4th Annual ACM Web Science Conference*, 213–222. https://doi.org/10.1145/2380718.2380747

85. Nguyen T., Nguyen G., Nguyen H. Misinformation Detection and Prevention on Social Media: A Survey // Computers & Security. — 2021. — Vol. 106. — 102309. DOI: 10.1016/j.cose.2021.102309.

86. Nowak, A., & Lewenstein, M. (1996). Modeling social change with cellular automata. In R. Hegselmann, U. Mueller, & K. G. Troitzsch (Eds.), *Modelling and Simulation in the Social Sciences from a Philosophy of Science Point of View* (pp. 249–285). Springer.

87. OpenSSL Project. (2023). OpenSSL: Cryptography and SSL/TLS Toolkit. https://www.openssl.org/

88. Palo Alto Networks. (2023). Security Operating Platform. https://www.paloaltonetworks.com/

89. Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physical Review Letters, 86*(14), 3200–3203. https://doi.org/10.1103/PhysRevLett.86.3200

90. Pavlik, J. V. (2021). *Fake news and the future of journalism*. Journalism & Mass Communication Educator, 76(1), 12–18. https://doi.org/10.1177/1077695820959778

91. Pennycook, G., & Rand, D. G. (2019). *Fighting misinformation on social media using crowdsourced judgments of news source quality*. Proceedings of the National Academy of Sciences, 116(7), 2521–2526. https://doi.org/10.1073/pnas.1806781116

92. Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

93. Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

94. Scarfone, K., & Mell, P. (2021). *Guide to Security Information and Event Management (SIEM) Implementation*. NIST Special Publication 800-92. https://doi.org/10.6028/NIST.SP.800-92

95. SemanticForce. (n.d.). *AI-powered media intelligence & analytics platform*. Отримано з: https://www.semanticforce.net/

96. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). *Information security risk management using cognitive modeling*. In Cybersecurity Providing in Information and Telecommunication Systems II, CEUR Workshop Proceedings, 3050, 297–305.

97. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Spasiteleva, S. (2021). *Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці*. Кібербезпека: освіта, наука, техніка, 1(13), 133–144. https://doi.org/10.28925/2663-4023.2021.13.133144

98. Shu K., Sliva A., Wang S., Tang J., Liu H. Fake News Detection on Social Media: A Data Mining Perspective // ACM SIGKDD Explorations Newsletter. — 2017. — Vol. 19, No. 1. — P. 22–36. DOI: 10.1145/3137597.3137600.

99. Smirnov, V., Moskalenko, O., Yatsenko, R., Kravchenko, D., & Osetskyi, O. (2023*). Improving cyber defense through synchronization of autonomous agents*

in critical infrastructure systems. CEUR Workshop Proceedings, 3654, 293–302. https://www.scopus.com/record/display.uri?eid=2-s2.0-85189138396

100. Sophos. (2023). Sophos Endpoint Protection. https://www.sophos.com/en-us/products/endpoint-antivirus.aspx

101. Splunk. (2023). Splunk Security Information and Event Management (SIEM). https://www.splunk.com/

102. Stallings, W. (2020). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley Professional.

103. Starbird, K. (2017). *Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on Twitter*. Proceedings of the International AAAI Conference on Web and Social Media, 11(1), 230–239. https://ojs.aaai.org/index.php/ICWSM/article/view/14878

104. Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.

105. Talkwalker. (n.d.). *Social listening and analytics platform*. Отримано з: https://www.talkwalker.com/

106. Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018). *Defining "Fake News"*. Digital Journalism, 6(2), 137–153. https://doi.org/10.1080/21670811.2017.1360143

107. Tandoc Jr, E. C., & Maitra, J. (2018). *News organizations' use of Twitter during crises: A study of tweets during Typhoon Haiyan in the Philippines*. Journalism, 19(7), 1008–1025. https://doi.org/10.1177/1464884916648095

108. TensorFlow. (2024). An end-to-end open-source machine learning platform. Отримано з: https://www.tensorflow.org/

109. Thomas, D. R., & Loader, B. D. (2017). *Cybercrime: Law and Regulation*. Routledge.

110. ThreatConnect, Inc. (2023). *Threat Intelligence Platform Overview*. Retrieved from https://threatconnect.com

111. Ukrainian Pravda. (2022). *Оперативні новини України та світу*. https://www.pravda.com.ua/

112. USAID & Internews. (2024). *Результати дослідження медіаграмотності в Україні*. Інфографіка. Отримано з: https://internews.in.ua/research/2024-disinformation-awareness

113. VeraCrypt. (2023). VeraCrypt – Free Open-source Disk Encryption Software. https://www.veracrypt.fr/en/Home.html

114. Vosoughi, S., Roy, D., & Aral, S. (2018). *The spread of true and false news online*. Science, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

115. Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

116. Watts, D. J. (2002). A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences, 99*(9), 5766–5771. https://doi.org/10.1073/pnas.082090499

117. YouScan. (n.d.). *AI-powered social media listening platform*. Отримано з: https://youscan.io/

118. Zaharia, M., Chowdhury, M., Das, T., Dave, A., Ma, J., McCauley, M., ... & Stoica, I. (2012). *Resilient distributed datasets: A fault-tolerant abstraction for in-memory cluster computing*. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI) (pp. 15–28). USENIX Association. https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final138.pdf

119. Zeek. (2023). Zeek Network Security Monitor. https://zeek.org/

120. Zollo, F., & Quattrociocchi, W. (2018). *Misinformation spreading on Facebook*. In *Complex Spreading Phenomena in Social Systems* (pp. 177–196). Springer. https://doi.org/10.1007/978-3-319-77332-2_10

121. Андрушко, П. П. (2019). Інформаційна безпека: основи теорії та практики. Київ: Центр учбової літератури.

122. Бидюк, П. І. (2014). Класифікація загроз інформаційній безпеці: проблеми та підходи. Збірник наукових праць Харківського університету Повітряних Сил, (1), 25–30.

123. Верховна Рада України. (2022). Закон України "Про медіа". Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/2712-20

124. Верховна Рада України. (2018). Закон України "Про національну безпеку України". Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/2469-19

125. Верховна Рада України. (2021). Закон України "Про основи національного спротиву". Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/1702-20

126. Володін, О. М., & Кравчук, Т. В. (2023). *Математичні моделі для виявлення та протидії фейковим новинам у соціальних мережах*. Інформаційні технології і системи, 27(3), 45–55. https://doi.org/10.32404/its.2023.03.045

127. Гуцалюк, М. І. (2021). Проблеми забезпечення національної безпеки України в умовах гібридних загроз. Вісник Національного університету оборони України, (1), 78–83.

128. Дмитрієнко, К. А. (2023). Адаптація моделі Курамото для аналізу розповсюдження інформації в соціальних мережах. Кібербезпека: освіта, наука, техніка, 1(21), 309–314. https://doi.org/10.28925/2663-4023.2023.20.272282

129. Дмитрієнко, К. А. (2023). Порівняльний аналіз моделей розповсюдження інформації в інтернет-середовищі. *Кібербезпека: освіта, наука, техніка, 4*(20), 272–282. https://doi.org/10.28925/2663-4023.2023.21.309314

130. Дмитрієнко, К. А. (2024). Вдосконалення моделі курамото для моделювання поширення інформації в соціальних мережах. *Телекомунікаційні та інформаційні технології, 4*(85), 16–28. https://doi.org/10.31673/2412-4338.2024.048612

131. Дмитрієнко, К., & Коршун, Н. (2025). Застосування вдосконалених моделей Курамото для ідентифікації дезінформації у соціальних мережах. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 406–416. https://doi.org/10.28925/2663-4023.2025.27.754

132. Долгіх, С. О. (2020). Інформаційні війни як загроза національній безпеці України. *Військово-науковий вісник*, (34), 45–52.

133. Дьяків, О. М., & Кисіль, М. М. (2021). Загрози інформаційній безпеці та засоби їх подолання. Наукові записки Українського науково-дослідного інституту зв'язку, (3), 45–50.

134. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII. (2023). Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/3855-12#Text

135. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР. (2023). Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

136. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. (2023). Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/2657-12#Text

137. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. (2017). Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/2163-19#Text

138. Коссей, А., Ліпшиц, В. (2018). Впливові користувачі у соціальних мережах: виявлення та аналіз. *Наукові записки Інституту журналістики*, 68(1), 96–103.

139. Міністерство культури та інформаційної політики України. (2020). Проєкт Закону України "Про дезінформацію". https://mkip.gov.ua/news/4076.html

140. Наливайко, Л. Р. (2020). Інформаційна безпека держави: концептуальні основи та механізми реалізації. *Київ: Інститут держави і права ім. В. М. Корецького НАН України*.

141. Притула, К. М. (2022). Кіберзагрози критичній інфраструктурі: аналіз українського досвіду. *Науковий вісник Ужгородського національного університету. Серія: Право*, (69), 123–127.

142. Рада національної безпеки і оборони України. (2016). Концепція інформаційної безпеки України. https://www.rnbo.gov.ua/files/2016/Konczepcziya.pdf

143. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). *Загрози та ризики використання штучного інтелекту.* Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

144. Слюсар, В. І. (2020). Кіберзагрози в інформаційному просторі України. *Інформаційне суспільство*, (28), 58–63.

145. Шевченко, Л. П. (2021). Фейкові новини як загроза інформаційній безпеці держави. *Інформаційне суспільство*, (28), 60–66.

146. Шевченко , С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). *Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки.* Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178. https://doi.org/10.28925/2663-4023.2023.22.168178

ДОДАТОК А.
Програмний код для графічної візуалізації порівняння базової моделі Курамото та її вдосконаленої версії, створеної із застосуванням каскадної моделі та порівняння за показником синхронізації

```
import numpy as np
import matplotlib.pyplot as plt
import networkx as nx

# Параметри моделі
N = 20  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Часові кроки
dt = 0.1  # Крок інтегрування

# Генерація Scale-Free мережі
np.random.seed(42)
G = nx.scale_free_graph(N, seed=42).to_undirected()
A = nx.adjacency_matrix(G).toarray()
np.fill_diagonal(A, 0)  # Вузол не зв'язаний із собою

# Кількість зв'язків для кожного вузла
d = np.sum(A, axis=1)

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)
theta_enhanced = theta.copy()

# Природні частоти вузлів
omega = np.random.normal(1.0, 0.1, N)

# Збереження фаз для обох моделей
theta_history_basic = [theta.copy()]
theta_history_enhanced = [theta_enhanced.copy()]

# Збереження середніх значень фаз
mean_phase_basic = []
mean_phase_enhanced = []

# Симуляція
for t in range(T):
    # Базова модель Курамото
    dtheta = omega + K / N * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1)
    theta += dtheta * dt
    theta_history_basic.append(theta.copy())
    mean_phase_basic.append(np.mean(theta))  # Середня фаза для
базової моделі
```

```
    # Покращена модель Курамото
    dtheta_enhanced = omega + (K / d) * np.sum(A *
np.sin(np.outer(theta_enhanced, np.ones(N)) -
np.outer(np.ones(N), theta_enhanced)), axis=1)
    theta_enhanced += dtheta_enhanced * dt
    theta_history_enhanced.append(theta_enhanced.copy())
    mean_phase_enhanced.append(np.mean(theta_enhanced))  #
Середня фаза для покращеної моделі

# Конвертуємо історію у масиви
theta_history_basic = np.array(theta_history_basic)
theta_history_enhanced = np.array(theta_history_enhanced)
mean_phase_basic = np.array(mean_phase_basic)
mean_phase_enhanced = np.array(mean_phase_enhanced)

# Розрахунок коефіцієнта порядку r
def order_parameter(theta):
    return np.abs(np.mean(np.exp(1j * theta)))

r_basic = [order_parameter(theta) for theta in
theta_history_basic]
r_enhanced = [order_parameter(theta) for theta in
theta_history_enhanced]

# Побудова графіків
plt.figure(figsize=(14, 10))

# Графік фаз
plt.subplot(2, 1, 1)
for i in range(N):
    plt.plot(range(T + 1), theta_history_basic[:, i],
color="blue", alpha=0.5, linewidth=1, label="Basic Kuramoto
Model" if i == 0 else "")
    plt.plot(range(T + 1), theta_history_enhanced[:, i],
color="red", alpha=0.5, linewidth=1, label="Enhanced Kuramoto
Model" if i == 0 else "")
plt.title("Evolution: Basic vs Enhanced Kuramoto Model (Scale-
Free Network)", fontsize=14, fontweight='normal', family='Times
New Roman')
plt.xlabel("Time Steps", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.ylabel("Phase", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.legend(loc="upper left", fontsize=10, frameon=False)  #
Легенда на графіку

# Графік коефіцієнта порядку r
plt.subplot(2, 1, 2)
plt.plot(range(T + 1), r_basic, label="Basic Kuramoto Model",
color="blue", linewidth=1)
```

```
plt.plot(range(T + 1), r_enhanced, label="Enhanced Kuramoto
Model", color="red", linewidth=1)
plt.title("Synchronization Order Parameter (r)", fontsize=14,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.ylabel("Order Parameter", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.legend(loc="upper right", fontsize=10, frameon=False)  #
Легенда на правій стороні

plt.tight_layout()
plt.show()
```

ДОДАТОК Б.
Код програми вдосконаленої моделі Курамото за допомогою каскадної моделі з використанням реальних даних

```
import numpy as np
import matplotlib.pyplot as plt
import pandas as pd
from collections import defaultdict

# Дані (20 об'єктів)
data = {
    "Impressions": [3920, 5394, 4021, 4528, 2518, 3884, 2621, 3541,
3749, 4115, 3234, 4344, 3216, 9453, 5055, 4002, 3169, 6168, 2407,
2064],
    "From_Home": [2586, 2727, 2085, 2700, 1704, 2046, 1543, 2071,
2384, 2609, 2414, 2168, 2524, 2525, 2017, 3401, 1979, 2177, 1338,
1304],
    "From_Hashtags": [1028, 1838, 1188, 621, 255, 1214, 599, 628, 857,
1104, 476, 1274, 212, 5799, 2351, 278, 707, 3450, 655, 362],
    "From_Explore": [619, 1174, 0, 932, 279, 329, 333, 500, 248, 178,
185, 673, 201, 208, 298, 128, 341, 153, 276, 249],
    "From_Other": [56, 78, 533, 73, 37, 43, 25, 60, 49, 46, 75, 40,
223, 794, 108, 73, 32, 296, 39, 37],
    "Saves": [98, 194, 41, 172, 96, 74, 22, 135, 155, 122, 122, 119,
121, 100, 101, 111, 106, 82, 40, 49],
    "Comments": [9, 7, 11, 10, 5, 7, 5, 4, 6, 6, 8, 7, 5, 6, 7, 17, 8,
6, 8, 4],
    "Shares": [5, 14, 1, 7, 4, 10, 1, 9, 8, 3, 14, 11, 5, 10, 11, 18,
1, 6, 20, 5],
    "Likes": [162, 224, 131, 213, 123, 144, 76, 124, 159, 191, 151,
162, 142, 294, 159, 205, 121, 151, 72, 76],
    "Profile_Visits": [35, 48, 62, 23, 8, 9, 26, 12, 36, 31, 15, 8,
20, 181, 17, 16, 21, 77, 10, 9],
    "Follows": [2, 10, 12, 8, 0, 2, 0, 6, 4, 6, 0, 2, 4, 42, 6, 2, 2,
30, 0, 0],
    "Hashtags": [
        "#finance #money #business #investing",
        "#healthcare #health #covid",
        "#data #datascience #dataanalysis",
        "#python #pythonprogramming",
        "#datavisualization #datascience",
        "#datascience #machinelearning",
        "#stockmarket #investing",
        "#python #pythonprogramming",
        "#dataanalytics #datascience",
        "#python #pythonprogramming",
        "#python #datascience #machinelearning",
        "#data #datascience",
        "#stockmarket #candlestick",
        "#datascience #nlp",
        "#timeseries #statistics",
        "#career #job",
        "#timeseries #iot",
        "#datascience #stress",
        "#data #zomato",
        "#boxplots"
```

```
    ],
    "Post_Time": ["2024-12-22 10:00:00"] * 20  # Час публікації
однаковий для всіх записів
}

# Перетворення даних у DataFrame
data = pd.DataFrame(data)

# Налаштування параметрів моделі
N = len(data)  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Кількість часових кроків
dt = 0.1  # Крок інтегрування

# Матриця зв'язків A (на основі Shares і Follows)
A = np.zeros((N, N))
for i in range(N):
    for j in range(N):
        if i != j:
            A[i, j] = data["Shares"][j] + data["Follows"][j]

# Кількість зв'язків для кожного вузла
d = np.sum(A, axis=1) + 1e-5  # Уникаємо ділення на нуль

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)

# Природні частоти (нормалізовані Likes)
omega = data["Likes"] / data["Impressions"]

# Історія фаз
theta_history = [theta.copy()]

# Симуляція покращеної моделі Курамото
for t in range(T):
    dtheta = omega + (K / d) * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1)
    theta += dtheta * dt
    theta_history.append(theta.copy())

# Конвертуємо історію у масив
theta_history = np.array(theta_history)

# Аналіз хештегів
categories = {"#finance": "Finance", "#health": "Health",
"#datascience": "Data Analytics", "#job": "Job", "#python": "Python"}
group_colors = {"Finance": "blue", "Health": "green", "Data
Analytics": "orange", "Job": "red", "Python": "purple", "Other":
"gray"}
node_colors = []

for i, hashtags in enumerate(data["Hashtags"]):
    for tag, category in categories.items():
        if tag in hashtags:
            node_colors.append(group_colors[category])
            break
    else:
```

```
        node_colors.append("gray")  # Default color for unknown
categories

# Побудова графіків
plt.figure(figsize=(12, 8))

# Графік фаз
for i in range(N):
    plt.plot(range(T + 1), theta_history[:, i], alpha=0.7,
linewidth=1.5, label="Node {}".format(i + 1) if i < 10 else "",
color=node_colors[i])

# Легенда
handles = [plt.Line2D([0], [0], color=color, lw=4, label=category) for
category, color in group_colors.items()]
plt.legend(handles=handles, bbox_to_anchor=(0.85, 1), loc='upper
left', fontsize=10, title="Hashtag Categories", frameon=False)

plt.title("Enhanced Kuramoto Model with Cascade Dynamics",
fontsize=14)
plt.xlabel("Time Steps", fontsize=12)
plt.ylabel("Phase", fontsize=12)
plt.grid(True)
plt.tight_layout()
plt.show()
```

