МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова

праця на правах

рукопису

ВАСИЛЬЄВА ОЛЬГА ОЛЕКСАНДРІВНА

УДК 004.[056.5:732(043.5)]

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ НА ОСНОВІ АГЕНТНОГО МОДЕЛЮВАННЯ

122 – Комп’ютерні науки

12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

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

_____ Васильєва Ольга

підпис

Науковий керівник Ткач Ю. М., завідувач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка», д.пед.н., к.т.н., професор

Чернігів – 2025

АНОТАЦІЯ

Ольга Васильєва. Інформаційна технологія виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки» (12 – «Інформаційні технології»). – Національний Університет «Чернігівська політехніка», МОН України, Чернігів, 2025.

В роботі вирішено актуальне наукове завдання з розробки методів та моделі для інформаційної технології виявлення інформаційних операцій в соціальних мережах, з врахуванням особливостей функціонування різних типів користувачів соціальних мереж.

Об'єктом дослідження є процес виявлення інформаційних операцій у соціальних мережах.

Предметом дослідження є методи, модель та інформаційна технологія виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання.

Метою дисертаційного дослідження є підвищення рівня інформаційної безпеки за рахунок розробки методів та моделі виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання.

Завдання дослідження полягає у розробці методів та моделі на основі агентного моделювання з різними типами агентів, а також створенні інформаційної технології для виявлення інформаційних операцій в соціальних мережах. Запропоновані методи та модель інтегруються в єдину інформаційну технологію, яка має потенціал для прикладного застосування в сфері національної інформаційної безпеки, інформаційної аналітики, стратегічних комунікацій та соціального моделювання.

Для проведення дослідження було застосовано метод системного аналізу, метод моделювання сценаріїв, методи експертних оцінок, контент-аналіз, мережеву аналітику, методи побудови математичних моделей впливу агентів, методи обчислення коефіцієнтів впливу агентів, імітаційне моделювання, методи математичного аналізу, графічне моделювання, моделювання динамічних процесів у багатоагентних системах, формування та дизайн баз даних, методи оптимізації, одно- та багатокритеріальний аналіз.

У вступі обґрунтовано актуальність теми дослідження, сформульовані мета, задачі та методи дослідження, наведено зв'язок дослідження з науковими програмами кафедри, описано наукову новизну і практичне значення результатів дисертаційної роботи. Визначено, що в умовах повномасштабної агресії РФ проти України, яка включає здійснення інформаційного впливу, моніторинг кіберпростору в частині соціальних медіа на предмет виявлення інформаційних загроз та організації протидії є важливим завданням національної безпеки України в інформаційній сфері. Також зазначено, що соціальні мережі наразі стали основним полем здійснення інформаційних операцій завдяки кількості цільової аудиторії, швидкості і горизонтальності розповсюдження контенту.

Оскільки існуючі на сьогодні методи виявлення інформаційних операцій у соціальних медіа не забезпечують комплексного вирішення проблеми, постає необхідність у розробленні підходів, що поєднують набір взаємодоповнюючих методів і моделі. Ефективне виявлення таких операцій вимагає міждисциплінарного підходу, який інтегрує знання та інструментарій із галузей інформатики, соціології, психології та комунікацій.

У першому розділі дисертації здійснено теоретико-аналітичне дослідження природи, змісту та особливостей інформаційних операцій у контексті їх впливу на інформаційну безпеку держави. Визначено, що на

сучасному етапі соціальні мережі набули ознак самостійного суб'єкта інформаційного впливу, що трансформує баланс сил у сфері інформаційних відносин. Наведено визначення поняття «інформаційна операція» та окреслено її відмінність від суміжного феномена психологічного впливу. Запропоновано структурно-функціональну модель інформаційних операцій, зокрема на прикладі деструктивної інформаційної діяльності російської федерації проти України. Аргументовано ефективність соціальних медіа як середовища реалізації інформаційних впливів. Проведено аналіз особливостей функціонування соціальних мереж як комунікаційних платформ, описано взаємодії користувачів і властивості поширення інформаційного контенту. Проаналізовано сучасні методи імітаційного моделювання соціальних процесів, зокрема моделі поширення інформації в соціальних мережах. Встановлено, що парадигма агентного моделювання найкраще відповідає завданню відтворення складних, багаторівневих інформаційних взаємодій із врахуванням поведінкових характеристик агентів (користувачів). Обґрунтовано доцільність застосування агентного моделювання для інформаційних операцій як процесу взаємодії множини гетерогенних агентів (користувачів різних типів), що діють у межах нелінійного цифрового середовища за певними правилами.

У другому розділі обґрунтовано доцільність застосування агентного моделювання як основного підходу до побудови моделі виявлення інформаційних операцій у соціальних мережах. Запропоновано комплексний метод моделювання, який поєднує п'ять сучасних методів: поширення впливу (Influence Maximization) для ідентифікації ключових агентів-інфлюенсерів; метод Монте-Карло для симуляції ймовірнісних рішень агентів; генетичний метод для покращення їхніх стратегій поведінки; метод Louvain для виявлення кластерної структури мережі; механізми зворотного зв'язку для відображення динамічних змін станів агентів у часі. Поєднання зазначених компонентів забезпечує створення гнучкої,

адаптивної та масштабованої моделі, здатної імітувати складні сценарії інформаційних операцій у соціальних мережах, включно з поширенням дезінформації, впливом лідерів думок, когнітивною реакцією аудиторії тощо. Визначено чотири типи користувачів – агентів – соціальних мереж, розроблено класифікацію цих агентів за рівнем впливу, а також запропоновано метод розрахунку коефіцієнтів впливу агентів під час здійснення інформаційної операції, що враховуватимуться при побудові агентної моделі.

У третьому розділі розроблено агентну модель виявлення інформаційних операцій у соціальних мережах з урахуванням як однорідного (звичайні користувачі), так і гетерогенного (чотири типи агентів: лідери думок, боти, тролі, звичайні користувачі) середовищ. Проведено імітаційні експерименти, що дозволили дослідити динаміку поширення контенту, вплив кожного типу агентів на зміну станів соціальної мережі та виявити ключові закономірності функціонування інформаційних потоків. Побудовано інформаційну технологію, яка базується на запропонованій агентній моделі й реалізує повний цикл аналізу інформаційних операцій: від збору метаданих до моделювання та візуалізації поширення інформації. Визначено її відповідність 10 базовим елементам інформаційних операцій, що дозволяє вважати розроблену систему перспективною для прикладного застосування в інформаційній безпеці, інформаційній аналітиці та стратегічних комунікаціях.

Четвертий розділ містить результати практичної реалізації за рахунок удосконалення системи моніторингу інформаційного контенту та експериментальної перевірки запропонованої агентної моделі в межах створеної інформаційної технології виявлення інформаційних операцій у соціальних мережах. Реалізовано інтеграцію чотирьох типів агентів із розрахунком коефіцієнтів їхнього впливу, а також перевірено комплексний метод у межах єдиної архітектури. Впроваджено метод автоматизованої

ідентифікації типів агентів на основі метаінформації про акаунти, що дало змогу формувати вхідні дані для симуляцій. Здійснено інтеграцію в модуль системи моніторингу з обробкою структурованих даних про контент, джерела та взаємодії, що забезпечило побудову моделі поширення інформації, візуалізацію мережевої структури та виявлення ознак скоординованої активності. Отримані результати – зокрема оцінка загального охоплення, автоматизована класифікація користувачів, виділення ключових вузлів впливу – підтвердили прикладну ефективність інформаційної технології та її спроможність до структурного аналізу інформаційних потоків у цифровому середовищі.

Основні результати дослідження та наукова новизна полягають у розробці та верифікації комплексного підходу до виявлення інформаційних операцій у соціальних мережах шляхом поєднання двох методів та агентної моделі з імітаційними експериментами. Уперше запропоновано агентну модель, яка враховує чотири типи агентів (лідери громадської думки, боти, тролі, звичайні користувачі) з диференційованими коефіцієнтами впливу. Наведено математичну постановку задачі моделювання, запропоновано комплексний метод виявлення ІО для агентної моделі, що інтегрований в єдину інформаційну технологію. Запропоновано програмну реалізацію моделі та проведено серію імітаційних експериментів, які підтверджують ефективність розробленого підходу для аналізу структурно-поведінкових характеристик інформаційних операцій у цифровому середовищі.

Мультимодальність запропонованої агентної моделі полягає у синтезі кількох підходів до імітаційного моделювання інформаційних операцій у соціальних мережах. У моделі одночасно враховано топологічні характеристики мережевої структури (структурний підхід), індивідуальні поведінкові особливості агентів (агентна парадигма), часову динаміку активності користувачів (динамічний підхід), а також соціальні реакції, що відображаються у зміні моделей взаємодії (соціологічний вимір). Такий

комплексний підхід забезпечує високий рівень адекватності моделі для аналізу складних інформаційних процесів і дозволяє відтворювати ключові характеристики реальних інформаційних операцій.

Визначено основні сутності, що закладають основу функціонування нової інформаційної технології:

1. Агентна модель виявлення інформаційних операцій в соціальних мережах на основі агентного моделювання та її програмний код.
2. Метод розрахунку коефіцієнту впливу кожного типу агенту.
3. Комплексний метод виявлення інформаційних операцій.
4. Моделювання з одним типом агентів (тільки звичайні користувачі).
5. Моделювання з чотирма типами агентів (всі типи агентів).

На основі отриманих результатів сформовано архітектуру інформаційної технології для виявлення інформаційних операцій у соціальних мережах. Ця інформаційна технологія є уніфікованим інструментом для проведення експериментів, побудови симуляцій інформаційних операцій, виявлення ключових акторів впливу, та формування системи стратегічного реагування на основі даних. Технологія має потенціал для прикладного застосування в сфері національної інформаційної безпеки, інформаційної аналітики, стратегічних комунікацій та соціального моделювання.

Ключові слова: інформаційна технологія, інформаційна безпека, кібербезпека, забезпечення національної безпеки, дезінформація, достовірність інформації, інформаційні загрози, моделювання, соціальні мережі, інформаційні операції, агентне моделювання, гібридний вплив, соціальна інженерія, кіберпростір, лідери громадської думки, боти, тролі, бот-мережі, фейкові акаунти, deepfake, маніпулятивний контент, гарантоздатність, інформаційні атаки, соціальні середовища, контент-аналіз, поширення інформації, ключові вузли, графова модель, соціальна

інженерія, захист інформації, загрози, інформація, користувач, математичне моделювання.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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

1. Ольга Васильєва Моделі виявлення та прогнозування динаміки інформаційних операцій у соціальних мережах. Технічні науки та технології: науковий журнал / Національний університет «Чернігівська політехніка». – Чернігів: НУ «Чернігівська політехніка», 2023. – № 2(32). – 418 с., С-193.

2. Ольга Васильєва Типологія агентів та їх вплив на поширення дезінформації в соціальній мережі X, Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" Том 4 № 28 (2025), с. 751-765, DOI: https://doi.org/10.28925/2663-4023.2025.28.862.

3. О.О. Васильєва Алгоритми та методи моделювання інформаційних операцій в соціальних мережах, Інформація та математичні методи в моделюванні, Том 15 № 2 (2025), с.176-186, DOI 10.15276 /imms.v15.no2.176.

Наукові статті, опубліковані у періодичних наукових виданнях, проіндексованих в базі даних Scopus

1. O Vasylieva, B Butvin, Y Shtyfurak Methodological Approach to Agent-Based Modeling of Social Networks, CEUR Workshop Proceedings, 2021, pp 343-348 (Особистий внесок здобувача: методологічні підходи, які використовуються для аналізу соціальних мереж та їхнє застосування при агентному моделюванні соціальних мереж).

2. Yuliia Tkach, Anatolii Shyian, Olha Vasylieva, Ihor Diuba Method of Effective Counteraction Against Negative Information-Psychological Impact on the Regional Community by Using Social Networks, Lecture Notes in Networks and Systems, 2024, pp 239-251 (Особистий внесок здобувача: метод аналізу наративів та формування баз даних при виявлення інформаційних операцій в соціальних мережах на регіональному рівні).

3. Olha Vasylieva, Tkach Yuliia Agent-based modelling of information dissemination processes in social networks, Lecture Notes in Networks and Systems, 25 April 2025, pp 195-211 (Особистий внесок здобувача: порівняльні характеристики середовищ агентного моделювання, імітаційна модель розповсюдження контенту в соціальних мережах на основі агентного моделювання).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Васильєва О.О. Виявлення в інформаційному просторі інформаційно-пропагандистських кампаній РФ з використанням соціальних мереж // Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. – Київ: НУОУ, 2017. – С. 22-25.

