КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.754
УДК 004.6

Дмитрієнко Катерина Анатоліївна
аспірант кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-7984-7279
k.dmytriienko.asp@kubg.edu.ua

Коршун Наталія Володимирівна
д.т.н., професор, професор кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

ЗАСТОСУВАННЯ ВДОСКОНАЛЕНИХ МОДЕЛЕЙ КУРАМОТО ДЛЯ ІДЕНТИФІКАЦІЇ ДЕЗІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація. У статті досліджено проблему поширення дезінформації у соціальних мережах та запропоновано вдосконалені підходи до її ідентифікації на основі вдосконалених моделей Курамото. У сучасному світі соціальні мережі стали потужними засобами комунікації, що забезпечують швидкий обмін інформацією між мільйонами людей. Водночас ці мережі сприяють поширенню дезінформації — свідомо неправдивої або маніпулятивної інформації, яка використовується для впливу на громадську думку та досягнення політичних, соціальних чи економічних цілей. Зростання масштабів поширення дезінформації становить серйозну загрозу для інформаційної безпеки, суспільної стабільності та довіри до державних інституцій. Для вирішення цієї проблеми у статті запропоновано дві модифіковані моделі Курамото. Перша модель поєднується з епідемічною моделлю SIR, що дозволяє враховувати стан користувачів (інфікований, здоровий або відновлений) і моделювати процес поширення інформації. Друга модель використовує аналіз впливовості користувачів шляхом інтеграції коефіцієнта центральності вузлів, що дає змогу визначати ключових учасників, які мають найбільший вплив на інформаційні потоки в мережі. Запропоновані моделі мають низку переваг. Модель із SIR дозволяє оцінювати динаміку поширення контенту, локалізувати джерела дезінформації та прогнозувати сценарії її поширення. Модель із впливовими користувачами забезпечує ідентифікацію ключових вузлів мережі, які можуть бути як джерелами дезінформації, так і засобами її стримування через поширення перевіреної інформації. У роботі наголошено на важливості адаптивності запропонованих моделей до різних соціальних платформ і типів інформаційних потоків. Інтеграція фазової синхронізації та центральності вузлів дає змогу виявляти не лише популярних користувачів, але й тих, хто активно впливає на інформаційні процеси. Це створює можливість швидко реагувати на інформаційні загрози, знижуючи їхній вплив на суспільство.

Ключові слова: дезінформація; соціальна мережа; інформаційна система; інформаційний вплив; інформація; модель впливових користувачів; кібербезпека; ідентифікація; соціальна інженерія; інформаційна безпека.

ВСТУП

У сучасному світі соціальні мережі, такі як Facebook, Twitter (X), Instagram, TikTok та YouTube, стали потужними інструментами комунікації, забезпечуючи миттєвий обмін інформацією між мільйонами людей. Вони сприяють поширенню корисних знань, але водночас стають середовищем для масового розповсюдження дезінформації — свідомо

неправдивої або маніпулятивної інформації, що має на меті ввести аудиторію в оману. Дезінформація використовується для впливу на громадську думку та досягнення політичних, соціальних чи економічних цілей [1] – [3].

З кожним роком масштаби її поширення зростають, створюючи серйозні ризики для інформаційної безпеки держави, суспільної стабільності та довіри громадян до державних інституцій. Українське законодавство приділяє значну увагу проблемі дезінформації. У Законі України «Про медіа» цей термін визначено як свідомо поширену недостовірну інформацію, яка вводить громадськість в оману. Закон покладає на медіа відповідальність за перевірку достовірності контенту [4].

Окрім цього, у законах «Про національну безпеку України» [5] та «Про основи національного спротиву» [6] дезінформація згадується як елемент інформаційних загроз, спрямованих на дестабілізацію суспільно-політичної ситуації та підрив довіри до держави. Також у 2020 році було розроблено проєкт закону «Про дезінформацію», який передбачав чітке визначення цього терміну та встановлення механізмів боротьби з ним. У цьому проєкті дезінформація визначалася як свідомо недостовірна інформація, спрямована на введення аудиторії в оману. Проте законопроєкт не був ухвалений через дискусії щодо його впливу на свободу слова та можливі ризики зловживання.

Проблематика дезінформації в Україні визнана критичною, що підкреслює необхідність її подальшого вивчення та розробки ефективних методів протидії [7].

Постановка проблеми. Дезінформація є однією з головних загроз сучасного інформаційного простору через специфіку соціальних мереж і їхній вплив на масову аудиторію.