ДОДАТОК В.

Набір реальних даних для моделювання та аналізу поширення інформації

Impressions	From Home	From Hashtags	From Explore	From Other	Saves	Comments	Shares	Likes	Profile Visits	Follows	Hashtags
3920	2586	1028	619	56	98	9	5	162	35	2	#finance #money #business #investing #investment #trading #stock market #data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #dataanalyst #amankharwal #thecleverprogrammer
5394	2727	1838	1174	78	194	7	14	224	48	10	#healthcare #health #covid #data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #dataanalyst #amankharwal #thecleverprogrammer
4021	2085	1188	0	533	41	11	1	131	62	12	#data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #deeplearning #machinelearningprojects #datascienceprojects #amankharwal #thecleverprogrammer #machinelearningmodels
4528	2700	621	932	73	172	10	7	213	23	8	#python #pythonprogramming #pythonprojects #pythoncode #pythonlearning #pythondeveloper #pythoncoding #pythonprogrammer #amankharwal #thecleverprogrammer #pythonprojects
2518	1704	255	279	37	96	5	4	123	8	0	#datavisualization #datascience #data #dataanalytics #machinelearning #dataanalysis #artificialintelligence #python #datascientist #bigdata #deeplearning #dataviz #ai #analytics #technology #dataanalyst #programming #pythonprogramming #statistics #coding #businessintelligence #datamining #tech #business #computerscience #tableau #database #thecleverprogrammer #amankharwal
3884	2046	1214	329	43	74	7	10	144	9	2	#data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #deeplearning #algorithm #algorithms #machinelearningalgorithms #ml #amankharwal #thecleverprogrammer #softskills

Impressions	From Home	From Hashtags	From Explore	From Other	Saves	Comments	Shares	Likes	Profile Visits	Follows	Hashtags
2621	1543	599	333	25	22	5	1	76	26	0	#stockmarket #investing #stocks #trading #money #investment #finance #forex #datavisualization #datascience #data #dataanalytics #machinelearning #dataanalysis #ai #candlestick #candlestickcharts
3541	2071	628	500	60	135	4	9	124	12	6	#python #pythonprogramming #pythonprojects #pythoncode #pythonlearning #pythondeveloper #pythoncoding #pythonprogrammer #amankharwal #thecleverprogrammer #pythonprojects #pythonbooks #bookstagram
3749	2384	857	248	49	155	6	8	159	36	4	#dataanalytics #datascience #data #machinelearning #datavisualization #bigdata #artificialintelligence #datascientist #python #analytics #ai #dataanalysis #deeplearning #technology #programming #coding #dataanalyst #business #pythonprogramming #datamining #tech #businessintelligence #database #computerscience #statistics #powerbi #dataanalysisprojects #businessanalytics #thecleverprogrammer #amankharwal
4115	2609	1104	178	46	122	6	3	191	31	6	#python #pythonprogramming #pythonprojects #pythoncode #pythonlearning #pythondeveloper #pythoncoding #pythonprogrammer #amankharwal #thecleverprogrammer #pythonprojects
2218	1597	411	162	15	28	6	3	81	29	4	#neuralnetwork #machinelearning #artificialintelligence #deeplearning #python #ai #datascience #neuralnetworks #programming #tensorflow #datascientist #pythonprogramming #tech #technology #artificialintelligenceai #machinelearningalgorithms #computerscience #coding #ml #data #amankharwal #thecleverprogrammer #alexnet
3234	2414	476	185	75	122	8	14	151	15	0	#python #pythonprogramming #pythonprojects #pythoncode #pythonlearning #pythondeveloper #pythoncoding #pythonprogrammer #amankharwal #thecleverprogrammer #pythonprojects
4344	2168	1274	673	40	119	7	11	162	8	2	#data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #deeplearning #algorithm #algorithms #machinelearningalgorithms #ml #amankharwal #thecleverprogrammer
3216	2524	212	201	223	121	5	5	142	20	4	#stockmarket #investing #stocks #trading #money #investment #finance #forex #datavisualization #datascience #data #dataanalytics #machinelearning #dataanalysis #ai #candlestick #candlestickcharts #amankharwal #thecleverprogrammer

Impressions	From Home	From Hashtags	From Explore	From Other	Saves	Comments	Shares	Likes	Profile Visits	Follows	Hashtags
9453	2525	5799	208	794	100	6	10	294	181	42	#data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #deeplearning #sentimentanalysis #sentiment #nlp #naturallanguageprocessing #amankharwal #thecleverprogrammer
5055	2017	2351	298	108	101	7	11	159	17	6	#timeseries #time #statistics #datascience #bigdata #machinelearning #python #ai #timeseriesanalysis #datavisualization #dataanalytics #data #iot #analysis #timeseriesmalaysia #artificialintelligence #analytics #amankharwal #thecleverprogrammer
4002	3401	278	128	73	111	17	18	205	16	2	#career #job #jobs #jobsearch #education #business #success #caregoals #motivation #work #careerdevelopment #careers #goals #resume #students #careeradvice #datascience #marketing #digitalmarketing #media #socialmedia #IT #webdevelopment #amankharwal #thecleverprogrammer
3169	1979	707	341	32	106	8	1	121	21	2	#timeseries #time #statistics #datascience #bigdata #machinelearning #python #ai #timeseriesanalysis #datavisualization #dataanalytics #data #iot #analysis #timeseriesmalaysia #artificialintelligence #analytics #amankharwal #thecleverprogrammer
6168	2177	3450	153	296	82	6	6	151	77	30	#data #datascience #dataanalysis #dataanalytics #datascientist #machinelearning #python #pythonprogramming #pythonprojects #pythoncode #artificialintelligence #ai #deeplearning #machinelearningprojects #datascienceprojects #amankharwal #thecleverprogrammer #machinelearningmodels #stress #stressdetection