2. Васильєва О.О. Застосування методу агентного моделювання для виявлення інформаційних операцій // Актуальні питання забезпечення кібербезпеки та захисту інформації: Матеріали VII міжнарод. наук.-практ. конф., 24–27 лютого 2021 р. / Редкол.: І.І. Тимошенко та ін. – К. : Вид-во Європейського університету, 2021. – С.10-12

3. Васильєва О.О. Протидія інформаційним операціям як елемент інформаційної безпеки держави // Формування дієвих механізмів державного управління з забезпечення державної безпеки: Збірник матеріалів круглого столу. – Харків, 2021. – С. 250-253

4. Васильєва О.О. Щодо міжвідомчої взаємодії для виявлення маніпуляцій в інформаційній сфері та автоматизації цих процесів // Протидія фейкам в Україні як складова інформаційної безпеки держави: Міжвідомчий круглий стіл, 20 травня 2021 року. – Київ: ІСТЕ СБУ, 2021. – С 20-26.

5. Olga Vasylieva Simulation models in modeling information operations in social networks. Proceedings of the XII International Scientific Conference "IT Sec-2023", May 2-4, 2023, Uzhgorod, P. 48-50

6. Olha Vasylieva Social media: from communication to security threats ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 265 с., С-46-48.

7. Ольга Васильєва Середовища для агент-орієнтовного моделювання: комплексний огляд XIV Міжнародна науково-практична конференція студентів, аспірантів та молодих учених «ЮНІСТЬ НАУКИ – 2024», 24-26 квітня 2024 р.

ABSTRACT

Olga Vasilyeva. Information technology for detecting information operations in social networks based on agent modelling. – Qualification scientific work in the form of a manuscript.

PhD in Engineering Science under Specialty 122 – "Computer Science – National University "Chernihiv Polytechnic", Ministry of Education and Science of Ukraine, Chernihiv, 2025.

The work solves a current scientific task of developing methods and model for an information technology to detecting information operations in social networks, taking into account the functional specifics of various types of social media users as components of decentralized systems.

The object of the research is the process of detecting information operations in social networks.

The subject of the research is models, methods and information technologies for detecting information operations in social networks based on agent-based modelling.

The purpose of the research is to enhance the level of information security by developing methods and a model for detecting information operations in social networks using agent-based modeling.

The task of the research is to develop methods and models of agent-based modelling with different types of agents, and developing an integrated information technology for detecting information operations in social networks. The proposed methods and model are consolidated into a unified technological framework with potential applications in national information security, information analytics, strategic communications, and social modeling.

The research employs system analysis, scenario modeling, expert evaluation methods, content analysis, network analytics, mathematical modeling of agent influence, computation of influence coefficients, simulation modeling, mathematical analysis, graphical modeling, modeling of dynamic processes in

multi-agent systems, database design, optimization methods, and single- and multi-criteria analysis.

The introduction substantiates the relevance of the research topic, formulates the purpose, objectives, and methods of the research, describes the connection between the research and the scientific programs of the department, and describes the scientific novelty and practical significance of the dissertation results. It is determined that in the context of full-scale aggression by the Russian Federation against Ukraine, which includes the use of information influence, monitoring cyberspace in terms of social media to identify information threats and organize countermeasures is an important task for Ukraine's national security in the information sphere. It is also noted that social networks have now become the main field for information operations due to the size of the target audience and the speed and horizontality of content distribution.

Since the methods currently used to detect information operations on social media do not provide a comprehensive solution to the problem, there is a need to develop approaches that combine a set of complementary methods and models. Effective detection of such operations requires an interdisciplinary approach that integrates knowledge and tools from the fields of computer science, sociology, psychology, and communications.

The first chapter provides a theoretical and analytical study of the nature, content, and characteristics of information operations in the context of their impact on state information security. It is determined that, at the present stage, social networks have acquired the characteristics of an independent subject of information influence, which transforms the balance of power in the sphere of information relations. The definition of the concept of “information operation” is given and its difference from the related phenomenon of psychological influence is outlined. A structural-functional model of information operations is proposed, in particular using the example of the Russian Federation's destructive information activities against Ukraine. The effectiveness of social media as a

medium for information influence is argued. An analysis of the features of social networks as communication platforms is conducted, and user interactions and the properties of information content dissemination are described. Modern methods of simulation modeling of social processes are analyzed, in particular, models of information dissemination in social networks. It is established that the agent-based modeling paradigm best suits the task of reproducing complex, multi-level information interactions, taking into account the behavioral characteristics of agents (users). The feasibility of using agent-based modeling for information operations as a process of interaction between a set of heterogeneous agents (users of different types) operating within a nonlinear digital environment according to certain rules is substantiated.

The second chapter justifies the feasibility of using agent-based modeling as the main approach to building a model for detecting information operations in social networks. A comprehensive modeling method is proposed that combines five modern methods: Influence Maximization for identifying key influencer agents; the Monte Carlo method for simulating probabilistic decisions of agents; the genetic method for improving their behavior strategies; the Louvain method for detecting the cluster structure of the network; feedback mechanisms for reflecting dynamic changes in agent states over time. The combination of these components provides a flexible, adaptive, and scalable model capable of simulating complex scenarios of information operations in social networks, including the spread of misinformation, the influence of opinion leaders, the cognitive response of the audience, etc. Four types of users—agents—of social networks have been identified, a classification of these agents by level of influence has been developed, and a method for calculating the influence coefficients of agents during an information operation has been proposed, which will be taken into account when constructing the agent model.

The third section develops an agent model for detecting information operations in social networks, taking into account both homogeneous (ordinary

users) and heterogeneous (four types of agents: opinion leaders, bots, trolls, ordinary users) environments. Simulation experiments were conducted to study the dynamics of content dissemination, the influence of each type of agent on changes in the state of the social network, and to identify key patterns in the functioning of information flows. An information technology was developed based on the proposed agent model, which implements a full cycle of information operations analysis: from metadata collection to modeling and visualization of information dissemination. Its compliance with the 10 basic elements of information operations has been determined, which allows us to consider the developed system promising for applied use in information security, information analytics, and strategic communications.

The fourth section contains the results of practical implementation through the improvement of the information content monitoring system and experimental testing of the proposed agent model within the framework of the created information technology for detecting information operations in social networks. The integration of four types of agents with the calculation of their impact coefficients has been implemented, and a comprehensive method has been tested within a single architecture. A method for automated identification of agent types based on meta-information about accounts has been implemented, which made it possible to generate input data for simulations. Integration into the monitoring system module with processing of structured data on content, sources, and interactions was carried out, which ensured the construction of a model of information dissemination, visualization of the network structure, and detection of signs of coordinated activity. The results obtained—in particular, the assessment of overall coverage, automated user classification, and identification of key nodes of influence—confirmed the applied effectiveness of information technology and its ability to structurally analyze information flows in a digital environment.

The main results of the study and scientific novelty lie in the development and verification of a comprehensive approach to identifying information operations in social networks by combining two methods and an agent-based model with simulation experiments. For the first time, an agent model is proposed that takes into account four types of agents (opinion leaders, bots, trolls, ordinary users) with differentiated influence coefficients. A mathematical formulation of the modeling problem is presented, and a comprehensive method for detecting IO for the agent model, integrated into a single information technology, is proposed. A software implementation of the model is proposed and a series of simulation experiments are conducted, confirming the effectiveness of the developed approach for analyzing the structural and behavioral characteristics of information operations in a digital environment.

The multimodality of the proposed agent model consists in the synthesis of several approaches to simulation modeling of information operations in social networks. The model simultaneously takes into account the topological characteristics of the network structure (structural approach), the individual behavioral characteristics of agents (agent paradigm), the temporal dynamics of user activity (dynamic approach), as well as social reactions reflected in changes in interaction patterns (sociological dimension). This comprehensive approach ensures a high level of model adequacy for analyzing complex information processes and allows reproducing key characteristics of real information operations.

The main entities that together constitute information technology have been identified:

1. Agent model for detecting information operations in social networks based on agent modelling and its program code.
2. Method for calculating the influence coefficient of each type of agent.
3. Comprehensive method for detecting information operations.
4. Modeling with one type of agent (only regular users).

5. Modeling with four types of agents (all types of agents).

Based on the results obtained, an information technology architecture has been developed to detect information operations in social networks. This information technology is a unified tool for conducting experiments, building simulations of information operations, identifying key actors of influence, and forming a data-driven strategic response system. The technology has the potential for practical application in the fields of national information security, information analytics, strategic communications, and social modeling.

Keywords: information technology, information security, cybersecurity, national security, disinformation, information reliability, information threats, modeling, social networks, information operations, agent modeling, hybrid influence, social engineering, cyberspace, opinion leaders, bots, trolls, botnets, fake accounts, deepfakes, manipulative content, guarantee ability, information attacks, social environments, content analysis, information dissemination, key nodes, graph model, social engineering, information protection, threats, information, user, mathematical modeling.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІО – інформаційна операція

АМ – агентне моделювання

МСМС – Метод Монте-Карло

ЛГД / ЛД – лідери громадської думки / лідери думок

ІТ – інформаційна технологія

ВСТУП

Актуальність теми дослідження. В умовах триваючої повномасштабної агресії Російської Федерації проти України інформаційна складова набуває дедалі більшого значення як інструмент гібридного впливу. Соціальні мережі використовуються агресором для ведення систематичних інформаційних операцій, спрямованих на деморалізацію українського суспільства, підрив довіри до інституцій влади, маніпулювання громадською думкою та дестабілізацію внутрішньої ситуації. Таким чином, моніторинг кіберпростору, зокрема сегменту соціальних мереж, з метою виявлення загроз і організації ефективної протидії, є одним із пріоритетних завдань у системі забезпечення національної безпеки.

Соціальні мережі надають нові можливості для організації інформаційного впливу завдяки своїй децентралізованій природі, алгоритмічній селекції контенту, відсутності редакційного контролю та високому рівню персоналізації. У такому середовищі навіть звичайний користувач без медійного бекграунду може отримати мільйонну аудиторію, що робить поширення дезінформації вкрай швидким, масштабним і складним для виявлення на ранніх етапах. Цей ефект підсилюється використанням бот-мереж, фейкових акаунтів і маніпулятивного контенту, який резонує з емоційним станом аудиторії.

Значна кількість інформаційних атак реалізується за допомогою новітніх технологій: використанням штучного інтелекту, генеративних моделей, інструментів мікротаргетингу та сценарного планування. Особливо небезпечними є операції, які не мають єдиної структури або шаблону, оскільки кожна з них розробляється під конкретну соціальну ситуацію та цільову аудиторію. Це значно ускладнює їхнє виявлення, адже класичні методи, що базуються на ретроспективному аналізі (наприклад, виявлення типового циклу «вкид – пауза – пік – згасання»), часто виявляються неефективними.

У зв’язку з цим, особливої актуальності набуває використання інструментів, що здатні враховувати динамічну, неконтрольовану та багатофакторну природу інформаційного простору. Одним з таких інструментів є агентне моделювання – метод, що дозволяє відтворювати поведінку окремих користувачів як автономних агентів, які взаємодіють між собою в умовах соціального середовища. У такому підході глобальні ефекти розповсюдження контенту виникають у результаті локальної взаємодії агентів, що відображає реальні процеси функціонування соціальних мереж.

Агентне моделювання дозволяє враховувати особливості різних типів користувачів: лідерів думок, акаунтів-ботів, акаунтів-тролів і звичайних користувачів. Це відкриває можливості для формалізованого опису сценаріїв поширення дезінформації, ідентифікації критичних агентів, які мають найбільший вплив на інформаційний простір, та прогнозування наслідків інформаційних кампаній. Крім того, це дозволяє створювати експериментальні середовища для тестування різних алгоритмів виявлення інформаційних операцій в умовах, максимально наближених до реальних.

Незважаючи на зростаючий інтерес до проблеми виявлення інформаційних операцій, сучасні дослідження здебільшого зосереджуються на контент-аналізі або використанні обмежених наборів індикаторів. Проте ситуація вимагає формування комплексної інформаційної технології, здатної здійснювати виявлення інформаційних операцій у реальному часі з урахуванням як структурних параметрів соціальних мереж, так і поведінкових характеристик користувачів.