По-перше, швидкість поширення контенту в соціальних мережах створює умови для миттєвого охоплення мільйонів користувачів, незалежно від достовірності інформації. Алгоритми платформ сприяють популяризації емоційно зарядженого контенту, що ускладнює виявлення джерел фейків та оперативне реагування.

По-друге, анонімність користувачів і можливість створення фальшивих акаунтів полегшують організацію інформаційних атак. Зловмисники часто використовують бот-мережі для масового поширення маніпулятивного контенту, залишаючись безкарними.

По-третє, алгоритми рекомендацій у соціальних мережах підсилюють провокаційний контент, сприяючи створенню «інформаційних бульбашок». Це ізолює користувачів від альтернативних поглядів, підсилюючи упередження і поширення фейків [8].

Окрім цього, дезінформація є потужним інструментом гібридних воєн, зокрема в Україні. Вона використовується для дестабілізації суспільства, дискредитації державних інституцій і впливу на політичні процеси.

Низький рівень медіаграмотності також сприяє поширенню дезінформації. Багато користувачів не перевіряють достовірність джерел і довіряють інформації, яка відповідає їхнім упередженням, що робить суспільство вразливим до маніпуляцій.

Дезінформація в соціальних мережах підриває політичну, соціальну та економічну стабільність [9]. Для ефективної протидії необхідний комплексний підхід, що включає розвиток математичних моделей, таких як вдосконалені моделі Курамото, програми медіаграмотності та посилення регулювання інформаційного простору.

Аналіз останніх досліджень та публікацій. Ефективна протидія дезінформації вимагає впровадження сучасних методів її виявлення, підвищення медіаграмотності населення та використання математичних моделей для аналізу й управління інформаційними потоками. Це дозволяє не лише реагувати на інформаційні атаки, але й запобігати їхньому впливу, забезпечуючи стабільність інформаційного середовища. В

роботі [10] відзначається роль соціальних медіа як основного каналу комунікації з цільовою аудиторією в цифровому середовищі, проаналізовано основні методи аналізу настроїв аудиторії, серед яких — методи із застосуванням машинного та глибокого навчання. В [11] представлено інструментальну платформу для виявлення модифікацій deepfake біометричних зображень, яка інтегрує інформаційну нейромережеву технологію та технологію підтримки прийняття рішень та створює основу для розробки системного підходу до захищеного виявлення deepfake у рамках профілів безпеки критичної інфраструктури. В [12] досліджуються процеси ідентифікації потенційних загроз, їх аналіз, визначення можливих наслідків і розробка стратегій захисту для запобігання цим загрозам.

Вдосконалені моделі Курамото є ефективним інструментом для моделювання поширення інформації в соціальних мережах. Їх інтеграція з епідемічними моделями та аналізом впливових користувачів дозволяє оцінювати динаміку поширення контенту, локалізувати джерела дезінформації та прогнозувати сценарії її поширення.

Застосування цих моделей сприяє глибшому розумінню механізмів розповсюдження дезінформації, прогнозуванню ризиків та розробці стратегій інформаційної безпеки. Автоматизація процесів через впровадження програмних засобів підвищує ефективність боротьби з інформаційними загрозами та забезпечує надійний захист інформаційного простору [13].

Метою статті є демонстрація можливостей застосування вдосконалених моделей Курамото для виявлення дезінформації та ідентифікації ключових вузлів у соціальних мережах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Використання вдосконаленої моделі Курамото для протидії дезінформації

У сучасному інформаційному просторі розуміння динаміки поширення інформації є одним із ключових завдань для боротьби з дезінформацією, прогнозування вірусних трендів та оптимізації комунікаційних стратегій. Вдосконалена модель Курамото із застосуванням епідемічної моделі (SIR) дозволяє моделювати процес поширення інформації у мережі, враховуючи як динаміку взаємодії між користувачами, так і їхній поточний стан (інфікований, здоровий або відновлений).

Вдосконалена модель Курамото із застосуванням епідемічної моделі (SIR) є потужним і ефективним інструментом для аналізу поширення інформації в соціальних мережах. Її ефективність ґрунтується на поєднанні механізмів синхронізації між користувачами (модель Курамото) та класифікації їхніх станів (модель SIR), що дозволяє детально моделювати динаміку поширення дезінформації. Такий підхід дозволяє враховувати як взаємодію користувачів у мережі, так і їхню схильність до поширення або блокування інформації. Завдяки цьому створюється точна модель інформаційного середовища, що відображає реальні процеси поширення як правдивої, так і фейкової інформації.