https://www.kaggle.com/code/bhanupratapbiswas/instagram-reach-analysis/notebook

ДОДАТОК Г.
Програмний код для графічної візуалізації порівняння базової моделі Курамото та її удосконаленої версії, створеної із застосуванням епідемічної моделі та порівняння за показником синхронізації

```
import numpy as np
import matplotlib.pyplot as plt
import networkx as nx

# Параметри моделі
N = 20  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
γ = 0.5  # Коефіцієнт впливу інформації
T = 50  # Часові кроки
dt = 0.1  # Крок інтегрування

# Генерація Barabási-Albert мережі
np.random.seed(42)
G = nx.barabasi_albert_graph(N, 2)
A = nx.to_numpy_array(G)

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)
theta_enhanced = theta.copy()

# Природні частоти вузлів
omega = np.random.normal(1.0, 0.1, N)

# Збереження фаз для обох моделей
theta_history_basic = [theta.copy()]
theta_history_enhanced = [theta_enhanced.copy()]

# Ініціалізація інформаційних показників для покращеної моделі
I = np.random.uniform(0.1, 0.9, N)  # Поточний рівень інформації
R = np.random.uniform(0, 0.3, N)  # Рівень "забуття" інформації

# Симуляція
for t in range(T):
    # Базова модель Курамото
    dtheta = omega + (K / N) * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1)
    theta += dtheta * dt
    theta_history_basic.append(theta.copy())

    # Покращена модель Курамото
    dtheta_enhanced = omega + (K / N) * np.sum(A *
np.sin(np.outer(theta_enhanced, np.ones(N)) - np.outer(np.ones(N),
theta_enhanced)), axis=1) \
                      + γ * (I - R)
    theta_enhanced += dtheta_enhanced * dt
    theta_history_enhanced.append(theta_enhanced.copy())

# Конвертуємо історію у масиви
```

```
theta_history_basic = np.array(theta_history_basic)
theta_history_enhanced = np.array(theta_history_enhanced)

# Розрахунок коефіцієнта порядку r
def order_parameter(theta):
    return np.abs(np.mean(np.exp(1j * theta)))

r_basic = [order_parameter(theta) for theta in theta_history_basic]
r_enhanced = [order_parameter(theta) for theta in
theta_history_enhanced]

# Побудова графіків
plt.figure(figsize=(14, 10))

# Графік фаз
plt.subplot(2, 1, 1)
for i in range(N):
    plt.plot(range(T + 1), theta_history_basic[:, i], color="blue",
alpha=0.5, linewidth=1, label="Basic Kuramoto Model" if i == 0 else
"")
    plt.plot(range(T + 1), theta_history_enhanced[:, i], color="red",
alpha=0.5, linewidth=1, label="Enhanced Kuramoto Model" if i == 0 else
"")
plt.title("Basic vs Enhanced Kuramoto Model", fontsize=14,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.ylabel("Phase", fontsize=12, fontweight='normal', family='Times
New Roman')
plt.legend(loc="upper left", fontsize=10, frameon=False)  # Легенда на
графіку

# Графік коефіцієнта порядку r
plt.subplot(2, 1, 2)
plt.plot(range(T + 1), r_basic, label="Basic Kuramoto Model",
color="blue", linewidth=1)
plt.plot(range(T + 1), r_enhanced, label="Enhanced Kuramoto Model",
color="red", linewidth=1)
plt.title("Synchronization Order Parameter (r)", fontsize=14,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.ylabel("Order Parameter", fontsize=12, fontweight='normal',
family='Times New Roman')
plt.legend(loc="upper right", fontsize=10, frameon=False)  # Легенда
на правій стороні

plt.tight_layout()
plt.show()
```

ДОДАТОК Д.
Код прогами удосконаленої моделі Курамото за допомогою епідемічної моделі з використанням реальних даних

```
import numpy as np
import matplotlib.pyplot as plt
import pandas as pd
from collections import defaultdict

# Дані (20 об'єктів)
data = {
    "Impressions": [3920, 5394, 4021, 4528, 2518, 3884, 2621, 3541,
3749, 4115, 3234, 4344, 3216, 9453, 5055, 4002, 3169, 6168, 2407,
2064],
    "From_Home": [2586, 2727, 2085, 2700, 1704, 2046, 1543, 2071,
2384, 2609, 2414, 2168, 2524, 2525, 2017, 3401, 1979, 2177, 1338,
1304],
    "From_Hashtags": [1028, 1838, 1188, 621, 255, 1214, 599, 628, 857,
1104, 476, 1274, 212, 5799, 2351, 278, 707, 3450, 655, 362],
    "From_Explore": [619, 1174, 0, 932, 279, 329, 333, 500, 248, 178,
185, 673, 201, 208, 298, 128, 341, 153, 276, 249],
    "From_Other": [56, 78, 533, 73, 37, 43, 25, 60, 49, 46, 75, 40,
223, 794, 108, 73, 32, 296, 39, 37],
    "Saves": [98, 194, 41, 172, 96, 74, 22, 135, 155, 122, 122, 119,
121, 100, 101, 111, 106, 82, 40, 49],
    "Comments": [9, 7, 11, 10, 5, 7, 5, 4, 6, 6, 8, 7, 5, 6, 7, 17, 8,
6, 8, 4],
    "Shares": [5, 14, 1, 7, 4, 10, 1, 9, 8, 3, 14, 11, 5, 10, 11, 18,
1, 6, 20, 5],
    "Likes": [162, 224, 131, 213, 123, 144, 76, 124, 159, 191, 151,
162, 142, 294, 159, 205, 121, 151, 72, 76],
    "Profile_Visits": [35, 48, 62, 23, 8, 9, 26, 12, 36, 31, 15, 8,
20, 181, 17, 16, 21, 77, 10, 9],
    "Follows": [2, 10, 12, 8, 0, 2, 0, 6, 4, 6, 0, 2, 4, 42, 6, 2, 2,
30, 0, 0],
    "Hashtags": [
        "#finance #money #business #investing",
        "#healthcare #health #covid",
        "#data #datascience #dataanalysis",
        "#python #pythonprogramming",
        "#datavisualization #datascience",
        "#datascience #machinelearning",
        "#stockmarket #investing",
        "#python #pythonprogramming",
        "#dataanalytics #datascience",
        "#python #pythonprogramming",
        "#python #datascience #machinelearning",
        "#data #datascience",
        "#stockmarket #candlestick",
        "#datascience #nlp",
        "#timeseries #statistics",
        "#career #job",
        "#timeseries #iot",
        "#datascience #stress",
        "#data #zomato",
        "#boxplots"
```

```
    ],
    "Post_Time": ["2024-12-22 10:00:00"] * 20  # Час публікації
однаковий для всіх записів
}

# Перетворення даних у DataFrame
data = pd.DataFrame(data)

# Налаштування параметрів моделі
N = len(data)  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Кількість часових кроків
dt = 0.1  # Крок інтегрування

# Матриця зв'язків A (на основі Shares і Follows)
A = np.zeros((N, N))
for i in range(N):
    for j in range(N):
        if i != j:
            A[i, j] = data["Shares"][j] + data["Follows"][j]

# Кількість зв'язків для кожного вузла
d = np.sum(A, axis=1) + 1e-5  # Уникаємо ділення на нуль

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)

# Природні частоти (нормалізовані Likes)
omega = data["Likes"] / data["Impressions"]

# Нормалізовані значення для Saves та Likes
I = data["Likes"] / data["Likes"].max()
R = data["Saves"] / data["Saves"].max()

# Історія фаз
theta_history = [theta.copy()]

# Симуляція покращеної моделі Курамото
for t in range(T):
    dtheta = omega + (K / d) * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1) + (I - R)
    theta += dtheta * dt
    theta_history.append(theta.copy())

# Конвертуємо історію у масив
theta_history = np.array(theta_history)

# Аналіз хештегів
categories = {"#finance": "Finance", "#health": "Health",
"#datascience": "Data Analytics", "#job": "Job", "#python": "Python"}
group_colors = {"Finance": "blue", "Health": "green", "Data
Analytics": "orange", "Job": "red", "Python": "purple", "Other":
"gray"}
node_colors = []

for i, hashtags in enumerate(data["Hashtags"]):
    for tag, category in categories.items():
        if tag in hashtags:
```

```
            node_colors.append(group_colors[category])
            break
    else:
        node_colors.append("gray")  # Default color for unknown
categories

# Побудова графіків
plt.figure(figsize=(12, 8))

# Графік фаз
for i in range(N):
    plt.plot(range(T + 1), theta_history[:, i], alpha=0.7,
linewidth=1.5, label="Node {}".format(i + 1) if i < 10 else "",
color=node_colors[i])

# Легенда
handles = [plt.Line2D([0], [0], color=color, lw=4, label=category) for
category, color in group_colors.items()]
plt.legend(handles=handles, bbox_to_anchor=(0.65, 1), loc='upper
left', fontsize=10, title="Hashtag Categories", frameon=False)

plt.title("Enhanced Kuramoto Model with SIR Model", fontsize=14)
plt.xlabel("Time Steps", fontsize=12)
plt.ylabel("Phase", fontsize=12)
plt.grid(True)
plt.tight_layout()
plt.show()
```