У цьому контексті актуальним науковим завданням є **розробка та впровадження методів і моделі**, які інтегровані в інформаційну технологію, що забезпечують ефективне виявлення інформаційних операцій у соціальних мережах.

У дисертаційному дослідженні запропоновано ряд **методів і модель** на основі агентного моделювання, які в сукупності формують інформаційну

технологію виявлення інформаційних операцій. Запропонована модель дозволяє досліджувати сценарії негативного інформаційного впливу, змінювати параметри мережевої взаємодії та адаптувати алгоритми під конкретні цілі і умови.

Таким чином, запропонована інформаційна технологія спрямована на усунення наявних обмежень традиційних методів виявлення інформаційних операцій і має практичну цінність для підвищення інформаційної безпеки держави, зокрема в контексті боротьби з гібридною агресією в кіберпросторі.

Зв'язок роботи з науковими програмами, планами, темами. Представлена дисертаційна робота запланована та виконана відповідно до плану науково–дослідної роботи Національного університету «Чернігівська політехніка» «Методи та засоби забезпечення безпеки ресурсів інформаційних систем» (№ 0117U003187); «Методологія побудови захищеного простору» (№ 0124U004485).

Мета й завдання дослідження. *Метою дисертаційного дослідження* є підвищення рівня інформаційної безпеки за рахунок розробки методів та моделі виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання.

Для досягнення мети дослідження в дисертації сформульовані та вирішені наступні **завдання**:

- проаналізувати сучасні методи та моделі виявлення інформаційних операцій у соціальних мережах та обґрунтувати доцільність використання агентного моделювання;
- розробити комплексний метод виявлення інформаційних операцій;
- розробити класифікацію агентів в соціальній мережі та метод розрахунку коефіцієнту впливу різних типів агентів на соціальну мережу;

- розробити агентну модель розповсюдження контенту, що дозволяє виявляти інформаційні операції з урахуванням поведінкових характеристик агентів;

- розробити архітектуру інформаційної технології, орієнтовану на практичне застосування для виявлення інформаційних операцій у соціальних мережах;

- удосконалити систему моніторингу інформаційного контенту та провести імітаційні експерименти для верифікації ефективності запропонованої моделі та методів.

Об'єкт дослідження – процес виявлення інформаційних операцій у соціальних мережах.

Предмет дослідження – методи, модель та інформаційна технологія виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання.

Методи дослідження. Для проведення дослідження було застосовано метод системного аналізу, метод моделювання сценаріїв, методи експертних оцінок, контент-аналіз, мережеву аналітику, методи побудови математичних моделей впливу агентів, методи обчислення коефіцієнтів впливу агентів, імітаційне моделювання, методи математичного аналізу, графічне моделювання, моделювання динамічних процесів у багатоагентних системах, формування та дизайн баз даних, методи оптимізації, одно- та багатокритеріальний аналіз.

Наукова новизна результатів досліджень полягає в наступному:

- *вперше* розроблено комплексний метод для виявлення інформаційних операцій на основі комбінації п'яти методів, що застосовуються у відповідній послідовності та інтегруються в агентну модель, який, на відміну від інших, забезпечує побудову агентної моделі, враховуючи як стратегічну поведінку агентів, так і динамічну взаємодію в соціальних мережах, що дозволяє

моделювати складні сценарії, як-от поширення дезінформації, вплив лідерів думок, динаміка зміни думок у мережі та адаптація агентів у реальному часі;

- *вперше* розроблено метод розрахунку коефіцієнтів впливу з урахуванням поведінкових характеристик чотирьох типів агентів: лідерів думок, ботів, тролів і звичайних користувачів, що, на відміну від інших, дозволяє конструювати стратегії впливу з акцентом на потрібний тип агентів та здійснювати більш точне прогнозування динаміки поширення повідомлень;
- *набула подальшого розвитку* модель інформаційних операцій в соціальних мережах на основі агентного моделювання, яка, на відміну від існуючих, орієнтована на функціонування різних типів агентів – користувачів, що дозволяє підвищити заходи з інформаційної безпеки завдяки врахуванню специфічної поведінки акторів в соціальних мережах;
- *удосконалено* систему моніторингу за рахунок впровадження модулю із застосуванням методів і агентної моделі для виявлення інформаційних операцій в соціальних мережах, що, на відміну від інших, дозволяє не лише фіксувати факт активності різних типів користувачів у межах інформаційної операції, але й кількісно оцінити реакцію аудиторії, побудувати агентні моделі поширення та виявити ключові маршрути трансляції контенту, що є критичним для раннього виявлення ймовірної інформаційної операції.

Практичне значення отриманих результатів.

Наведені вище наукові результати у своїй сукупності утворюють нову інформаційну технологію виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання. Дана інформаційна технологія може слугувати основою для побудови ефективного захисту соціальних систем від негативного інформаційного впливу, основаних на агентному

моделюванні. Отримана інформаційна технологія може імплементуватися окремими модулями в системи моніторингу та налаштовуватися на вимогу конкретної ситуації, в тому числі здійснювати оптимізацію за вибраними критеріями. *Практична цінність полягає в наступному:*

- розроблено інформаційну технологію для виявлення інформаційних операцій у соціальних мережах, яка, на відміну від існуючих, використовує методи і агенту модель, де агентами є різні типи користувачів соціальних мереж, що дозволяє одночасно здійснювати чітку ідентифікацію агентів впливу та симуляцію їхньої ролі при моделюванні поширення інформації, включаючи ефект «порогу охоплення», виявляти ключові спільноти у мережі для цільового впливу та цільові аудиторії, аналізувати вплив різних сценаріїв активності ботів і тролів на загальну ефективність інформаційної операції та будувати топології інформаційної операції, що значно підвищило ефективність при виявленні інформаційних операцій та сприяло в подальшому організації протидії та підвищенню рівня інформаційної безпеки;
- запропонований метод розрахунку коефіцієнту впливу різних типів користувачів на розповсюдження контенту дозволив здійснювати оцінку впливу різних типів користувачів під час інформаційної операції, що забезпечило точну ідентифікацію структурно-важливих елементів мережі, які є критичними для детекції та подальшої нейтралізації організованих інформаційних впливів, зокрема в рамках координації інформаційних атак чи кампаній дезінформації (акт про впровадження № 435/25 від 29.07.2025);
- результати досліджень впроваджено в навчальний процес до робочих програм навчальних дисциплін освітніх програм «Кібербезпека» у Національному університеті «Чернігівська політехніка» (акт впровадження від 30.06.2025);

- удосконалено систему моніторингу соціальних мереж «Capsmi» за рахунок програмних модулів для розрахунку коефіцієнтів впливу агентів при різних вхідних параметрах, для побудови агентних моделей з одним та з чотирма типами користувачів, що дозволило здійснювати оцінку впливу контенту, ідентифікацію ключових вузлів за критеріями центральності, визначати охоплення цільової аудиторії та будувати стратегію подальшого поширення контенту, що є критичним для раннього виявлення ймовірної інформаційної операції (довідка про впровадження №2121/25-03/2-25 від 24.07.2025).

Результати дисертаційного дослідження впроваджені:

в Раді національної безпеки і оборони України при виявленні та аналізі інформаційних загроз в соціальних медіа кіберпростору для прийняття стратегічних рішень для протидії (Довідка про впровадження № 2121/25-03/2-25 від 24.07.2025, Додаток 1);

в ТОВ «НВЦ «ІНФОЗАХИСТ» при виявляти ознаки інформаційних операцій у соціальних мережах та оцінці інформаційних впливів (Акт про впровадження вих. № 435/25 від 29.07.2025, Додаток 2);

в освітньому процесі Національного університету «Чернігівська політехніка» кафедри кібербезпеки та математичного моделювання до робочих програм навчальних дисциплін освітніх програм «Кібербезпека» зі спеціальності F5 «Кібербезпека та захист інформації» (Акт про впровадження від 30.06.2025, Додаток 3).

Особистий внесок здобувача. Наукові результати, викладені в дисертаційній роботі, отримані автором особисто. В наукових роботах, опублікованих у співавторстві, в дисертації використані лише ті ідеї та положення, що є результатом особистої роботи.

Апробація результатів дисертації.

Основні положення дисертаційного дослідження доповідалися та обговорювалися на міжнародній міжнародної науково-практичної

конференції «Інформаційний вимір гібридної війни: досвід України» (м. Київ, квітень 2017), VII Міжнародній науково-практичній конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», (м. Київ, 24-27 лютого 2021р.), круглому столі «Формування дієвих механізмів державного управління з забезпечення державної безпеки» (Харків, 2021), Міжвідомчому круглому столі «Протидія фейкам в Україні як складова інформаційної безпеки держави» (м. Київ, 20 травня 2021 року), XII Міжнародній науковій конференції «IT Sec-2023» (м. Ужгород, 2-4 травня 2023 р.), XIV Міжнародній науково-практичній конференції студентів, аспірантів та молодих учених «ЮНІСТЬ НАУКИ – 2024» (м. Чернігів, 24-26 квітня 2024 р.) та XIII Міжнародній науково-технічній конференції «Безпека інформаційних технологій» (м. Львів, 9-11 трав. 2024).

Публікації. За темою дисертаційного дослідження з викладенням основних результатів опубліковано 13 наукових праць. Серед них 3 статті у фахових журналах, 3 включені до міжнародної наукометричної бази Scopus та опубліковані в закордонних виданнях. Результати роботи доповідалися на 7 міжнародних наукових конференціях.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, 4 розділів (глав), висновків, переліку умовних скорочень, переліку посилань зі 118 джерел та 7 додатків. Загальний обсяг роботи становить 167 сторінок, з яких основний текст на 153 сторінках, зміст на 2 сторінках, вступ на 7 сторінках, перелік умовних скорочень на 1 сторінці, список використаних джерел із 118 найменувань на 14 сторінках, 7 додатків на 68 сторінках. Робота містить 32 рисунки та 18 таблиць.

РОЗДІЛ 1. АНАЛІЗ ПІДХОДІВ ТА ОСНОВНИХ МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ

1.1. Інформаційні операції як загроза інформаційної безпеки держави: поняття, ключові елементи, алгоритм проведення

В умовах повномасштабної гібридної війни країни-агресора проти України виявлення та прогнозування інформаційних загроз є важливим завданням забезпечення національної безпеки України в інформаційній сфері.

У статті 17 Конституції України [1] визначено, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та *інформаційної безпеки* є найважливішими функціями держави, справою всього Українського народу».

Таким чином, Конституція України ставить досягнення інформаційної безпеки держави на один щабель із захистом її суверенітету і територіальної цілісності. І це є невипадковим, оскільки у сучасній ситуації цілеспрямовані інформаційні впливи здатні формувати у населення викривлену картину світу [2], спонукати до вчинення таких дій, на які б воно (населення) самостійно не наважилося і, скоріш за все, об’єктивно не хотіло.

Засади забезпечення інформаційної безпеки України та протидії загрозам безпеці держави в інформаційній сфері визначені в Стратегії інформаційної безпеки України (2021 року) [3], зокрема:

глобальних дезінформаційних кампаній стає все більше і до них долучаються не лише державні актори;

та захист особистих/приватних прав людини;

зростання значення цифрових технологій на фоні низького рівня медіа грамотності та цифрової обізнаності населення;

інформаційно-психологічний вплив на населення з боку зарубіжних країн;

обмежені можливості реагувати на дезінформаційні кампанії;

слабка координація протидії зовнішнім та внутрішнім інформаційним загрозам;

маніпуляція свідомістю громадян щодо вступу України в ЄС та НАТО;

недостатній рівень культури цифрової та медіаграмотності населення для протидії маніпулятивним та інформаційно-психологічним впливам.

Отже поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у її чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних, в тому числі використання інформації для здійснення психологічних чи інформаційних впливів на населення держави [56].

У науковому, військовому, політичному та міжнародному дискурсі термін «інформаційно-психологічна війна» поєднує в собі інформаційні та психологічні операції. Він підкреслює особливу небезпеку та руйнівний характер даного явища особливо тому, що наразі практично повністю відсутні механізми міжнародного регулювання і контролю за проведенням інформаційних та психологічних операцій, що дозволяє країнам-агресорам безкарно проводити їх в інформаційному просторі різних країнах і зонах міжнародних конфліктів і втручатися у внутрішні справи інших держав [57].

Однак слід розмежувати поняття інформаційні та психологічні операції: інформаційні операції на відміну від психологічних базуються не стільки на особливостях людської психіки, скільки на характерних рисах соціально-політичної комунікації у суспільствах, де вони здійснюються. Тобто заходи і прийоми інформаційної операції передбачають вплив на структуру суспільної комунікації супротивника, а не безпосередньо на свідомість [4].