Формула моделі:

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

Особливу роль у цій моделі відіграє здатність ідентифікувати ключові вузли, які найбільше впливають на поширення інформації. Аналіз змін фаз активності користувачів

і відстеження їхніх станів за SIR-моделлю дає можливість виявити впливових поширювачів контенту [13]. Це дозволяє оперативно реагувати на появу дезінформації, локалізувати її джерела та здійснювати цілеспрямовані заходи для обмеження її впливу. Такий підхід забезпечує проактивну боротьбу з інформаційними загрозами, дозволяючи запобігти масштабному розповсюдженню шкідливого контенту.

Крім того, інтеграція моделей Курамото і SIR дає змогу моделювати різні сценарії інформаційних атак, варіюючи параметри поширення та взаємодії між користувачами. Це дозволяє гнучко адаптувати модель до реальних умов і розробляти ефективні стратегії інформаційної безпеки. Наприклад, можна змоделювати, як блокування окремих акаунтів або поширення спростувань вплине на зниження поширення фейків, що допомагає обґрунтовано приймати рішення щодо захисту інформаційного простору.

Додатковою перевагою моделі є можливість виявлення критичних моментів у поширенні інформації — так званих фазових переходів, коли локальне поширення фейкової новини може стати глобальним. Це дозволяє оперативно вжити заходів для запобігання ескалації дезінформації. Завдяки цьому можна своєчасно блокувати або обмежувати поширення шкідливого контенту, мінімізуючи його вплив на суспільство.

Написання програмної реалізації моделі з використанням графічних візуалізацій може зробити процес аналізу прозорим і наочним. Наприклад на рис. 1 показано можливий варіант реалізації цього методу.

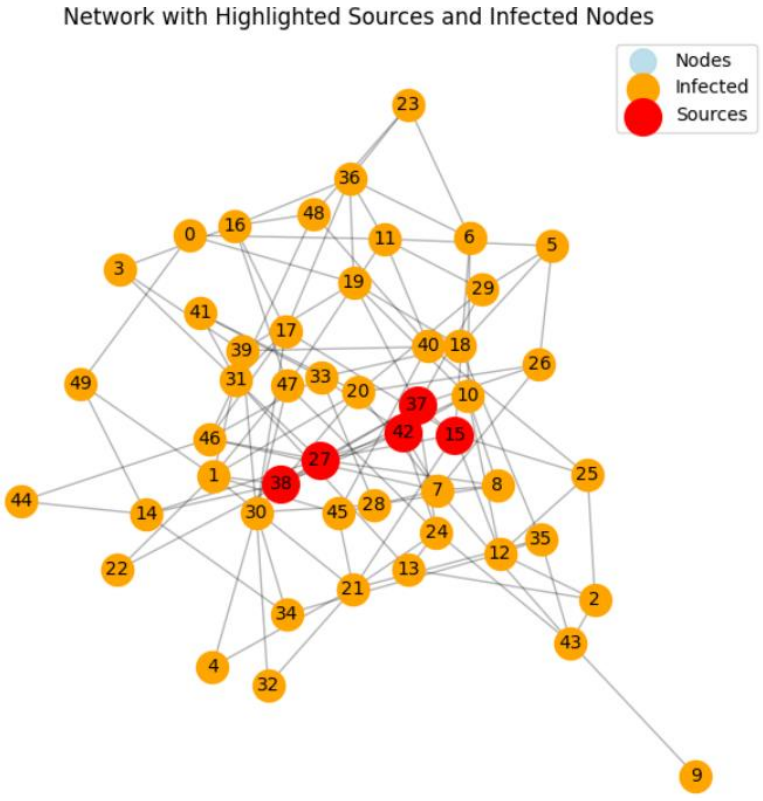

Рис. 1. Мережа з виділеними джерелами та зараженими вузлами

На рис. 1 представлено граф взаємодії між вузлами в мережі. Жовтими позначено інфіковані вузли, а червоним — можливі джерела дезінформації. Всі вузли в графі взаємодіють один з одним, створюючи складну мережу зв’язків. Завдяки такій візуалізації можна ефективно визначати джерела дезінформації в мережі, оскільки метод

дозволяє виділити як інфіковані вузли, так і ймовірні точки початку поширення неправдивої інформації. Також саме тому цей метод пошуку дезінформації є ефективним тому що:

1. Комплексний підхід

Ефективність розробленого методу забезпечується завдяки поєднанню аналізу синхронізації інформаційних потоків і оцінки центральності вузлів у соціальних мережах. Синхронізація дозволяє виявити аномальні сплески активності, що можуть свідчити про скоординовані кампанії з поширення дезінформації, наприклад, масові репости або одночасне публікування подібного контенту різними акаунтами. Оцінка вектора центральності допомагає ідентифікувати користувачів, які мають найбільший вплив на інформаційний потік. Це забезпечує високу точність виявлення джерел дезінформації, оскільки враховуються не лише окремі дії користувачів, а й їхнє місце у загальній мережевій структурі. Комплексний аналіз дозволяє точно визначати як ініціаторів фейків, так і ключових поширювачів.

2. Оперативність

Запропонований метод забезпечує швидке реагування на появу дезінформації завдяки безперервному аналізу динаміки поширення інформації. Використання вдосконаленої моделі Курамото дозволяє в реальному часі відстежувати аномальні сплески активності в інформаційних потоках, що можуть бути свідченням скоординованих атак або масових кампаній з дезінформації. Оперативне виявлення таких активностей дає змогу швидко локалізувати джерела фейків і вжити заходів для обмеження їхнього впливу. Це дозволяє значно зменшити шкоду від поширення шкідливого контенту, що є критично важливим у кризових ситуаціях або під час політичних подій.

3. Адаптивність

Метод є гнучким і може бути адаптований для різних соціальних мереж і типів інформаційних потоків. Це досягається завдяки використанню універсальних показників, таких як синхронізація та центральність вузлів, які залишаються ефективними незалежно від особливостей конкретної платформи. Метод може бути інтегрований у різні інформаційні системи моніторингу, що дозволяє налаштувати аналіз під конкретні цілі — від виявлення фейкових новин до боротьби з бот-мережами. Адаптивність методу робить його ефективним як для відкритих платформ (Facebook, Twitter, Instagram), так і для закритих або спеціалізованих мереж.

4. Прогнозування

Важливою перевагою є можливість не лише реагувати на вже існуючі загрози, але й прогнозувати потенційні інформаційні атаки. Завдяки ідентифікації впливових користувачів та аналізу динаміки інформаційних потоків, метод дозволяє передбачити, які теми або події можуть стати об’єктами дезінформаційних кампаній. Це забезпечує проактивний підхід до захисту інформаційного простору: завдяки ранньому виявленню потенційних загроз можна завчасно вжити заходів для їх нейтралізації. Визначення впливових вузлів також дозволяє використовувати їх для поширення достовірної інформації, що сприяє зменшенню ефективності фейкових кампаній.

Отже, поєднання математичної моделі Курамото, розширеної за рахунок аналізу центральності вузлів, із динамічним аналізом інформаційних потоків створює потужний інструмент для боротьби з дезінформацією. Метод дозволяє швидко виявляти джерела фейкових новин, прогнозувати загрози та гнучко адаптуватися до різних соціальних платформ, що робить його надзвичайно ефективним для забезпечення інформаційної безпеки.

Аналіз впливових користувачів у соціальних мережах на основі вдосконаленої моделі Курамото

У сучасних соціальних мережах інформаційний простір нерівномірно формується під впливом окремих користувачів, які володіють широкою аудиторією та високою довірою. Ці лідери думок активно впливають на суспільну думку, поширення ідей, трендів і навіть на політичні процеси. Вони здатні ініціювати ланцюгові реакції поширення інформації, що може як підтримувати позитивні ініціативи, так і сприяти поширенню дезінформації.

Особливо важливим є виявлення тих користувачів, які несвідомо чи навмисно поширюють фейкові новини або маніпулятивний контент. У сучасних умовах інформаційної війни дезінформація стала потужним інструментом впливу. Ідентифікація таких користувачів дозволяє не лише локалізувати джерела шкідливого контенту, але й спрямовувати їхній вплив на поширення достовірної інформації.

Аналіз впливових вузлів у мережах сприяє кращому розумінню структури інформаційних потоків. Це дозволяє передбачати ризики деструктивного впливу та оперативно реагувати на шкідливий контент. Завдяки ідентифікації можна блокувати акаунти або знижувати їхній вплив, мінімізуючи масштаби поширення дезінформації.

Впливові користувачі також можуть бути інструментом боротьби з фейками через поширення перевіреної інформації, що зміцнює довіру до достовірних джерел. Їхня участь сприяє підвищенню рівня медіаграмотності та зменшенню впливу фейкових новин [14] – [17].