ДОДАТОК Е.
Програмний код для графічної візуалізації порівняння базової моделі Курамото та її адаптованої версії, створеної із застосуванням моделі поширення чуток та порівняння за показником синхронізації

```
import numpy as np
import matplotlib.pyplot as plt
import networkx as nx

# Параметри моделі
N = 20  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Часові кроки
dt = 0.1  # Крок інтегрування

# Генерація Barabási-Albert мережі
np.random.seed(42)
G = nx.barabasi_albert_graph(N, 2)
A = nx.to_numpy_array(G)

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)
theta_enhanced = theta.copy()

# Природні частоти вузлів
omega = np.random.normal(1.0, 0.1, N)

# Збереження фаз для обох моделей
theta_history_basic = [theta.copy()]
theta_history_enhanced = [theta_enhanced.copy()]

# Збереження середніх значень фаз
mean_phase_basic = []
mean_phase_enhanced = []

# Симуляція
for t in range(T):
    # Базова модель Курамото
    dtheta = omega + K / N * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1)
    theta += dtheta * dt
    theta_history_basic.append(theta.copy())
    mean_phase_basic.append(np.mean(theta))  # Середня фаза для
базової моделі

    # Покращена модель Курамото з додатковим терміном
    dtheta_enhanced = omega + (K / N) * np.sum(A *
np.sin(np.outer(theta_enhanced, np.ones(N)) - np.outer(np.ones(N),
theta_enhanced)), axis=1) + (theta_enhanced - np.mean(theta_enhanced))
    theta_enhanced += dtheta_enhanced * dt
    theta_history_enhanced.append(theta_enhanced.copy())
    mean_phase_enhanced.append(np.mean(theta_enhanced))  # Середня
фаза для покращеної моделі

# Конвертуємо історію у масиви
theta_history_basic = np.array(theta_history_basic)
```

```
theta_history_enhanced = np.array(theta_history_enhanced)
mean_phase_basic = np.array(mean_phase_basic)
mean_phase_enhanced = np.array(mean_phase_enhanced)

# Розрахунок коефіцієнта порядку r
def order_parameter(theta):
    return np.abs(np.mean(np.exp(1j * theta)))

r_basic = [order_parameter(theta) for theta in theta_history_basic]
r_enhanced = [order_parameter(theta) for theta in
theta_history_enhanced]

# Побудова графіків
plt.figure(figsize=(12, 6))  # Збільшено розмір графіка

# Графік фаз
plt.subplot(2, 1, 1)
for i in range(N):
    plt.plot(range(T + 1), theta_history_basic[:, i], color="blue",
alpha=0.5, linewidth=1, label="Basic Kuramoto Model" if i == 0 else
"")
    plt.plot(range(T + 1), theta_history_enhanced[:, i], color="red",
alpha=0.5, linewidth=1, label="Enhanced Kuramoto Model" if i == 0 else
"")
plt.title("Basic vs Enhanced Kuramoto Model", fontsize=12,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=10, fontweight='normal',
family='Times New Roman')
plt.ylabel("Phase", fontsize=10, fontweight='normal', family='Times
New Roman')
plt.legend(loc="upper left", fontsize=10, frameon=False)  # Легенда на
графіку

# Графік коефіцієнта порядку r
plt.subplot(2, 1, 2)
plt.plot(range(T + 1), r_basic, label="Basic Kuramoto Model",
color="blue", linewidth=1)
plt.plot(range(T + 1), r_enhanced, label="Enhanced Kuramoto Model",
color="red", linewidth=1)
plt.title("Synchronization Order Parameter (r)", fontsize=10,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=10, fontweight='normal',
family='Times New Roman')
plt.ylabel("Order Parameter", fontsize=10, fontweight='normal',
family='Times New Roman')
plt.legend(loc="upper right", fontsize=10, frameon=False)  # Легенда
на правій стороні

plt.tight_layout()
plt.show()
```

ДОДАТОК Є.

Код прогами адаптованої моделі Курамото за допомогою моделі поширення чуток з використанням реальних даних

```
import numpy as np
import matplotlib.pyplot as plt
import pandas as pd
from collections import defaultdict

# Дані (розширені до 20 об'єктів)
data = {
    "Impressions": [3920, 5394, 4021, 4528, 2518, 3884, 2621, 3541,
3749, 4115, 3234, 4344, 3216, 9453, 5055, 4002, 3169, 6168, 2407,
2064],
    "From_Home": [2586, 2727, 2085, 2700, 1704, 2046, 1543, 2071,
2384, 2609, 2414, 2168, 2524, 2525, 2017, 3401, 1979, 2177, 1338,
1304],
    "From_Hashtags": [1028, 1838, 1188, 621, 255, 1214, 599, 628, 857,
1104, 476, 1274, 212, 5799, 2351, 278, 707, 3450, 655, 362],
    "From_Explore": [619, 1174, 0, 932, 279, 329, 333, 500, 248, 178,
185, 673, 201, 208, 298, 128, 341, 153, 276, 249],
    "From_Other": [56, 78, 533, 73, 37, 43, 25, 60, 49, 46, 75, 40,
223, 794, 108, 73, 32, 296, 39, 37],
    "Saves": [98, 194, 41, 172, 96, 74, 22, 135, 155, 122, 122, 119,
121, 100, 101, 111, 106, 82, 40, 49],
    "Comments": [9, 7, 11, 10, 5, 7, 5, 4, 6, 6, 8, 7, 5, 6, 7, 17, 8,
6, 8, 4],
    "Shares": [5, 14, 1, 7, 4, 10, 1, 9, 8, 3, 14, 11, 5, 10, 11, 18,
1, 6, 20, 5],
    "Likes": [162, 224, 131, 213, 123, 144, 76, 124, 159, 191, 151,
162, 142, 294, 159, 205, 121, 151, 72, 76],
    "Profile_Visits": [35, 48, 62, 23, 8, 9, 26, 12, 36, 31, 15, 8,
20, 181, 17, 16, 21, 77, 10, 9],
    "Follows": [2, 10, 12, 8, 0, 2, 0, 6, 4, 6, 0, 2, 4, 42, 6, 2, 2,
30, 0, 0],
    "Hashtags": [
        "#finance #money #business #investing",
        "#healthcare #health #covid",
        "#data #datascience #dataanalysis",
        "#python #pythonprogramming",
        "#datavisualization #datascience",
        "#datascience #machinelearning",
        "#stockmarket #investing",
        "#python #pythonprogramming",
        "#dataanalytics #datascience",
        "#python #pythonprogramming",
        "#python #datascience #machinelearning",
        "#data #datascience",
        "#stockmarket #candlestick",
        "#datascience #nlp",
        "#timeseries #statistics",
        "#career #job",
        "#timeseries #iot",
        "#datascience #stress",
        "#data #zomato",
        "#boxplots"
    ],
```

```
    "Post_Time": ["2024-12-22 10:00:00"] * 20  # Час публікації
однаковий для всіх записів
}

# Перетворення даних у DataFrame
data = pd.DataFrame(data)

# Налаштування параметрів моделі
N = len(data)  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Кількість часових кроків
dt = 0.1  # Крок інтегрування

# Матриця зв'язків A (на основі Shares і Follows)
A = np.zeros((N, N))
for i in range(N):
    for j in range(N):
        if i != j:
            A[i, j] = data["Shares"][j] + data["Follows"][j]

# Кількість зв'язків для кожного вузла
d = np.sum(A, axis=1) + 1e-5  # Уникаємо ділення на нуль

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)

# Природні частоти (нормалізовані Likes)
omega = data["Likes"] / data["Impressions"]

# Нормалізовані значення для Saves та Likes
I = data["Likes"] / data["Likes"].max()
R = data["Saves"] / data["Saves"].max()

# Історія фаз
theta_history = [theta.copy()]

# Симуляція покращеної моделі Курамото
for t in range(T):
    dtheta = omega + (K / d) * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1) + (I - R)
    theta += dtheta * dt
    theta_history.append(theta.copy())

# Конвертуємо історію у масив
theta_history = np.array(theta_history)

# Аналіз хештегів
categories = {"#finance": "Finance", "#health": "Health",
"#datascience": "Data Analytics", "#job": "Job", "#python": "Python"}
group_colors = {"Finance": "blue", "Health": "green", "Data
Analytics": "orange", "Job": "red", "Python": "purple", "Other":
"gray"}
node_colors = []

for i, hashtags in enumerate(data["Hashtags"]):
    for tag, category in categories.items():
        if tag in hashtags:
            node_colors.append(group_colors[category])
```

```
            break
    else:
        node_colors.append("gray")  # Default color for unknown
categories

# Побудова графіків
plt.figure(figsize=(12, 8))

# Графік фаз
for i in range(N):
    plt.plot(range(T + 1), theta_history[:, i], alpha=0.7,
linewidth=1.5, label="Node {}".format(i + 1) if i < 10 else "",
color=node_colors[i])

# Легенда
handles = [plt.Line2D([0], [0], color=color, lw=4, label=category) for
category, color in group_colors.items()]
plt.legend(handles=handles, bbox_to_anchor=(0.85, 1), loc='upper
left', fontsize=10, title="Hashtag Categories", frameon=False)

plt.title("Enhanced Kuramoto Model with Rumor Spreading Model",
fontsize=14)
plt.xlabel("Time Steps", fontsize=12)
plt.ylabel("Phase", fontsize=12)
plt.grid(True)
plt.tight_layout()
plt.show()
```