В роботах автора [5] визначено відмінність між інформаційними та психологічними операціями, керуючись відмінністю не лише функцій, а також і суб'єктів, об'єктів та цільових аудиторій даних видів інформаційного протиборства (див. Табл. 1.1).

Таблиця 1.1

Відмінність між інформаційними та психологічними операціями.

	Інформаційні операції	Психологічні операції
Функція	Забезпечити інформаційну підтримку дій у фізичному просторі	Надати психологічну допомогу
Цільова аудиторія	Визначена група осіб/особа, що ухвалює рішення	Населення регіону конфлікту, військовослужбовці
Основний суб'єкт	Спецслужби, сили спеціальних операцій	Служби психологічного забезпечення у штаті військових підрозділів
Об'єкт впливу	Контент, канали комунікації (ЗМІ, Інтернет ЗМІ, соціальні мережі, тимчасово переміщені особи тощо)	Індивідуальна та масова свідомість

Інформаційні операції – це поняття, зміст якого охоплює та розкриває інформаційний вплив на масову свідомість (як на ворожу, так і на дружню), вплив на інформацію, доступну супротивникові та необхідну йому для прийняття рішень, а також на інформаційно-аналітичні системи супротивника [6].

Деякі фахівці визначають інформаційні операції як сукупність заходів гласного та негласного характеру, спрямованих на приховане керування процесами інформаційної сфери. На відміну від пропагандистських заходів, вони мають обмежену у часі тривалість, підпорядковані конкретній меті та координуються єдиним центром – спеціальними службами [7].

У матеріалах конференції «Актуальні проблеми управління інформаційною безпекою держави» зазначається, що «інформаційний вплив на державу, суспільство, громадянина зараз більш ефективний і економний, ніж політичний, економічний і навіть воєнний» [8].

На це вплинула в тому числі і поява нових методів і прийомів, вони отримали наукове обґрунтування, на цьому фоні виникають наукові дисципліни про управління поведінкою людини та спільнот – соціологія, психоаналіз, теорія реклами, сугестологія, нейролінгвістичне програмування, контент-аналіз. Також виникають принципово нові електронні засоби масової інформації – фокус інформаційного впливу змістився у бік соціальних мереж [9].

Це стало можливим також тому, що соціальні платформи, такі як X та Facebook, мають принципово іншу структуру ніж будь-яка медіа-технологія минулого. Контент потрапляє до користувачів без фільтрів, без перевірки фактів на достовірність, без редакційної оцінки, а користувач без бекграунду та репутації може досягти такої самої кількості читачів як Fox News, CNN або New York Times.

Дослідженню феномену інформаційних операцій в соціальних мережах присвячно значну кількість наукових праць, серед яких В. Бех, Л. Дудко, В. Лепський, І. Петренко, Т. Хелмус, Е. Бодин-Барон, А. Радин, М. Магнусон, Дж. Мендельсон, В. Марчеллино, З. Винкельман, К. Старберд, К. Уордл, Х. Дерахшан та інші.

На основі аналізу зазначених робіт можна виділити 6 ключових елементів інформаційної операції.

1. Мета ІО – визначає стратегічну ціль ІО: вплинути на громадську думку, дестабілізувати ситуацію, делегітимізувати інститути влади. Так автори [10, 11] визначають мету як когнітивне моделювання реакцій аудиторії на певні наративи.

2. Визначення цільової аудиторії залежно від соціальних, вікових, політичних або національних ознак. В роботах [12, 13] підкреслюється важливість мікротаргетингу через алгоритми соціальних мереж.
3. Про формування наративу (інформаційного меседжу) йдеться в роботах [14], а саме вказується на гібридність меседжів (правда + маніпуляція). Автори [13, 15] зазначають, що меседж формується як наратив, прив'язаний до культурних кодів аудиторії.
4. Інфраструктура поширення (Distribution Infrastructure). Соціальні мережі (Facebook, X/Twitter, Telegram, TikTok) є основними платформами, завдяки комунікативним процесам та залученню таких акторів як бот-акаунти, тролі та лідери думок, що в свою чергу розширює коло залучених справжніх користувачів. За аналітичними матеріалами NATO Strategic Communications Centre of Excellence [16]: «комунікаційна архітектура» ІО є ключем до її ефективності.
5. Застосування механізмів впливу, таких як емоційні тригери (страх, гнів, ідентичність) [17], алгоритмічні підсилення – механізми рекомендацій на платформах [10], а також соціальне підтвердження, коли аудиторія бачить, що меседж вже підтриманий іншими.
6. Зворотний зв’язок і адаптація. Успішні ІО є динамічними – з корекцією меседжів залежно від реакції цільової аудиторії [18, 19].

Таким чином інформаційна операція в соціальних мережах – це системна, багатоетапна діяльність, що об'єднує когнітивні, соціотехнічні та алгоритмічні інструменти впливу. Її ключовими елементами виступають: мета, цільова аудиторія, меседж, мережеві канали, механізм впливу та адаптивність. Розуміння цих елементів є основою для виявлення ІО.

Схематично представити здійснення інформаційної операції можемо наступним чином (рис. 1.1.).

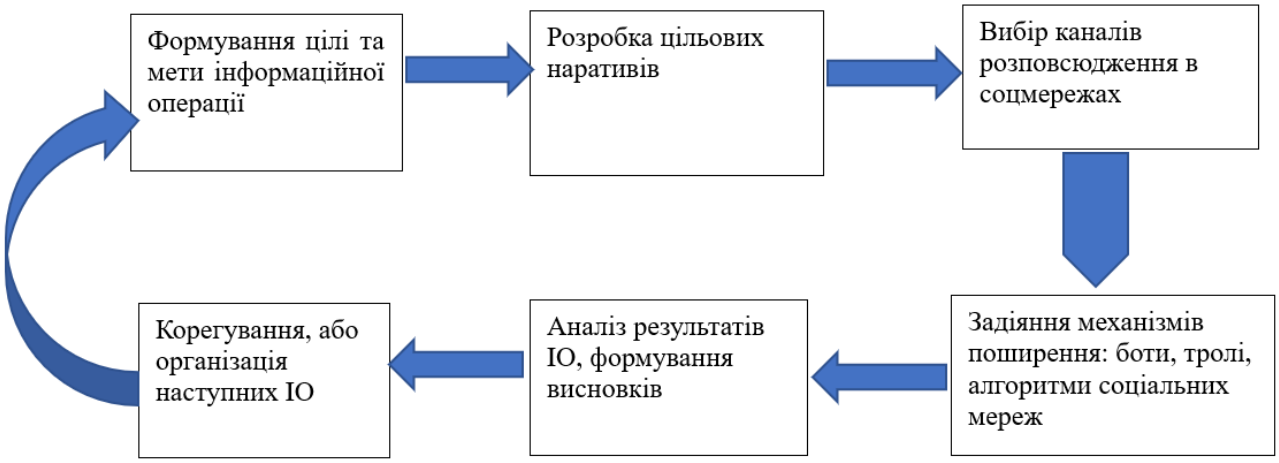

Рисунок 1.1 – Структурно-функціональна схема організації інформаційних операції проти України

На схемі графічно зображено цикл здійснення інформаційних операцій, що включає виявлення та формування відповідними структурами цілі та мети інформаційної операції, а також вибір цільових аудиторій, вплив на які ймовірно сприятиме досягненню обраної мети. Відповідно до поставленої мети формуються спеціальні цільові наративи та готується перелік каналів для поширення цих наративів. Наступний етап – безпосереднє здійснення розповсюдження наративів із задіянням соціальних мереж (в тому числі із використанням бот-мереж). Останній етап передбачає аналіз результатів інформаційної операції та формування на основі висновків наступних пропозицій до подальших заходів.

1.2. Соціальні мережі як інструмент здійснення інформаційних операцій та інформаційно-комунікаційні процеси

Глобалізація інформаційних процесів, заснованих на цифрових технологіях, сприяє формуванню нових світоглядних установок, поведінкових моделей і форм соціальної взаємодії. Розширення доступу до інформації та зростання кількості інформаційних ресурсів сприяють інтелектуальному, культурному та технологічному розвитку суспільства,

проте одночасно породжують нові загрози для національної безпеки в інформаційній сфері.

Функціональні особливості соціальних медіа – мультимедійність, персоналізація, відсутність географічних і редакційних обмежень – значно посилюють їх впливовий потенціал. Алгоритми видачі контенту, з урахуванням індивідуальних характеристик користувачів, сприяють формуванню сегментованих інформаційних просторів, які можуть бути легко використані для цілеспрямованого впливу, зокрема під час проведення інформаційних операцій. Це робить соціальні мережі не лише інструментом комунікації, а й потужною платформою реалізації маніпулятивного впливу на суспільно-політичні процеси.

Перше звернення до соціальних структур як поняття соціальної філософії другої половини XIX ст. можна знайти в роботах Давида Емілья Дюркгейма [20], Георга Левіна [21] і Герберта Спенсера [22]. Дослідниками були сформульовані базові аспекти аналізу мережного суспільства.

Ключовими роботами в дослідженні природи соціальних мереж вважають праці Дж. Морено [23]. У дослідженнях провідних соціологів на основі експериментальних даних вперше побудовано просторові форми соціальних об’єктів. Теоретико-методологічні основи аналізу соціальних мереж, закладені дослідниками, стали базою для цілого напряму соціальної філософії, предметом вивчення якої є формування «мережі стосунків».

Сам термін «соціальна мережа» у 1954 р. запропонував англійський соціолог Джеймс Барнс у збірці робіт «Людські стосунки» [24]. Цим терміном він висловив думку про те, що суспільство – це складне переплетення особистісних соціокомунікаційних стосунків. Барнс досліджував взаємозв’язки між людьми (членами соціуму) за допомогою візуальних діаграм, в яких окремі особи зображались крапками, а зв’язки між ними – лініями.

Ще до створення глобальної мережі (Інтернет) соціолог Марк

Грановеттер [25] і математик Лінтон Фріман опублікували праці за цією тематикою [26]. М. Грановеттер визначив, що всередині соціальних мереж слабкі зв'язки (сусіди, знайомі, знайомі знайомих, формальні контакти на роботі) мають більше значення, ніж сильні (родичі, друзі). Таке явище пояснюється тим, що інформація швидше і ширше розповсюджується саме через «слабкі зв'язки». Більш сильну теоретичну аргументацію на користь тези про силу слабких зв'язків запропонував Рональд Берт у своїй теорії «структурних дір» [27].

Наприкінці XX – початку XXI ст. виникають перші так звані «віртуальні соціальні мережі»: у 1995 р. – Classmates.com, у 1997 р. – SixDegrees.com, з 2001 р. з'являються сайти, у яких використовувалася технологія «коло друзів». Одним з них була спільнота Friendster, яка набула популярності в 2002 р. Станом на 2025 рік у світі функціонує близько 78 соціальних мереж, які відрізняються за структурою, видами комунікацій і типами контенту. Соціальні платформи виступають не лише засобами комунікації, а й ефективними інструментами для реалізації інформаційних впливів, зокрема – інформаційних операцій. Згідно зі статистикою 63,9 % населення світу (понад 5 млрд осіб) є користувачами соціальних мереж. Середній користувач має близько 7 акаунтів і проводить у соціальних мережах приблизно 2 години 25 хвилин щодня.

З технологічної точки зору соціальна мережа – це інтерактивний, з великою кількістю користувачів, веб-сайт, контент якого наповнюється самими учасниками. Сайт є автоматизованим соціальним середовищем, яке дозволяє спілкуватися групі користувачів, об'єднаних загальним інтересом. Теоретично як соціальну мережу можна розглядати будь-яку онлайнову спільноту [28].

О. Онищенко, В. Горовий, В. Попик визначають соціальні мережі як «технологічні комплекси організації і управління обмінами електронною інформацією між суб'єктами соціальних відносин, призначені для

забезпечення горизонтального спілкування зацікавлених у ньому абонентів, об’єднаних спільними інтересами, інформаційними потребами і навичками спілкування» [29].

Основною рисою соціальної мережі є створення та використання користувачами публічного або напівпублічного профілю, зазначивши список тих, з ким хочуть налагодити зв’язок і переглядати й передавати свій список контактів і списки інших користувачів системи [30].