Застосування сучасних математичних моделей, зокрема моделі Курамото, значно підвищує ефективність виявлення таких користувачів. Інтеграція вдосконаленої моделі Курамото із застосуванням моделі впливових користувачів дозволяє автоматизувати моніторинг мереж, прогнозувати ризики та сприяти створенню безпечного інформаційного середовища, де дезінформація мінімізована.

Таким чином, ідентифікація впливових користувачів є важливим інструментом у забезпеченні стійкості інформаційного простору. Завдяки їй зменшуються масштаби поширення шкідливого контенту, а цифрове середовище стає безпечнішим і прозорішим для користувачів.

Ефективність використання вдосконаленої моделі Курамото для виявлення впливових користувачів у соціальних мережах зумовлена її здатністю комплексно аналізувати як динамічні процеси поширення інформації, так і структуру самої мережі.

Інтеграція динаміки Курамото є ключовою перевагою цього методу. Поєднання фазових взаємодій між вузлами з урахуванням їхньої центральності дає змогу точніше визначити користувачів, які відіграють роль лідерів думок. Фазова синхронізація показує, як швидко користувачі підлаштовуються під інформаційні потоки. Якщо певні вузли швидко синхронізуються з іншими або, навпаки, задають загальний ритм поширення інформації, це свідчить про їхню значущість у мережі. Таким чином, модель дозволяє виявити не лише популярних користувачів, а саме тих, хто активно впливає на інформаційні процеси.

Формула моделі:

$$\theta_i = \omega_i + K\sum_{j=1}^{N} \mathrm{A_{ij}}\sin\left(\theta_j - \theta_i\right) + \delta * C_i \qquad (2)$$

Однією з ключових переваг цієї моделі є інтеграція впливовості вузлів у динаміку мережі. Використання коефіцієнта C_i, що враховує впливовість кожного вузла, дозволяє точно виділяти ключових користувачів, які мають найбільший вплив на поширення

інформації [13]. Це дає змогу ефективніше концентрувати зусилля на боротьбі з дезінформацією, спрямовуючи заходи на найбільш важливі вузли мережі.

1. Синхронізація інформаційних потоків.

Модель враховує не тільки взаємодії між вузлами, але й те, як впливові вузли синхронізують інформацію у своїй локальній мережі. Це дозволяє виявляти аномальні зміни у поведінці мережі, які можуть свідчити про масові кампанії або скоординовані дії зі сторони ботів або шкідливих акторів.

2. Виявлення критичних точок поширення інформації.

Вузли, які виконують роль «переломних точок», є ключовими для поширення інформації. Їхня нейтралізація може суттєво знизити масштаб дезінформаційних кампаній, що робить цей підхід надзвичайно ефективним у порівнянні з традиційними методами.

3. Адаптивність.

Модель також є надзвичайно гнучкою, оскільки її можна адаптувати до різних платформ і типів інформаційних потоків. Використання універсальних показників, таких як синхронізація та центральність вузлів, забезпечує її ефективність незалежно від особливостей конкретної соціальної мережі. Це дозволяє використовувати модель як для відкритих платформ (Facebook, Twitter), так і для спеціалізованих мереж. Наприклад реалізація програми (рис. 2.) на основі цієї моделі може виглядати так:

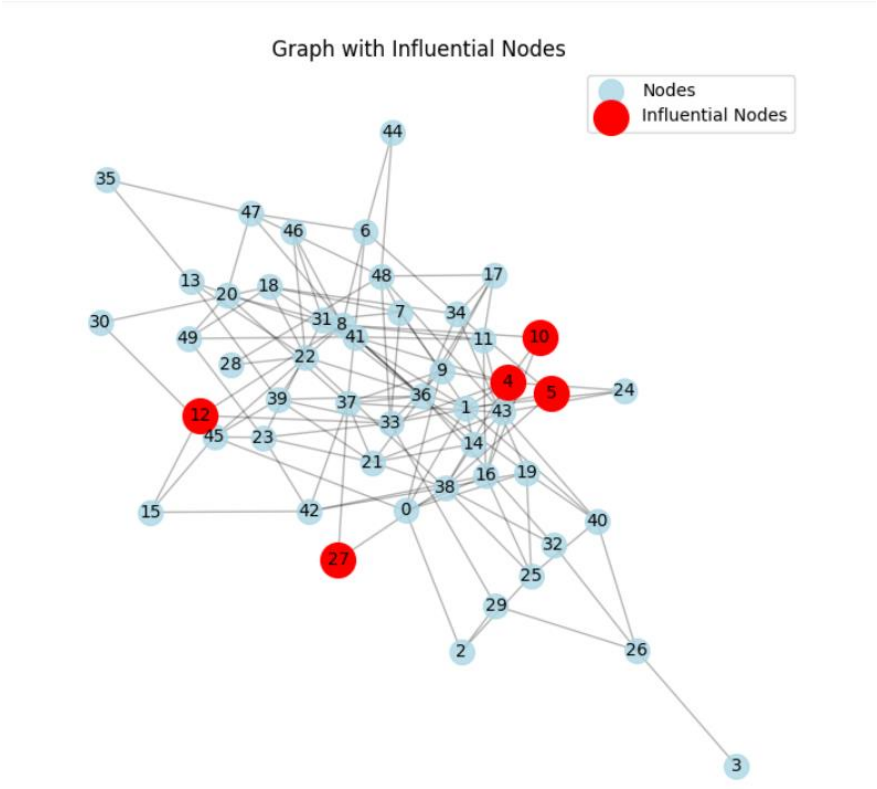

Рис. 2. Граф з впливовими вузлами

Цей рис. 2 містить граф мережі, де вузли позначають користувачів, а зв’язки між ними показують їх взаємодію. Червоні вузли виділяють впливових користувачів, які ідентифіковані за допомогою вдосконаленої моделі Курамото із врахуванням впливовості. Світло-блакитні вузли представляють інші користувачі, які мають менший вплив на поширення інформації.

4. Оперативність аналізу

Модель дозволяє відстежувати аномалії в реальному часі, що забезпечує швидке реагування на появу дезінформації. Це критично важливо у кризових ситуаціях, коли затримка у реагуванні може призвести до значної шкоди.

Завдяки комплексному підходу до визначення впливовості користувачів модель враховує не тільки прямий вплив вузлів на інших, але й їх місце у загальній мережевій структурі. Це забезпечує точну ідентифікацію як ініціаторів дезінформації, так і користувачів, які відіграють ключову роль у поширенні інформації.

5. Прогнозування

Прогнозування динаміки мережі є ще однією сильною стороною цієї моделі. Вона дозволяє моделювати різні сценарії поширення інформації та оцінювати ефект видалення ключового вузла або впровадження альтернативної інформації через впливових користувачів. Це дає можливість не тільки реагувати на поточні загрози, але й прогнозувати майбутні інформаційні атаки, розробляючи проактивні стратегії.

Отже, модель Курамото ефективно поєднує з аналізом впливових користувачів для ідентифікації ключових вузлів у соціальних мережах. Виявлені користувачі можуть бути як рушіями позитивних змін, так і потенційними джерелами дезінформації. Завдяки використанню фазової динаміки та центральності цей підхід забезпечує точний і ефективний аналіз інформаційних потоків.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розглянуто можливості застосування вдосконаленої моделі Курамото для аналізу поширення інформації та виявлення дезінформації у соціальних мережах. Запропонований підхід дозволяє ефективно ідентифікувати ключові вузли, що впливають на динаміку інформаційних потоків, моделювати сценарії поширення дезінформації та розробляти стратегії її нейтралізації. Основні переваги методу включають комплексний аналіз синхронізації інформаційних потоків, визначення критичних точок у мережі, гнучкість у застосуванні до різних платформ і оперативність аналізу. Інтеграція епідемічних моделей і врахування впливовості вузлів підвищує точність локалізації джерел дезінформації та ефективність боротьби з інформаційними загрозами. Подальші дослідження можуть бути спрямовані на удосконалення алгоритмів для адаптації моделі до різних типів мереж і платформ, інтеграцію вдосконаленої моделі Курамото з методами машинного навчання для автоматизації процесу виявлення дезінформації, розробку програмних засобів для візуалізації та моніторингу інформаційних потоків у реальному часі, а також на застосування моделі для аналізу не лише соціальних мереж, а й інших сфер, де поширення інформації відіграє важливу роль (економічні, медичні або політичні мережі). Запропонований підхід має значний потенціал для забезпечення інформаційної безпеки, що є особливо актуальним у сучасному світі інформаційних воєн та дестабілізуючих інформаційних кампаній.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Zittrain, J. L. (2018). The science of fake news. *Science, 359(6380),* 1094–1096. https://doi.org/10.1126/science.aao2998
2. Litvinchuk, I. S. (2023). Disinformation in social networks: Countermeasure algorithms. *Scientific Notes of V. I. Vernadsky Taurida National University, Series: Philology. Journalism, 2(1),* 181–186. https://doi.org/10.32782/2710-4656/2023.1.2/29

3. Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C. M., Brugnoli, E., Schmidt, A. L., Scala, A. (2020). The COVID-19 social media infodemic. *Scientific Reports, 10(1).* https://doi.org/10.1038/s41598-020-73510-5
4. On Media, Law of Ukraine № 2849-IX (2022) (Ukraine). https://zakon.rada.gov.ua/laws/show/2849-20#Texthttps://zakon.rada.gov.ua/laws/show/2849-20#Text
5. On National Security of Ukraine, Law of Ukraine. № 2469-VIII (2018) (Ukraine). https://zakon.rada.gov.ua/laws/show/2469-19#Text
6. On the Fundamentals of National Resistance, Law of Ukraine № 1702-IX (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/1702-20#Text
7. On the Decision of the National Security and Defence Council of Ukraine of 25 January 2015 'On the Establishment and Operation of the Main Situation Centre of Ukraine', Decree of the President of Ukraine № 115/2015 (2015) (Ukraine). https://zakon.rada.gov.ua/laws/show/115/2015#Text
8. 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
9. Pakhnin, M. L. (2024). Russian Disinformation as a Challenge to Ukrainian Statehood. *Bulletin of the Criminological Association of Ukraine, 31(1),* 860–868. https://doi.org/10.32631/vca.2024.1.79
10. Buhas, V., Ponomarenko, I., Kazak, O., Korshun, N. (2024). AI-Driven Sentiment Analysis in Social Media Content. In *Digital Economy Concepts and Technologies, vol. 3665,* 12–21.
11. Dudykevych, V., Yevseiev, S., Mykytyn, H., Ruda, K., Hulak, H. (2024). Detecting Deepfake Modifications of Biometric Images using Neural Networks. In *Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654,* 391–397.
12. Rzaieva, S., Rzaiev, D., Kostyuk, Y., Hulak, H., Shcheblanin, O. (2024). Methods of Modeling Database System Security. In *Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654,* 384–390.
13. Dmytriienko, K. A. (2024). Improvement of the Kuramoto Model for Modeling Information Dissemination in Social Networks. *Telecommunications and Information Technologies, 4(85),* 16–28. https://doi.org/10.31673/2412-4338.2024.048612
14. Rajeh, S., Savonnet, M., Leclercq, E., & Cherifi, H. (2021). Identifying influential nodes using overlapping modularity vitality. In A*SONAM '21: International conference on advances in social networks analysis and mining.* https://doi.org/10.1145/3487351.3488277
15. Chen, D., Lü, L., Shang, M.-S., Zhang, Y.-C., & Zhou, T. (2012). Identifying influential nodes in complex networks. *Physica A: Statistical Mechanics and Its Applications, 391(4),* 1777–1787. https://doi.org/10.1016/j.physa.2011.09.017
16. Lee, Y.-L., Wen, Y.-F., Xie, W.-B., Pan, L., Du, Y., & Zhou, T. (2024). Identifying influential nodes on directed networks. *Information Sciences, 677,* 120945. https://doi.org/10.1016/j.ins.2024.120945
17. Liu, P., Li, L., Fang, S., & Yao, Y. (2021). Identifying influential nodes in social networks: A voting approach. *Chaos, Solitons & Fractals, 152,* 111309. https://doi.org/10.1016/j.chaos.2021.111309
18. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Kateryna Dmytriienko
Graduate student of the Department ofInformation and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-7984-7279
k.dmytriienko.asp@kubg.edu.ua

Nataliia Korshun
Doctor of Science, Professor, Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

APPLICATION OF IMPROVED KURAMOTO MODELS FOR IDENTIFYING DISINFORMATION IN SOCIAL NETWORKS

Abstract. This article examines the problem of disinformation spreading in social networks and proposes advanced approaches for its identification based on improved Kuramoto models. In the modern world, social networks have become powerful communication tools that enable the rapid exchange of information among millions of people. At the same time, these networks facilitate the dissemination of disinformation — deliberately false or manipulative information used to influence public opinion and achieve political, social, or economic goals. The increasing scale of disinformation poses a serious threat to information security, societal stability, and trust in state institutions. To address this issue, the article proposes two modified Kuramoto models. The first model integrates with the SIR epidemic model, which accounts for the user states (infected, healthy, or recovered) and simulates the process of information dissemination. The second model incorporates the analysis of user influence by integrating a node centrality coefficient, allowing the identification of key participants who exert the greatest impact on information flows in the network. The proposed models offer several advantages. The SIR-based model enables the evaluation of content dissemination dynamics, localization of disinformation sources, and prediction of its propagation scenarios. The model based on influential users facilitates the identification of key network nodes, which can act as either sources of disinformation or instruments for its containment through the dissemination of verified information. The study highlights the importance of the adaptability of the proposed models to various social platforms and types of information flows. By integrating phase synchronization and node centrality, these models allow for the identification of not only popular users but also those who actively influence informational processes. This provides the ability to respond quickly to informational threats, reducing their impact on society.