ДОДАТОК Ж.

Програмний код для графічної візуалізації порівняння базової моделі Курамото та її розширеної версії, створеної із застосуванням моделі впливових користувачів та порівняння за показником синхронізації

```
import numpy as np
import matplotlib.pyplot as plt
import networkx as nx

# Параметри моделі
N = 20  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Часові кроки
dt = 0.1  # Крок інтегрування
delta = 0.5  # Параметр для покращеної моделі, що визначає вплив C_i

# Генерація Barabási-Albert мережі
np.random.seed(42)
G = nx.barabasi_albert_graph(N, 2)
A = nx.to_numpy_array(G)

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)
theta_enhanced = theta.copy()

# Природні частоти вузлів
omega = np.random.normal(1.0, 0.1, N)

# Збереження фаз для обох моделей
theta_history_basic = [theta.copy()]
theta_history_enhanced = [theta_enhanced.copy()]

# Збереження середніх значень фаз
mean_phase_basic = []
mean_phase_enhanced = []

# Симуляція
for t in range(T):
    # Базова модель Курамото
    dtheta = omega + K / N * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1)
    theta += dtheta * dt
    theta_history_basic.append(theta.copy())
    mean_phase_basic.append(np.mean(theta))  # Середня фаза для
базової моделі

    # Покращена модель Курамото з додатковим терміном
    C_i = np.random.uniform(0, 1, N)  # Може бути функція або
константа для кожного вузла
    dtheta_enhanced = omega + (K / N) * np.sum(A *
np.sin(np.outer(theta_enhanced, np.ones(N)) - np.outer(np.ones(N),
theta_enhanced)), axis=1) + delta * C_i
```

```
    theta_enhanced += dtheta_enhanced * dt
    theta_history_enhanced.append(theta_enhanced.copy())
    mean_phase_enhanced.append(np.mean(theta_enhanced))  # Середня
фаза для покращеної моделі

# Конвертуємо історію у масиви
theta_history_basic = np.array(theta_history_basic)
theta_history_enhanced = np.array(theta_history_enhanced)
mean_phase_basic = np.array(mean_phase_basic)
mean_phase_enhanced = np.array(mean_phase_enhanced)

# Розрахунок коефіцієнта порядку r
def order_parameter(theta):
    return np.abs(np.mean(np.exp(1j * theta)))
r_basic = [order_parameter(theta) for theta in theta_history_basic]
r_enhanced = [order_parameter(theta) for theta in
theta_history_enhanced]

# Побудова графіків
plt.figure(figsize=(14, 6))

# Графік фаз
plt.subplot(2, 1, 1)
for i in range(N):
    plt.plot(range(T + 1), theta_history_basic[:, i], color="blue",
alpha=0.5, linewidth=1, label="Basic Kuramoto Model" if i == 0 else
"")
    plt.plot(range(T + 1), theta_history_enhanced[:, i], color="red",
alpha=0.5, linewidth=1, label="Enhanced Kuramoto Model" if i == 0 else
"")
plt.title("Basic vs Enhanced Kuramoto Model", fontsize=12,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=10, fontweight='normal',
family='Times New Roman')
plt.ylabel("Phase", fontsize=10, fontweight='normal', family='Times
New Roman')
plt.legend(loc="upper left", fontsize=10, frameon=False)

# Графік коефіцієнта порядку r
plt.subplot(2, 1, 2)
plt.plot(range(T + 1), r_basic, label="Basic Kuramoto Model",
color="blue", linewidth=2)
plt.plot(range(T + 1), r_enhanced, label="Enhanced Kuramoto Model",
color="red", linewidth=2)
plt.title("Synchronization Order Parameter (r)", fontsize=12,
fontweight='normal', family='Times New Roman')
plt.xlabel("Time Steps", fontsize=10, fontweight='normal',
family='Times New Roman')
plt.ylabel("Order Parameter", fontsize=10, fontweight='normal',
family='Times New Roman')
plt.legend(loc="upper right", fontsize=10, frameon=False)
plt.tight_layout()
plt.show()
```