Соціальні мережі відрізняються за функціональним інтерфейсом, призначенням, характером цільової аудиторії та специфікою алгоритмів взаємодії. Кожна платформа регламентує свою діяльність власними нормативними правилами користування, дотримання яких є обов’язковою умовою участі в комунікаційному процесі для всіх зареєстрованих користувачів. Універсальної класифікації видів соціальних мереж на сьогодні не існує, у дослідженні [31] пропонується така класифікація:

1. «професійні» або «мережа професійних контактів» такі як LinkedIn, e-LearningPRO),
2. «традиційні» або «універсальні» такі як Facebook, MySpace, «ВКонтакте», «Одноклассники»),
3. «для авторських записів» або «мікроблоги» такі як X,
4. «за інтересами» або «тематичні», «академічні», «дослідницькі» наприклад, Academia.edu,
5. «освітні», наприклад, TheStudentRoom, TheMathForum.

Інші дослідження виділяють інформаційні (informative) та комунікативні (collaborative) соціальні мережі [32]:

- Інформаційні соціальні мережі орієнтовані на обмін знаннями та поширення інформації у цифровому середовищі. Їх функціонування базується на тематичних обговореннях і систематичному оновленні контенту, який, як правило, подається у хронологічному порядку. Користувачі таких мереж проявляють регулярну активність, переважно

звертаючись до інформаційних матеріалів, що мають для них практичну або когнітивну цінність. Незважаючи на наявність елементів дискусії та інтерактивної взаємодії, домінуючим мотивом участі у подібних мережах залишається отримання актуальної інформації та знань.

- Комунікативні соціальні мережі структуровані навколо персоналізованих профілів користувачів та інтегрованих інструментів, які забезпечують взаємодію та спілкування між учасниками. Саме цей тип соціальних платформ найчастіше асоціюється з класичною моделлю соціальної мережі, оскільки відображає структуру міжособистісних відносин і комунікативних зв’язків, що формуються у цифровому середовищі.

Хоча на сьогодні така класифікація в чистому вигляді не існує, майже кожна соціальна мережі комбінує в собі характеристики інших та є універсальною.

Однією з задач соціальних мереж є процес комунікації, при чому наразі вже не лише невербальної, оскільки типи соціальних мереж поповнилися як аудіо-, так і відео контентом. Отже, слід визначити, яким саме чином здійснюється комунікація, та хто є її основними суб’єктами [78, 79].

Д. Брас пропонує наступну класифікацію суб’єктів соціальних мереж та зв'язків між ними (див. Табл. 1.2 та Табл. 1.3) [33].

Таблиця 1.2

суб’єкти соціальних мереж	
зірка (Star)	суб’єкт в значній мірі центральний в соціальній мережі
зв'язковий (Liason)	суб’єкт, який має зв'язки з двома чи більше не пов’язаними між собою групами, при цьому не є членом жодної з них
міст (Bridge)	суб’єкт, який є членом двох і більше груп
хранитель воріт (Gatekeeper)	користувач, який є одноосібним посередником або контролює потік двох частин соціальної мережі

ізольований (Isolate)	суб’єкт, який не має або має відносно мало зв'язків з іншими суб’єктами

Також в роботах автора визначені типи зв’язків між суб’єктами (див. Табл. 1.3) [33].

Таблиця 1.3

Типи звязків між суб’єктами соціальної мережі

Властивості	Визначення
непряме посилання (indirect links)	Шлях від одного суб’єкта до іншого опосередкований одним або більше осіб
частота (frequency)	Кількість посилання на суб’єкта
стабільність (stability)	Поява посилання на суб’єкта з певною періодичністю
множинність (multiplexity)	Поява зв'язків між двома суб’єктами в двох і більше різних контекстах
сила (strength)	Кількість часу, емоційної близькості та взаємних послуг
напрямок (direction)	Частота звернення одного суб’єкта до іншого
симетрія (symmetry)	Частота обопільних звернень суб’єктів

Процес комунікації в соціальних мережах може здійснюватися між окремими користувачами – друзі, підписники, фоловери, як в односторонньому, так і в двосторонньому напрямку. Так, наприклад, соціальна мережа Instagram або X (Twitter) не передбачають обов’язкової двосторонньої комунікації, тобто, якщо один користувач стає підписником іншого алгоритм роботи мережі не передбачає обопільної дії. В свою чергу соціальна мережа Facebook, або російські мережі «ВКонтакте» та «Одноклассники» застосовують здебільшого алгоритм обопільної «дружби».

Інший вид комунікації – групова – здійснюється в межах створених груп – це віртуальні співтовариства, об'єднання певного числа користувачів на основі певних спільних інтересів. При цьому, кожна група керується одним або декількома адміністраторами, які, як правило, поширюють в ній

певний контент відповідної спрямованості конкретної групи. В даному випадку процес обміну інформацією скоріш за все буде представлений у вигляді відцентрованих променів, тобто від одного або декількох адміністраторів до певної кількості користувачів. Але надалі частина користувачів може активно вступати в так звані багатосторонні дискусії-обговорення (залучена одночасно велика кількість користувачів).

Найчастіше процес поширення контенту починається з надходження до «лідерів думок» певної інформації щодо тієї чи іншої події. Далі «лідер думки» інтерпретує її з урахуванням суб'єктивної оцінки, необхідної для інформаційного впливу, вкладаючи окрім перекручування фактів емоційну складову, та розміщує контент на власній сторінці, або представляє її у вигляді інформаційного повідомлення в групі [76]. Суб'єкти, які побачили дану інформацію, можуть виконати наступні дії:

- пасивно сприймають дану інформацію як фейк
- пасивно сприймають інформацію як достовірний факт
- висловлюють своє ставлення шляхом відмітки «лайк/дизлайк» (подобається / не подобається)
- перепощують (розміщують) контент на власній сторінці
- коментують контент, тим самим залучаються до активної багатосторонньої комунікації.

Будь-які із зазначених дій є свого роду комунікацією в мережі, тобто, якщо ми застосуємо теорію графів для візуалізації топології розповсюдження контенту, всі користувачі, навіть ті, які сприймають контент пасивно та не продовжують його розповсюдження, є вершинами такого графу.

Кількість суб'єктів, які потрапили під інформаційний вплив даного контенту, буде залежати від швидкості його поширення до моменту затухання чи втрати актуальності, що, в свою чергу, залежить від авторитетності групи чи лідера думки, на сторінках яких контент був

розміщений, від кількості учасників групи, від його правдоподібності і актуальності. Не менш важливим при цьому є і фактор «активності» учасників групи [34, 35].

Під «активністю» користувачів соціальних мереж слід розуміти співвідношення загального часу перебування конкретного користувача в режимі онлайн в соціальній мережі за добу, кількості розміщених ним за цей час інформаційних повідомлень, кількості коментарів та лайків під постами інших користувачів.

Коефіцієнт «активності» можна умовно записати формулою: $A_x = \frac{T}{S}$

де A_x - показник активності конкретного користувача,

T - загальний час перебування користувача в режимі онлайн за добу,

S - приблизна кількість активних дій в мережі за час перебування онлайн.

Виходячи з показника «активність» можемо класифікувати користувачів соціальних мереж на наступні групи:

- активні користувачі, коефіцієнт «активності» яких більше показника загального часу перебування в режимі онлайн;
- малоактивні користувачі, коефіцієнт «активності» яких дорівнює показнику загального часу перебування в режимі онлайн;
- пасивні користувачі, коефіцієнт активності яких менше показника загального часу перебування в режимі онлайн.

Одразу слід зазначити, що структурна та технологічна будова соціальної мережі буде відігравати значну роль у проведенні інформаційної операції, а отже показники відповідно в кожній окремо визначеній соціальній мережі можуть відрізнятися [36, 37].

В 2010-х роках отримані фундаментальні експериментальні результати щодо поширення деструктивного контенту та інформаційних операцій у соціальних мережах [38, 39, 58, 74]. Серед них такі.

1. Дослідження результатів застосування ботів у Twitter під час президентської виборчої кампанії у Франції 2017 року виявили, що автоматизовані акаунти впливали на ключові етапи суспільного обговорення та потенційно сприяли поширенню дезінформації.

2. Показано, що боти в Twitter брали участь у дискусіях щодо виборів у США 2016 року, та демонстровано значний масштаб їхнього впливу.

3. Досліджено вплив фейкових новин у соціальних мережах під час виборчої кампанії у США 2016 року, звернувши увагу на мережеву структуру поширення контенту та роль окремих впливових користувачів.

4. Дослідження фейків і дезінформації на основі великого обсягу даних із Twitter виявили, що фейкові новини поширюються швидше та охоплюють ширшу аудиторію, ніж правдива інформація.

5. Виявлена ключова роль лідерів думок та інфлюенсерів в розповсюдження контенту через соціальну мережу, що є важливим для аналізу інформаційних операцій.

6. Проаналізовано процес поширення протестних настроїв у соціальних мережах, зокрема виділено користувачів, які мають прихований вплив на великий масштаб мережі.

7. У контексті референдуму щодо Brexit продемонстровано, як боти у Twitter впливали на громадську думку, поширюючи повідомлення із визначеними хештегами та гаслами.

8. Висвітлено роль тролів та координованих груп користувачів, які поширюють дезінформацію. Підкреслено колективний характер таких інформаційних операцій.

Приклади таких втручань зафіксовано під час парламентських та президентських виборів в Україні у 2019. Так Міжнародний фонд виборчих систем (International Foundation for Electoral Systems) у своєму дослідженні [117] наводить приклад кластеризації та сегментації акаунтів-ботів в

соціальній мережі X (Twitter), які використовувалися РФ для проведення інформаційних операцій (рис. 1.2).

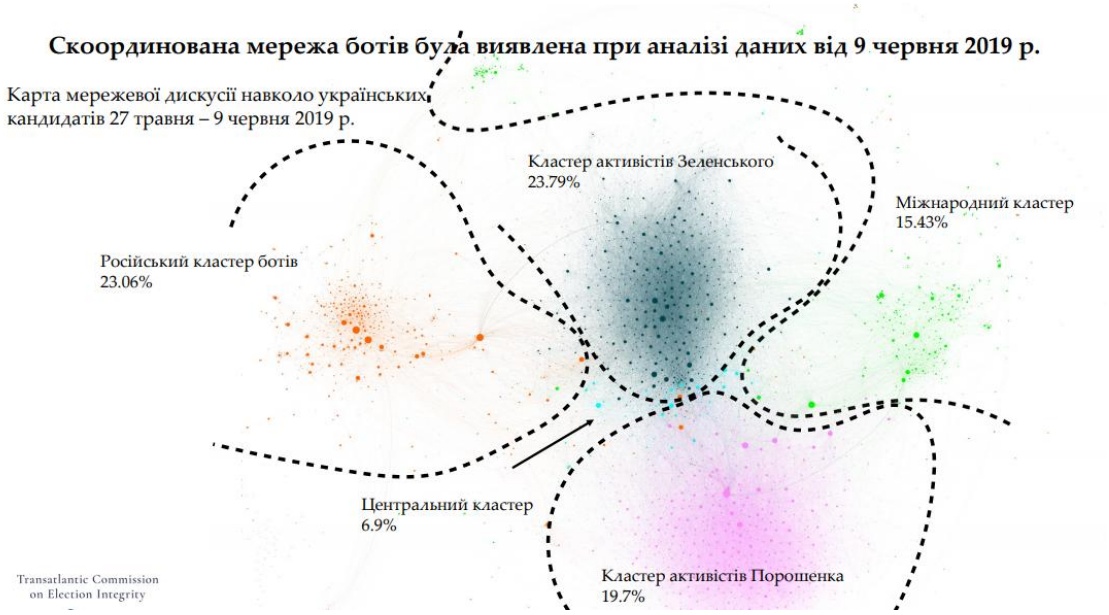

Рисунок 1.2 – Кластеризація та сегментація акаунтів-ботів в соціальній мережі X (Twitter)

На малюнку зображені кластери зафіксованих мереж ботів в соціальній мережі X, які були виявлені за відповідними наративами, що розповсюджувались.

Ще одним прикладом стала інформаційна операція з дискредитації дій влади в Україні під час заходів збереження енергоресурсів. Аналіз українського аналітичного центру «Громадянська мережа ОПОРА» [118] соціальної мережі X (Twitter) продемонстрував розповсюдження повідомлень із хештегом #LightOnZelenskyyOff, де зафіксовано мережу ботів (рис. 1.3).

В рамках дослідження було проаналізовано активність ботів через «твіт» та «ретвіт», що відбувалась в межах проросійської інформаційної кампанії, націленої на дискредитацію політики політичного керівництва країни.