Keywords: disinformation; social networks; improved Kuramoto model with the epidemic model; influential user model.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Zittrain, J. L. (2018). The science of fake news. *Science, 359(6380),* 1094–1096. https://doi.org/10.1126/science.aao2998
2. Litvinchuk, I. S. (2023). Disinformation in social networks: Countermeasure algorithms. *Scientific Notes of V. I. Vernadsky Taurida National University, Series: Philology. Journalism, 2(1),* 181–186. https://doi.org/10.32782/2710-4656/2023.1.2/29
3. Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C. M., Brugnoli, E., Schmidt, A. L., Scala, A. (2020). The COVID-19 social media infodemic. *Scientific Reports, 10(1).* https://doi.org/10.1038/s41598-020-73510-5
4. On Media, Law of Ukraine № 2849-IX (2022) (Ukraine). https://zakon.rada.gov.ua/laws/show/2849-20#Texthttps://zakon.rada.gov.ua/laws/show/2849-20#Text
5. On National Security of Ukraine, Law of Ukraine. № 2469-VIII (2018) (Ukraine). https://zakon.rada.gov.ua/laws/show/2469-19#Text

6. On the Fundamentals of National Resistance, Law of Ukraine № 1702-IX (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/1702-20#Text
7. On the Decision of the National Security and Defence Council of Ukraine of 25 January 2015 'On the Establishment and Operation of the Main Situation Centre of Ukraine', Decree of the President of Ukraine № 115/2015 (2015) (Ukraine). https://zakon.rada.gov.ua/laws/show/115/2015#Text
8. 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
9. Pakhnin, M. L. (2024). Russian Disinformation as a Challenge to Ukrainian Statehood. *Bulletin of the Criminological Association of Ukraine, 31(1),* 860–868. https://doi.org/10.32631/vca.2024.1.79
10. Buhas, V., Ponomarenko, I., Kazak, O., Korshun, N. (2024). AI-Driven Sentiment Analysis in Social Media Content. In *Digital Economy Concepts and Technologies, vol. 3665,* 12–21.
11. Dudykevych, V., Yevseiev, S., Mykytyn, H., Ruda, K., Hulak, H. (2024). Detecting Deepfake Modifications of Biometric Images using Neural Networks. In *Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654,* 391–397.
12. Rzaieva, S., Rzaiev, D., Kostyuk, Y., Hulak, H., Shcheblanin, O. (2024). Methods of Modeling Database System Security. In *Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654,* 384–390.
13. Dmytriienko, K. A. (2024). Improvement of the Kuramoto Model for Modeling Information Dissemination in Social Networks. *Telecommunications and Information Technologies, 4(85),* 16–28. https://doi.org/10.31673/2412-4338.2024.048612
14. Rajeh, S., Savonnet, M., Leclercq, E., & Cherifi, H. (2021). Identifying influential nodes using overlapping modularity vitality. In A*SONAM '21: International conference on advances in social networks analysis and mining.* https://doi.org/10.1145/3487351.3488277
15. Chen, D., Lü, L., Shang, M.-S., Zhang, Y.-C., & Zhou, T. (2012). Identifying influential nodes in complex networks. *Physica A: Statistical Mechanics and Its Applications, 391(4),* 1777–1787. https://doi.org/10.1016/j.physa.2011.09.017
16. Lee, Y.-L., Wen, Y.-F., Xie, W.-B., Pan, L., Du, Y., & Zhou, T. (2024). Identifying influential nodes on directed networks. *Information Sciences, 677,* 120945. https://doi.org/10.1016/j.ins.2024.120945
17. Liu, P., Li, L., Fang, S., & Yao, Y. (2021). Identifying influential nodes in social networks: A voting approach. *Chaos, Solitons & Fractals, 152,* 111309. https://doi.org/10.1016/j.chaos.2021.111309
18. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.