ДОДАТОК З.
Код програми розширеної моделі Курамото за допомогою моделі впливових користувачів з використанням реальних даних

```
import numpy as np
import matplotlib.pyplot as plt
import pandas as pd

# Дані (розширені до 20 об'єктів)
data = {
    "Impressions": [3920, 5394, 4021, 4528, 2518, 3884, 2621,
3541, 3749, 4115, 3234, 4344, 3216, 9453, 5055, 4002, 3169, 6168,
2407, 2064],
    "Shares": [5, 14, 1, 7, 4, 10, 1, 9, 8, 3, 14, 11, 5, 10, 11,
18, 1, 6, 20, 5],
    "Likes": [162, 224, 131, 213, 123, 144, 76, 124, 159, 191,
151, 162, 142, 294, 159, 205, 121, 151, 72, 76],
    "Follows": [2, 10, 12, 8, 0, 2, 0, 6, 4, 6, 0, 2, 4, 42, 6,
2, 2, 30, 0, 0],
    "Hashtags": [
        "#finance #money #business #investing",
        "#healthcare #health #covid",
        "#data #datascience #dataanalysis",
        "#python #pythonprogramming",
        "#datavisualization #datascience",
        "#datascience #machinelearning",
        "#stockmarket #investing",
        "#python #pythonprogramming",
        "#dataanalytics #datascience",
        "#python #pythonprogramming",
        "#python #datascience #machinelearning",
        "#data #datascience",
        "#stockmarket #candlestick",
        "#datascience #nlp",
        "#timeseries #statistics",
        "#career #job",
        "#timeseries #iot",
        "#datascience #stress",
        "#data #zomato",
        "#boxplots"
    ]
}

data = pd.DataFrame(data)

# Налаштування параметрів моделі
N = len(data)  # Кількість вузлів
K = 2  # Коефіцієнт зв'язку
T = 50  # Кількість часових кроків
dt = 0.1  # Крок інтегрування

delta = 0.5  # Вплив центральності користувача
```

```
# Матриця зв'язків A
A = np.zeros((N, N))
for i in range(N):
    for j in range(N):
        if i != j:
            A[i, j] = data["Shares"][j] + data["Follows"][j]

# Центральність вузлів (нормалізована)
C = np.sum(A, axis=1) / np.max(np.sum(A, axis=1))

# Початкові значення фаз
theta = np.random.uniform(0, 2 * np.pi, N)

# Природні частоти (нормалізовані Likes)
omega = data["Likes"] / data["Impressions"]

# Історія фаз
theta_history = [theta.copy()]

# Симуляція покращеної моделі Курамото
for t in range(T):
    dtheta = omega + (K / N) * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1) + delta * C
    theta += dtheta * dt
    theta_history.append(theta.copy())

# Конвертуємо історію у масив
theta_history = np.array(theta_history)

# Аналіз хештегів
categories = {"#finance": "Finance", "#health": "Health",
"#datascience": "Data Analytics", "#job": "Job", "#python":
"Python"}
group_colors = {"Finance": "blue", "Health": "green", "Data
Analytics": "orange", "Job": "red", "Python": "purple", "Other":
"gray"}
node_colors = []

for i, hashtags in enumerate(data["Hashtags"]):
    for tag, category in categories.items():
        if tag in hashtags:
            node_colors.append(group_colors[category])
            break
    else:
        node_colors.append("gray")  # Default color for unknown
categories

# Побудова графіків
plt.figure(figsize=(12, 8))

# Графік фаз
for i in range(N):
```

```
    plt.plot(range(T + 1), theta_history[:, i], alpha=0.7,
linewidth=1.5, label="Node {}".format(i + 1) if i < 10 else "",
color=node_colors[i])

# Легенда
handles = [plt.Line2D([0], [0], color=color, lw=4,
label=category) for category, color in group_colors.items()]
plt.legend(handles=handles, bbox_to_anchor=(0.85, 1), loc='upper
left', fontsize=10, title="Hashtag Categories", frameon=False)

plt.title("Enhanced Kuramoto Model with Influential Spreaders",
fontsize=14)
plt.xlabel("Time Steps", fontsize=12)
plt.ylabel("Phase", fontsize=12)
plt.grid(True)
plt.tight_layout()
plt.show()
```

ДОДАТОК И.
Код програми реалізації знаходження ключових вузлів для протидії дезінформації за допомогою моделі Курамото удосконаленої за допомогою епідемічної моделі

```
import numpy as np
import matplotlib.pyplot as plt
import networkx as nx

# Model parameters
N = 50  # Number of nodes
T = 100  # Number of time steps
dt = 0.1  # Integration step
K = 1  # Coupling coefficient
gamma = 0.5  # Influence of "infected" and "recovered" nodes

# Constructing a Scale-Free graph using Barabási–Albert model
G = nx.barabasi_albert_graph(N, 2)  # Each new node attaches to 2
existing nodes
A = np.array(nx.to_numpy_array(G))  # Convert graph to adjacency
matrix

# Initial states
theta = np.random.uniform(0, 2 * np.pi, N)  # Initial phases
omega = np.random.normal(0, 0.1, N)  # Natural frequencies

# Initial conditions for SIR
S = np.ones(N)  # Initially, all nodes are susceptible
I = np.zeros(N)  # No infected nodes initially
R = np.zeros(N)  # No recovered nodes initially
I[0] = 1  # Initial infected node

# SIR model parameters
beta = 0.3  # Infection probability
mu = 0.1  # Recovery rate

# Phase and state history
theta_history = [theta.copy()]
S_history, I_history, R_history = [S.copy()], [I.copy()], [R.copy()]

# Simulation
for t in range(T):
    # Update phases (Kuramoto model + SIR influence)
    dtheta = omega + (K / N) * np.sum(A * np.sin(np.outer(theta,
np.ones(N)) - np.outer(np.ones(N), theta)), axis=1)
    dtheta += gamma * (I - R)  # Additional SIR influence
    theta += dtheta * dt

    # Update SIR states
    new_infections = beta * S * (A @ I)  # Information spread
    recoveries = mu * I  # Recovery
```

```
        S -= new_infections * dt
        I += (new_infections - recoveries) * dt
        R += recoveries * dt

        # Record history
        theta_history.append(theta.copy())
        S_history.append(S.copy())
        I_history.append(I.copy())
        R_history.append(R.copy())

# Visualization of results
time = np.arange(0, T + 1) * dt
theta_history = np.array(theta_history)
S_history, I_history, R_history = np.array(S_history),
np.array(I_history), np.array(R_history)

plt.figure(figsize=(12, 6))

# Phase graph
plt.subplot(1, 2, 1)
for i in range(N):
    plt.plot(time, theta_history[:, i], alpha=0.7)
plt.title("Phases in the Kuramoto Model")
plt.xlabel("Time")
plt.ylabel("Phase")
plt.grid(True)

# SIR graph
plt.subplot(1, 2, 2)
plt.plot(time, S_history.sum(axis=1), label="Susceptible (S)")
plt.plot(time, I_history.sum(axis=1), label="Infected (I)")
plt.plot(time, R_history.sum(axis=1), label="Recovered (R)")
plt.title("SIR Model")
plt.xlabel("Time")
plt.ylabel("Number of Nodes")
plt.legend()
plt.grid(True)

plt.tight_layout()
plt.show()

# Function to calculate synchronization measure (R)
def calculate_synchronization(theta):
    return np.abs(np.mean(np.exp(1j * theta)))

# Function to identify top nodes by eigenvector centrality
def find_influential_nodes(G):
    centrality = nx.eigenvector_centrality(G)
    influential_nodes = sorted(centrality, key=centrality.get,
reverse=True)[:5]
    return influential_nodes

# Function to locate source of disinformation
```

```
def locate_source(G, theta_history, I_history, time_step):
    # Identify nodes with maximum influence at given time step
    theta = theta_history[time_step]
    infected_nodes = np.where(I_history[time_step] > 0)[0]

    # Synchronization measure
    R = calculate_synchronization(theta)
    print("Synchronization (R) at time step {}:
{:.4f}".format(time_step, R))

    # Find most influential nodes
    influential_nodes = find_influential_nodes(G)
    print("Top influential nodes: {}".format(influential_nodes))

    # Check infected nodes for potential sources
    potential_sources = list(set(influential_nodes) &
set(infected_nodes))
    print("Potential sources of disinformation:
{}".format(potential_sources))
    return potential_sources

# Visualization of potential sources
def visualize_sources(G, sources, infected_nodes):
    plt.figure(figsize=(8, 8))
    pos = nx.spring_layout(G)

    # Draw the network
    nx.draw_networkx_edges(G, pos, alpha=0.3)
    nx.draw_networkx_nodes(G, pos, node_color="lightblue",
node_size=200, alpha=0.8, label="Nodes")

    # Highlight infected nodes
    nx.draw_networkx_nodes(G, pos, nodelist=infected_nodes,
node_color="orange", node_size=300, label="Infected")

    # Highlight sources
    nx.draw_networkx_nodes(G, pos, nodelist=sources, node_color="red",
node_size=400, label="Sources")

    # Add labels
    nx.draw_networkx_labels(G, pos, font_size=10, font_color="black")

    plt.title("Network with Highlighted Sources and Infected Nodes")
    plt.legend(loc="upper right")
    plt.axis("off")
    plt.show()

# Example usage with simulation data
time_step_to_analyze = 10  # Adjust as needed
potential_sources = locate_source(G, theta_history, I_history,
time_step_to_analyze)
visualize_sources(G, potential_sources,
np.where(I_history[time_step_to_analyze] > 0)[0])
```

ДОДАТОК І.