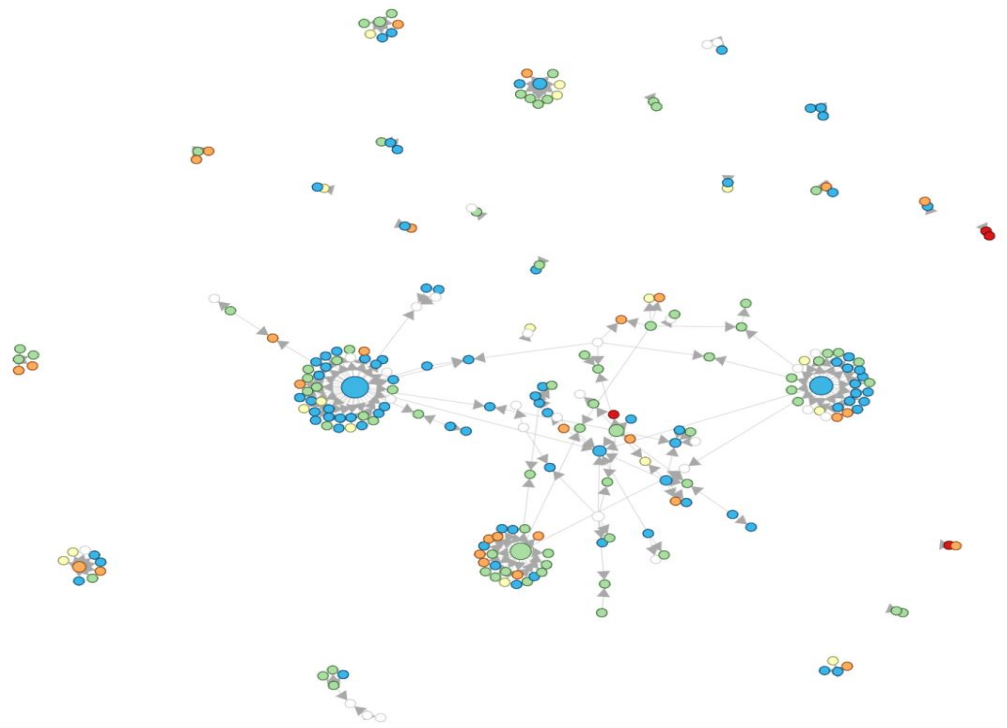

Рисунок 1.3 – Розповсюдження вірусного контенту акаунтами-ботів в соціальній мережі X з хештегом #LightOnZelenskyyOff

Таким чином, в умовах активного використання соціальних мереж як основного середовища для проведення інформаційних операцій постає необхідність у розробці таких моделей, які дозволили б адекватно відтворювати динаміку поширення інформаційного впливу, враховуючи нелінійний, стохастичний і децентралізований характер взаємодії користувачів. У той час, як більшість сучасних підходів орієнтовані на контент-аналіз у межах структурованих електронних ЗМІ, реальна інформаційна загроза в соціальних мережах формується шляхом складних взаємодій між різними типами агентів [71-73]. Тому наукова задача полягає у створенні імітаційної агентної моделі, яка дозволяє формалізувати процес розгортання інформаційної операції як поведінкову систему множини агентів, що взаємодіють у цифровому середовищі за визначеними правилами. Така модель має забезпечити дослідження та аналіз сценаріїв поширення контенту, виявлення аномальних інформаційних хвиль і раннє попередження інформаційних загроз у соціальних мережах, зокрема шляхом

аналізу ролей, взаємозв’язків, динаміки змін та інформаційної активності користувачів.

1.3. Аналіз підходів до моделювання та імітаційних моделей інформаційних операцій в соціальних мережах

Описані структурні та мережеві зв’язки, типи комунікації та алгоритми соціальних мереж демонструють, що аналітичним шляхом та шляхом експертної оцінки питання виявлення інформаційних операцій в соціальних мережах не вирішується.

Проаналізувати соціальну мережу та дослідити поширення контенту безпосередньо в соціальній мережі важке завдання, зв'язки між учасниками мережі носять випадковий характер, мережа постійно збільшується в розмірах через появу нових користувачів, що приєдналися до неї, непередбачуваним є факт зацікавленості учасників в поширенні інформації. Однак існує можливість досліджувати поширення інформації не в мережі, а в її моделі [34, 67-70].

Наразі існують чотири основні методологічні підходи щодо аналізу соціальних мереж.

Структурний підхід зосереджується на формальних характеристиках мережевих структур, зокрема на топології взаємозв’язків між акторами. Соціальна мережа в цьому випадку інтерпретується як граф, де вузли представляють акторів, а ребра – соціальні зв’язки. Вивчаються такі характеристики, як центральність, кластеризація, ступінь зв’язності, транзитивність, модульність та інші показники, що дозволяють аналізувати як індивідуальні позиції, так і глобальну конфігурацію мережі. Особливу увагу приділяють виявленню спільнот, тобто підгруп акторів, які інтенсивно взаємодіють між собою. Методологічно це пов’язано із задачами кластеризації, алгоритмами сегментації графів та вивченням еволюції мережевої структури в динаміці. Його застосування виправдане при

дослідженні статичних мереж, пошуку ключових вузлів (інфлюенсерів), визначенні ступеня згуртованості спільнот і рівня ієрархії у мережі. Обмеження такого підходу – недостатньо враховує часову динаміку і зміни зв'язків, а також контекст (контент або мотивації акторів) [40].

Динамічний підхід На відміну від статичних методів, динамічний підхід зосереджений на змінах у структурі соціальної мережі з плином часу. Центральним є аналіз виникнення та зникнення зв'язків, появи або відходу акторів, зміни взаємодій та їх стабільності. Такий підхід дозволяє моделювати закономірності розвитку спільнот, прогнозувати майбутні зв'язки та оцінювати ймовірність трансформацій мережі під впливом зовнішніх або внутрішніх факторів. Застосовуються моделі часових графів, предикативна аналітика, машинне навчання, структурні та реляційні моделі [41].

Нормативний підхід орієнтований на вивчення соціальних норм, ролей та довіри, що опосередковують поведінку учасників у мережі. Соціальна взаємодія розглядається не лише як обмін інформацією, а й як результат нормативних очікувань, правил, санкцій і культурних контекстів. Аналіз включає вивчення ролей (керівник–підлеглий, експерт–споживач), впливових вузлів (інфлюенсерів) і посередників (інформаційних брокерів), а також моделювання процесів поширення впливу. Часто застосовуються соціометричні методи, теорія соціального капіталу, а також алгоритми ідентифікації ключових агентів, зокрема методи мурашиної оптимізації. Однак, такий підхід потребує великих обсягів якісних даних (контент-аналіз, опитування), що ускладнює масштабні обчислювальні завдання [42].

У **ресурсному підході** акценти робляться на потенціалі акторів до мобілізації ресурсів – як індивідуальних (знання, престиж, статус), так і мережевих (вплив, доступ до інформації, стратегічні позиції). Соціальна мережа розглядається як система обміну ресурсами, де структурна позиція актора визначає його можливості. Основною категорією аналізу виступає

«структурна сила позиції», яка дозволяє прогнозувати доступ до стратегічної інформації або можливість здійснення впливу. Також проводиться змістовий аналіз контенту мережі: текстового, мультимедійного, потокового. Використовуються методи обробки природної мови, аналіз тегів, алгоритми ранжування (PageRank), інтеграція сенсорних даних та мультимодальні аналітичні моделі. Такий підхід дозволяє оцінити не лише структуру, але і змістову вагу зв'язків та комунікацій [43].

Кожен із зазначених підходів аналізу соціальних мереж може лежати в основі моделювання процесів розповсюдження контенту в соціальних мережах, а отже виявлення інформаційних операцій. Найбільш ефективними визнають гібридні підходи, де структурний аналіз поєднується з динамічним і контентним. Динамічний та ресурсний підходи отримують найбільший розвиток через важливість прогнозування та аналізу контенту (особливо під час інформаційних атак). У сфері інформаційних операцій нормативний підхід цінується за можливість аналізувати не лише структуру, а й мотивації та культурні особливості спільнот. Поєднати всі чотири підходи можна в концептуальну рамку: «структура → динаміка → норми → ресурси/вплив» (Таблиця 1.4).

Таблиця 1.4

Застосування підходів до аналізу соціальних мереж при виявлення інформаційних операцій

Підхід	Сила	Слабкість	Використання для виявлення інформаційних операцій
Структурний	Формальна мережева діагностика; масштабованість	Не ловить швидкі зміни	Виявлення бот-кластерів, хабів розповсюдження.
Динамічний	Моделює ескалацію/дифузію	Високі вимоги до даних	Виявлення фаз кампаній, прогноз поширення.
Нормативний	Пояснює сприйнятливість аудиторій	Суб'єктивні метрики	Оцінка легітимності джерел, вразливість до фейків.

Ресурсний	Ідентифікує стратегічні вузли впливу	Латентність ресурсів, неповні мережі	Виявлення цільових аудиторій (таргетування) та нейтралізація ключових розповсюджувачів.

Слід зазначити, що спроби моделювання соціальних мереж та їх внутрішніх процесів, зокрема інформаційних операцій, робилися давно, але вони гальмувалися обчислювальними труднощами, особливо в разі необхідності опису динаміки систем із зворотними зв'язками. На сьогодні є потужні технологічні спроможності для ефективної обробки даних, і це дозволяє як здійснювати підготовку сетів вхідних параметрів (наприклад, результатів статистичних досліджень), так і вирішувати формалізовані завдання з достатнім ступенем точності [44-46].

Імітаційне моделювання виступає ефективною альтернативою аналітичним моделям, особливо у випадках дослідження складних соціальних процесів. У контексті моделювання соціальних явищ – зокрема, інформаційних операцій – імітаційне моделювання дозволяє проводити обчислювальні експерименти у випадках, коли натурні експерименти є обмеженими, складними або етично неприйнятними [59-64].

Для моделювання інформаційних операцій в соціальних мережах можна використовувати різні імітаційні моделі.

- моделі з порогами;
- моделі незалежних каскадів;
- «теоретико-ігрові» моделі;
- моделі «дифузії інновацій»;
- моделі просочування і зараження;
- моделі Ізінга;
- моделі на основі клітинних автоматів;
- моделі на основі ланцюгів Маркова;
- агентне моделювання.

Розглянемо деякі з них.

Моделі з порогами, в тому числі з лінійними (Linear Threshold Model). Агент – вузол соціальної мережі (вершина графа) – може перебувати в активному та неактивному станах, причому можливий перехід тільки з неактивного стану в активний (зворотний перехід не допускається). Якщо в моделі агент зазнає впливу кожного свого сусіда в мережі, то стає активним в залежності від обраного ним порога. А в іншому випадку обирається випадково відповідно до деякого імовірнісного розподілу. В загальному індивідуальні відмінності обумовлюються досвідом агенту, його переконаністю, особистісними рисами, впливом засобів інформації, витратами [47].

Моделі незалежних каскадів (Independent Cascade Model) належать до моделей так званих систем частинок, що взаємодіють (Interacting Particles Systems). Вузол мережі (агент) визначається аналогічно з моделлю з порогами. Коли агент *i* стає активним в певний момент часу *t*, він отримує шанс активувати на наступному (і тільки на наступному) кроці кожного зі своїх сусідів j з імовірністю Pji (причому j можуть намагатися незалежно активувати і інших агентів) [48].

«Теоретико-ігрові» моделі, в яких акцент робиться на інформованість і взаємозв'язок між гравцями (агентами). Виграш, що отримується агентом (гравцем), залежить від дій опонентів (інших гравців). Агент діє так, щоб максимізувати свою вигоду. До теоретико-ігрових моделей відносять: 1) моделі взаємної інформованості; 2) моделі узгоджених колективних дій (суспільних благ); 3) моделі комунікацій і завдання пошуку мінімально достатньої мережі; 4) моделі стабільності мережі; 5) моделі інформаційного впливу та управління; 6) моделі інформаційного протиборства [49].

Моделі «дифузії інновацій». Динаміка процесу поширення традиційно моделюється логістичною кривою (^ -образною), що по суті є характеристикою будь-якого інфекційного процесу або процесу навчання з

наступними стадіями: новатори (innovators) – початківці, які першими сприймають та використовують нововведення; ранні послідовники (early adopters) – початківці, які починають сприймати та використовувати нововведення незабаром після його появи; рання більшість (early majority) – сегмент, який сприймає нововведення після новаторів і ранніх послідовників, але раніше більшості інших агентів; пізня більшість (late majority) – сегмент, що сприймає нововведення після широкого розповсюдження даного вірусу; і пізні послідовники (late adopters), які сприймають нововведення останніми [50].

Процес поширення нововведень, як і багато інших процесів в природі і суспільстві, має межі можливих змін, які в першу чергу обумовлені обмеженістю ресурсів. S'-образна функція містить три фази розвитку: формування бази розвитку, різке зростання та насичення. Швидкість процесів дифузії напряму залежить від міжособистісного спілкування між прихильниками інновації та тими, хто ще вагається або нічого не чув про нововведення.

Моделі просочування і зараження. Моделі просочування (percolation) і зараження (contagion) являють собою популярний спосіб вивчення поширення інформації та використовуються від моделей епідемій до дослідження нафтових родовищ. Класична модель поширення епідемії являє собою такий цикл захворювання носія: агент сприйнятливий до захворювання (susceptible); агент, який входить в контакт з інфікованим та заражається (infected & infectious) з деякою вірогідністю; агент, який через деякий період часу стає здоровим, набуваючи імунітет або вмирає (recovered / removed); імунітет з часом знижується, і агент знову стає сприйнятливим до хвороби (susceptible) [51].

Існують і інші аналогічні більш складні моделі, зокрема, в моделі SIRS агент, який одужав стає сприйнятливим до хвороби через деякий час. Найпростіший приклад ситуації, де така модель є природною є

захворювання на грип. Інший приклад – поширення інформації в соціальний мережі.

Для соціальних мереж ключовим показником є «епідемічний поріг» – критична ймовірність зараження сусіда, при перевищенні якої «інфекція» поширюється по всій мережі. Епідемічний поріг залежить від властивостей графа соціальної мережі: числа вершин, розподілу зв'язків, коефіцієнта кластеризації. Тому поширення інфекції сильно залежить від обраної моделі представлення графа мережі [66].

Модель Ізінга. Модель Ізінга – математична модель, що описує виникнення намагнічування матеріалу. Передбачається, що конформність або незалежність у великій соціальній групі може моделюватися за допомогою моделі Ізінга; вплив найближчих сусідів є визначальним, а аналогом температури є готовність групи мислити творчо, готовність прийняти нові ідеї. Зовнішнім полем для соціальної групи є вплив «авторитету» або управління [52].

Моделі на основі клітинних автоматів. Для опису процесів поширення інформації в соціальній мережі цю модель можна розглядати як складну адаптивну систему, яка складається з великої кількості агентів, взаємодія між якими призводить до масштабної, колективної поведінки, яку важко передбачити і аналізувати. Для моделювання та аналізу таких складних систем іноді використовуються клітинні автомати. Клітинний автомат складається з набору об'єктів (в даному випадку агентів), які зазвичай утворюють регулярну решітку. Стан окремо взятого агента в будь-який дискретний момент часу характеризується деякою зміною. Стани синхронно змінюються через дискретні інтервали часу відповідно до незмінних локальних вірогідних правил, які можуть залежати від станів найближчих сусідніх агентів в оточенні даного агента, а також, можливо, від стану самого агента [53].

Ланцюги Маркова. В даній моделі вивчається вплив в команді (групі агентів). Запропонована модель є динамічною Баєсовою мережею (Dynamic Bayesian Network – DBN) з дворівневою структурою: рівнем індивідів (моделюються дії кожного агента) і рівнем групи (моделюються дії групи в цілому).

У більшості моделей в основному розглядаються правила взаємодії агентів, але що стосується самої мережі впливу в цілому, її властивостей, взаємозв'язків і процесів взаємодії, то наявний аналіз цих моделей надає дуже небагато результатів [54].

Агентне моделювання. Агентне моделювання – відносно новий напрямок в імітаційному моделюванні, що використовується для дослідження децентралізованих систем, динаміка функціонування яких визначається не глобальними правилами і законами (як в інших парадигмах імітаційного моделювання), а навпаки, коли ці глобальні правила і закони є результатом індивідуальної активності членів групи [55].

Агентна модель являє реальний світ у вигляді багатьох активних підсистем, які окремо специфікуються, та називаються агентами (автономні об'єкти, що цілеспрямовано функціонують в конкретному середовищі за певним набором правил, взаємодіють один з одним і адаптуються в процесі функціонування). Зазвичай в таких системах не існує глобального централізованого управління, агенти функціонують за своїми законами асинхронно.

Поведінка агентів регулюється їх власною схемою, тобто когнітивною структурою, яка визначає, яку дію агент робить в момент часу t з урахуванням його сприйняття навколишнього середовища. Існує безліч визначень поняття агента. Спільним у всіх визначеннях цього поняття є те, що агент – це деяка сутність, що володіє активністю, автономною поведінкою, яка може приймати рішення відповідно до деякого набору правил, взаємодіяти з оточенням та іншими агентами, а також може

самостійно змінюватися (еволюціонувати). Ґрунтуючись на простих правилах поведінки і взаємодії агентів, природні системи явно виявляють груповий інтелект [65, 80].

Для аналізу зазначених моделей наведено порівняння характеристик в табл.1.5. У таблиці вказані ключові аспекти кожної моделі, включно із застосовністю до моделювання інформаційних операцій.

Таблиця 1.5

Ключові аспекти моделей (порівняльна характеристика)

Модель	Основні характеристики	Застосовність до моделювання інформаційних операцій
Моделі з порогами	Базуються на порозі, який визначає, коли агент прийме рішення, ґрунтуючись на поведінці сусідів.	Ефективні для моделювання ухвалення рішень у соціальних мережах, але обмежені при аналізі складних взаємодій.
Моделі незалежних каскадів	Базуються на ймовірності того, що інформація передається від активованого агента до сусідів.	Підходять для моделювання поширення інформації, особливо вірусного характеру.
Теоретико-ігрові моделі	Використовують концепції теорії ігор для моделювання взаємодій агентів, враховуючи їхню раціональну поведінку.	Корисні для аналізу стратегічної поведінки учасників, але можуть бути складними в реалізації.
Моделі дифузії інновацій	Описують процес поширення нововведень серед агентів, заснований на соціальних впливах і контактних мережах.	Добре підходять для моделювання поширення інформації, але обмежені інноваційними контекстами.

Моделі просочування і зараження	Імітують процес поширення інформації через мережі, аналогічно поширенню вірусу.	Ефективні для моделювання вірусного поширення інформації, але можуть не враховувати соціальний контекст.
Моделі Ізінга	Базуються на фізичній моделі магнетизму, що застосовується для моделювання групової поляризації та думок.	Корисні для моделювання поляризації думок, але менш підходять для моделювання динаміки думок у реальному часі.
Моделі на основі клітинних автоматів	Використовують дискретні моделі, у яких агенти змінюють свій стан на основі локальних правил.	Підходять для моделювання локальних взаємодій, але складні для опису складних мережевих структур.
Моделі на основі ланцюгів Маркова	Засновані на ймовірнісних переходах між станами агентів, що описують послідовність подій.	Підходять для моделювання ймовірнісних процесів, але можуть бути обмежені в передбаченні тривалих процесів.
Агентне моделювання	Імітує поведінку окремих агентів, враховуючи їхні взаємодії та адаптацію до змін у навколишньому середовищі.	Універсальний підхід, який може враховувати різні аспекти інформаційних операцій, включно із соціальними та когнітивними елементами.

Таким чином, найбільш підходящим підходом для моделювання інформаційних операцій у соціальних мережах є агентне моделювання. Цей підхід дає змогу моделювати складні та багатошарові взаємодії агентів (користувачів), враховуючи їхню поведінку, адаптацію до змін, соціальні впливи та поширення інформації. Агентне моделювання надає можливості для імітації як простих, так і складних сценаріїв інформаційних операцій, що робить його універсальним інструментом для таких завдань.

Також, можна стверджувати, що з усіх зазначених моделей агентна модель дозволяє задіяти всі чотири методологічні підходи до аналізу соціальних мереж, взявши до уваги як саму структуру динамічної системи, так і окремих її акторів, визначивши їх взаємодію, певні правила гри, а також надавши їм певних характеристик.

Висновки до Розділу 1.

1. В результаті аналізу інформаційних операцій як загрози національній безпеці України та її складовій – інформаційній безпеці, зроблено висновки, що соціальні мережі набувають все більшого значення як платформи розповсюдження деструктивного контенту, а також набувають суб'єктності, що призводить до зміни балансу інформаційних відносин.
2. Проаналізовано відмінність інформаційної операції від психологічного впливу. Наведено структурно-функціональну схему інформаційних операцій, які здійснює рф проти України. На основі аналізу існуючих досліджень виділено 6 ключових елементів інформаційних операцій.
3. Аргументовано використання соціальних мереж як основного та ефективного середовища для здійснення інформаційних операцій. Проаналізовано типи соціальних мереж, визначено їхні функціональні особливості. Описано комунікаційні процеси, які здійснюються між користувачами. Проаналізовано експериментальні результати щодо поширення деструктивного контенту та здійснення інформаційних операцій у соціальних мережах, що дозволяє розглядати інформаційну операцію як поведінкову систему множини агентів, які взаємодіють у цифровому середовищі за визначеними правилами, що сприяло розробці методу та моделі на основі чотирьох типів агентів.

4. Проведено аналіз підходів до моделювання та імітаційні моделі, що застосовуються для моделювання інформаційних операцій. Здійснено порівняння ключових характеристик зазначених імітаційних моделей включно із застосовністю до моделювання інформаційних операцій в соціальних мережах. Наведено аргументи на користь агентного моделювання як найбільш підходящого, оскільки воно дає змогу моделювати складні та багатошарові взаємодії агентів (користувачів), враховуючи їхню поведінку, адаптацію до змін, соціальні впливи та поширення інформації.

РОЗДІЛ 2. МЕТОДИ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В СОЦІАЛЬНИХ МЕРЕЖАХ.

2.1. Парадигма агентного моделювання

Агентне моделювання – це метод імітаційного моделювання, який досліджує поведінку децентралізованих автономних агентів, їх взаємодію (як індивідуальних агентів, так і колективних, таких як організації або групи) і те, як така поведінка визначає поведінку всієї системи в цілому. Він поєднує в собі елементи теорії ігор, складних систем, емерджентність, обчислювальної соціології, багатоагентних систем, еволюційне програмування та використовується в не пов'язаних з обчисленнями наукових областях, включаючи біологію, екологію та соціальні науки [81].

Агентне моделювання застосовується для аналізу децентралізованих систем, які мають досить великі розміри, неоднорідні структури та динамічно змінюються: старі зв’язки відмирають, нові з’являються. Саме тому цей метод є ефективним для дослідження процесу розповсюдження інформаційного впливу в соціальних мережах.

Для створення агентної моделі всі актори розглядаються як окремі агенти. Відповідно до структурного підходу соціальну мережу можна розглядати як вершини з певними зв’язками між ними. Мережева структура моделі – динамічна, це свого роду система, що самозароджується, елементи якої з’являються та відмирають. У такій системі також визначаються правила поведінки кожного з агентів та їхні соціальні ролі. І нарешті, кожному з агентів надається певний пул персональних характеристик, що визначає ресурсний підхід [82-85].

Розглядаючи парадигми системного моделювання можливо зробити висновок що агентне моделювання є найбільш універсальним. На відміну від дискретно-подійного моделювання, яке відповідає низькому та середньому рівню абстракції, і підходу системної динаміки з високим рівнем абстракції, агентні моделі можуть бути як дуже деталізованими, коли агенти

представляють фізичні об'єкти, так і гранично абстрактними, коли за допомогою агентів моделюються конкуруючі компанії або уряди держав (рис. 2.1).