Код програми реалізації знаходження ключових вузлів для аналізу впливових користувачів у соціальних мережах на основі вдосконаленої моделі Курамото за допомогою моделі впливових користувачів

```
import numpy as np
import networkx as nx
import matplotlib.pyplot as plt

# Model parameters
N = 50  # Number of nodes
K = 1.0  # Coupling coefficient
T = 100  # Number of simulation iterations
delta = 0.5  # Influence of centrality

# Create a Scale-Free (Barabási–Albert) graph
G = nx.barabasi_albert_graph(N, m=2)  # Each new node connects to 2
existing nodes
A = nx.to_numpy_array(G)  # Adjacency matrix

# Intrinsic frequencies (random)
omega = np.random.normal(0, 0.1, N)

# Initial phases (random)
theta = np.random.uniform(0, 2 * np.pi, N)

# Calculate node centrality (eigenvector centrality)
centrality = nx.degree_centrality(G)  # Using degree centrality
C = np.array([centrality[i] for i in range(N)])

# Iterative phase updates
for t in range(T):
    dtheta = omega + K * np.sum(A * np.sin(np.outer(theta, np.ones(N))
- np.outer(np.ones(N), theta)), axis=1)
    dtheta += delta * C  # Influence of centrality
    theta += dtheta * 0.1  # Integration step (dt=0.1)

# Identifying influential users
influential_users = np.argsort(-theta)[:5]  # Top-5 influential nodes

# Output results
print("Top-5 influential users:", influential_users)
print("Phases of the influential users:", theta[influential_users])

# Visualization of influential nodes
def visualize_influential_nodes(G, influential_nodes):
    pos = nx.spring_layout(G)
    plt.figure(figsize=(8, 8))

    # Draw graph
    nx.draw_networkx_edges(G, pos, alpha=0.3)
```

```
    nx.draw_networkx_nodes(G, pos, node_color="lightblue",
node_size=200, alpha=0.8, label="Nodes")

    # Highlight influential nodes
    nx.draw_networkx_nodes(G, pos, nodelist=influential_nodes,
node_color="red", node_size=400, label="Influential Nodes")

    # Add labels
    nx.draw_networkx_labels(G, pos, font_size=10, font_color="black")

    plt.title("Scale-Free Graph with Influential Nodes")
    plt.legend(loc="upper right")
    plt.axis("off")
    plt.show()

visualize_influential_nodes(G, influential_users)
```

ДОДАТОК Ї.

Акти та довідки впровадження результатів дисертаційного дослідження

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА МАТЕМАТИКИ
вул. Левка Лук'яненка, 13-Б, м. Київ, Україна, 04207
Тел.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

BORYS GRINCHENKO
KYIV METROPOLITAN UNIVERSITY

FACULTY
OF INFORMATION TECHNOLOGIES
AND MATHEMATICS
13-B, Levka Lukianenka St, Kyiv, Ukraine, 04207
Tel.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

14.02.2025 № 3/1

АКТ

про впровадження результатів дисертаційного дослідження
Дмитрієнко Катерини Анатоліївни
на тему «Моделі та методи ідентифікації ключових вузлів у соціальних мережах для забезпечення інформаційної безпеки держави»,
поданої на здобуття наукового ступеня доктора філософії
зі спеціальності 125 Кібербезпека

Цим Актом, грунтуючись на рішенні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, засвідчуємо, що нижчеперелічені наукові положення, а саме:

1. метод аналізу синхронізації інформаційних процесів у соціальних мережах на основі базової моделі Курамото з урахуванням індивідуальної сприйнятливості користувачів та сили зв'язків між ними;
2. поєднання моделі Курамото з каскадною моделлю поширення інформації, що забезпечує можливість моделювання лавиноподібного передавання інформації в мережах при досягненні порогових значень активності вузлів;
3. модель виявлення лідерів думок шляхом включення метрик центральності вузлів у модель Курамото;
4. метод ідентифікації ключових вузлів для знаходження дезінформації за рахунок інтеграції моделі Курамото та епідемічної моделі;
5. метод для визначення ключових вузлів що дозволяє виявити лідерів думок у соціальних мережах, заснований на вдосконаленій моделі Курамото з використанням методів аналізу впливових користувачів.

Розроблені особисто Дмитрієнко Катериною Анатоліївною у ході проведення нею дисертаційних досліджень та отримали високу оцінку при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка у робочих програмах навчальних дисциплін спеціальності 125 Кібербезпека за захист інформації першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового) рівнів вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення лабораторій безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації.

Дослідження Дмитрієнко Катерини Анатоліївни відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Декан
Факультету інформаційних технологій та математики
кандидат фізико-математичних наук,
старший науковий співробітник Оксана ЛИТВИН

ЗАТВЕРДЖУЮ
Директор Інституту програмних систем
Національної академії наук України
_____Ігор СІНІЦИН
06 січня 2025 року

АКТ
впровадження матеріалів дисертаційних досліджень
Дмитрієнко Катерини Анатоліївни
на тему:
«Моделі та методи ідентифікації ключових вузлів у соціальних мережах для забезпечення інформаційної безпеки держави»

Комісія у складі:
голова комісії – заступник директора з наукової роботи Шевченко В.Л.;
члени комісії:
учений секретар Дергильова О.В.
заступник завідувача відділу Ігнатенко П.П.

Встановила та цим актом засвідчує, що нижчеперелічені матеріали дисертаційних досліджень Дмитрієнко Катерини Анатоліївни, а саме:

- метод аналізу синхронізації інформаційних процесів у соціальних мережах на основі базової моделі Курамото з урахуванням індивідуальної сприйнятливості користувачів та сили зв'язків між ними;
- поєднання моделі Курамото з каскадною моделлю поширення інформації, що забезпечує можливість моделювання лавиноподібного передавання інформації в мережах при досягненні порогових значень активності вузлів;
- модель виявлення лідерів думок шляхом включення метрик центральності вузлів у модель Курамото;
- метод ідентифікації ключових вузлів для знаходження дезінформації за рахунок інтеграції моделі Курамото та епідемічної моделі;
- метод для визначення ключових вузлів що дозволяє виявити лідерів думок у соціальних мережах, заснований на вдосконаленій моделі Курамото з використанням методів аналізу впливових користувачів.

Впроваджені в Інституті програмних систем Національної академії наук України. Надані матеріали були використані при формуванні плану перспективних досліджень. Даний акт не є підставою для фінансових зобов'язань.

Голова комісії Віктор ШЕВЧЕНКО

Члени комісії Олена ДЕРГИЛЬОВА

Петро ІГНАТЕНКО

ЗАТВЕРДЖУЮ
Перший заступник начальника Національного центру управління та випробувань космічних засобів

_____ Андрій ЖИЛКОВ
12.05 2025 року

АКТ №37/А
впровадження результатів дисертаційних досліджень
Дмитрієнко Катерини Анатоліївни
на тему:
«Моделі та методи ідентифікації ключових вузлів у соціальних мережах для забезпечення інформаційної безпеки держави»

Комісія Національного центру управління та випробувань космічних засобів у складі: голова комісії - заступник начальника Національного центру (із розвитку, науково-дослідної та випробувальної роботи) к.т.н. Анатолій ПОІХАЛО, члени комісії: начальник центру інформаційних систем та захисту інформації Олександр СУХОДУБ, начальник відділу науково-дослідної та випробувальної роботи к.т.н., доцент Андрій КОЗУБ, заступник начальника центру інформаційно-аналітичного центру к.т.н. Віктор МАМАРЄВ, встановила та цим актом засвідчує, що нижчеперелічені результати дисертаційних досліджень Дмитрієнко Катерини Анатоліївни, а саме:

- метод аналізу синхронізації інформаційних процесів у соціальних мережах на основі базової моделі Курамото з урахуванням індивідуальної сприйнятливості користувачів та сили зв'язків між ними;
- метод ідентифікації ключових вузлів для знаходження дезінформації за рахунок інтеграції моделі Курамото та епідемічної моделі,

впроваджені в повсякденну діяльність центру інформаційних систем та захисту інформації НЦУВКЗ і використовуються для знаходження дезінформації під час створення інформаційних бюлетенів спостережень за космічною обстановкою, аналітичних документів з інформаційної безпеки НЦУВКЗ та інших звітних документів.

Голова комісії Анатолій ПОІХАЛО

Члени комісії Олександр СУХОДУБ

Андрій КОЗУБ

Віктор МАМАРЄВ