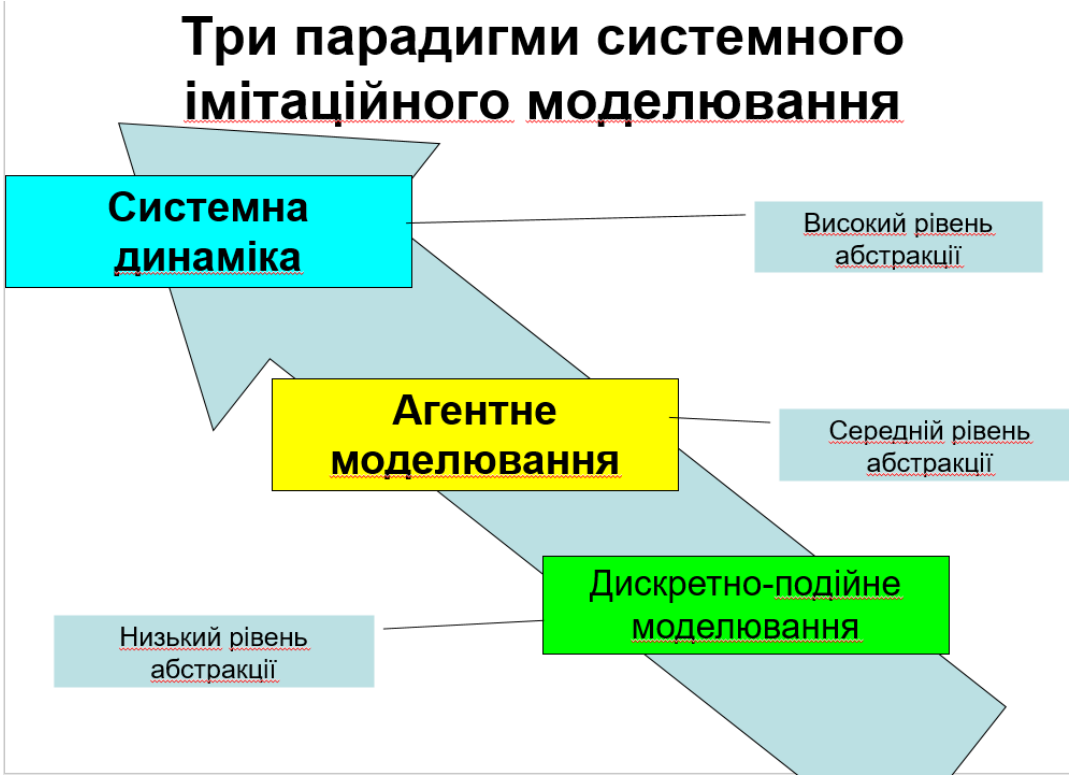

Рисунок 2.1 – Три основні парадигми системного імітаційного моделювання

Основною відмінністю агентного підходу від перших двох є побудова моделі за принципом знизу-вгору. Залежності між агрегованими величинами не задаються виходячи зі знань про реальний світ, а виходять в процесі моделювання індивідуальної поведінки десятків, сотень або тисяч агентів, їх взаємодії один з одним і з об'єктами, що моделюють навколишнє середовище.

До переваг агентного підходу слід віднести: відсутність визначеності в поведінці системи на глобальному рівні, що може привести до появи нових гіпотез про її функціонування в ході симуляції моделі; реалізм і гнучкість в описі системи, можливість моделювати найскладніші нелінійні зворотні зв'язки, використовувати будь-який необхідний рівень деталізації і

абстракції. В АМ відсутні обмеження на гетерогенність елементів моделі; з'являється можливість моделювання спілкування і обміну інформацією [85].

Агентне моделювання у цьому контексті виступає як ефективний інструмент багатоваріантного ситуаційного аналізу. Його сутність полягає у створенні штучного середовища, що складається з автономних агентів, кожен з яких наділений власною логікою поведінки, цілями, правилами взаємодії з іншими агентами та адаптивними механізмами. Це дозволяє досліджувати емерджентні ефекти, встановлювати нові закономірності, когнітивні зв’язки та моделі взаємовпливу. В результаті формуються комплексні математичні моделі сценарного типу, реалізовані у вигляді програмних моделюючих комплексів, що підтримують прогнозування та аналітичне оцінювання інформаційних процесів [86, 87].

В імітаційній агентній моделі її складові – агенти – функціонують незалежно один від одного та від системи загалом. Вони діють за своїми законами, на основі яких й формуються загальні правила функціонування системи загалом, тобто побудова моделі «від низу до верху».

Для створення агентної моделі поширення інформації, перш за все, необхідно сформувати близький до реальності віртуальний інформаційний простір, «населений» віртуальними агентами. При побудові агентної моделі однією з основних задач є визначення взаємодії агентів між собою, яким чином дані агенти формуються (виникають), що впливає на передачу інформації від одного агенту до іншого, якою може бути динаміка цієї передачі [64, 65].

Ключовою особливістю АМ є емерджентність, яка передбачає, по-перше, неможливість розділення мікро- та макрорівня аналізу, по-друге, неможливість зведення явищ макрорівня до сукупності явищ мікро-рівня [88, 89]. За Р. Москотіною: агентне моделювання є сенс застосовувати в соціологічному дослідженні тоді, коли потрібно надати теоретичне

пояснення соціальним явищам чи процесам [80]. В роботах В. Гужви обґрунтовуються можливості використання агентно-орієнтованого моделювання для побудови соціально-економічних процесів і систем використання [83].

Принципи АМ.

- Агенти: автономні сутності з атрибутами та поведінкою.
- Взаємодія: агенти взаємодіють один з одним і з навколишнім середовищем.
- Емерджентність: складна поведінка на рівні системи виникає з індивідуальних взаємодій.
- Адаптація: агенти можуть адаптуватися і змінювати свою поведінку залежно від місцевих умов.
- Моделювання: АМ передбачає запуск симуляцій для спостереження за динамікою системи.

Враховуючи ключові принципи АМ можемо визначати індивідуальну поведінку та взаємодію автономних агентів, кожен з яких має свої власні атрибути, поведінку та процеси прийняття рішень. У контексті соціальних мереж це означає наступне:

- гетерогенність користувачів: дозволяє враховувати різноманітну поведінку, вподобання та джерела інформації людей у соціальній мережі, визнає, що користувачі можуть мати різні мотивації для обміну або споживання інформації;
- поведінкова динаміка: АМ фіксує динаміку індивідуальних взаємодій, включаючи обмін інформацією, вподобання, коментування та стеження за іншими користувачами, враховує такі фактори, як тривалість уваги та вплив думок оточуючих;
- адаптивне прийняття рішень;
- топології мережі: АМ може моделювати різноманітні мережеві топології, включаючи безмасштабні, малі та кластерні структури, що

дозволяє вивчати, як мережеві структури впливають на розповсюдження інформації;

- гомофільність та вплив: АМ моделює концепцію гомофілії, коли індивіди зв'язуються з іншими людьми, які мають схожі характеристики, інтереси чи думки. АМ також враховує вплив, який добре пов'язані користувачі (інфлюенсери) здійснюють на поширення інформації;
- вірусне поширення: АМ може відтворювати вірусне поширення інформації через мережі, відстежуючи поширення контенту в міру того, як він потрапляє до різних спільнот користувачів.

АМ використовується для вивчення екологічних систем, включаючи динаміку хижак-жертва, ріст лісів і поширення хвороб серед видів. Ці моделі допомагають екологам зрозуміти, як індивідуальна поведінка впливає на динаміку екосистеми. В економіці АМ використовується для моделювання динаміки ринку, поведінки споживачів і фінансових систем, що дозволяє дослідникам вивчати виникнення економічних явищ та наслідки політичних втручань. Також АМ допомагає бізнесу та маркетологам оптимізувати свої стратегії охоплення цільових аудиторій та максимального поширення рекламного контенту. Агентні моделі відіграють важливу роль в епідеміології, особливо під час спалахів захворювань. Може використовуватись у розробці кампаній у сфері громадського здоров'я, вивчаючи, як інформація поширюється через соціальні мережі та впливає на поведінку, пов'язану зі здоров'ям. Завдяки АМ можливо спрогнозувати шляхи передачі хвороб, стратегії втручання та впливу політики громадського здоров'я [90-95].

АМ є цінним для вивчення таких соціальних явищ, як поведінка натовпу, формування громадської думки та поширення культурних особливостей. Воно допомагає зрозуміти, як індивідуальні взаємодії породжують суспільні моделі. АМ надає обґрунтування для вивчення сценаріїв та аналізу втручання в контексті поширення інформації в

соціальних мережах. Дослідники та політики можуть використовувати АМ для оцінки впливу політики, пов'язаної з обміном інформацією, модерацією контенту та боротьбою з дезінформацією.

2.2. Комплексний метод для забезпечення реалізації агентної моделі.

Під час використання агентного моделювання для виявлення інформаційних операцій у соціальних мережах можна застосувати різні методи, які забезпечують реалізацію цих моделей. Нижче наведено основні з них.

Метод на основі теорії ігор

- Метод «Наївного баєсівського гравця» використовується для моделювання поведінки агентів в умовах невизначеності, коли вони ухвалюють рішення на основі ймовірнісних оцінок.

Так, агент Ai оцінює ймовірність стану середовища S як $P\ (S|Oi)$, де Oi – спостереження. Рішення приймається згідно з: $\arg\max S \sum P(S|Oi) \times U(a,S)$

- Метод динамічних ігор дає змогу моделювати стратегії агентів, які взаємодіють із плином часу, беручи до уваги як минулу, так і майбутню поведінку інших агентів.

Формалізуються як послідовність стратегічних взаємодій $G = (N, Ai, T, Ui(t))$

де агенти оптимізують стратегію з урахуванням змін у середовищі

- N – множина агентів (наприклад, $i \in Ni$ – конкретний агент);
- Ai – множина допустимих дій агента і (наприклад: постинг, репостинг, коментування, зміна теми, зміна тону);
- T – дискретний або безперервний часовий інтервал моделювання;
- $Ui(t)$ – функція корисності агента *i* в момент часу *t*, яка залежить як від поточних, так і від попередніх станів мережі та інших агентів.

Методи поширення впливу

- Метод поширення (максимізації) впливу (Influence Maximization) застосовується для визначення ключових агентів, які можуть максимізувати поширення інформації в мережі.

Для заданої мережі $G = (V, E)$ знаходять підмножину $S \subseteq V$, що максимізує охоплення: $\max\_\{|S| \leq k\}\, \sigma(S)$, де σ(S) – очікувана кількість активованих вузлів.

- Метод відсікання та обрізки (Cutoff and Pruning) використовується для скорочення розміру мережі, зберігаючи при цьому найбільш значущі зв'язки для поширення інформації. Видаляються вузли та ребра з низьким коефіцієнтом центральності, зберігаючи функціональне ядро мережі.

Методи машинного навчання

- Методи класифікації (наприклад, SVM, Decision Trees) застосовуються для класифікації агентів за групами залежно від їхньої поведінки або сприйняття інформації.

SVM або Decision Tree – модель $f: X \to Y$

де X – ознаки агента, Y – мітка класу (інфлюенсер, ретранслятор тощо).

- Методи кластеризації (наприклад, K-Means, DBSCAN) використовуються для виявлення спільнот або груп агентів зі схожими характеристиками.

K-Means або DBSCAN – розбиття простору на кластери $C = \{C_1, C_2, \ldots, C_k\}$ на основі евклідових відстаней.

Еволюційні методи

- Генетичні методи застосовуються для оптимізації стратегій агентів, даючи їм змогу «еволюціонувати» та адаптуватися до змін в інформаційному середовищі.

Стратегії кодуються як хромосоми, над якими виконуються відбір, кросовер, мутація. Оптимізація функції U_i = f(strategy_i, network_context).

- Метод диференціальної еволюції використовується для пошуку оптимальних параметрів моделі, враховуючи адаптивні здібності агентів.

Пошук оптимальних параметрів: $x\_\{i\}\^\{t + 1\} = x\_r\^1 + F \cdot (x\_r\^2 - x\_r\^3)$.

Методи мережевого аналізу

- Метод пошуку шляхів (наприклад, Dijkstra (Де́йкстра) Алгоритм): використовуються для визначення найкоротших шляхів поширення інформації через мережу.

Визначення найкоротших шляхів: $d(u, v) = min \sum\_\{e \in path(u, v)\} w(e)$,

де

- *path(u,v)* — усі можливі шляхи між вузлами *u* і *v*,
- *w(e)* — вага ребра *e*, яка може означати «вартість поширення інформації».

- Метод виявлення спільнот (наприклад, Girvan-Newman, Louvain) дають змогу ідентифікувати групи агентів, які активно взаємодіють один з одним, що важливо для моделювання кластерів інформації. Виділення спільнот шляхом максимізації модульності Q.

Методи прийняття рішень

- Метод Монте-Карло (MCMC) використовується для моделювання ухвалення рішень агентами, що ґрунтуються на ймовірнісних оцінках майбутніх станів.

$$arg\ max_2 \sum_{s\prime \in S} P\ (s'|s, a)\ \times\ U\ (a, s')$$

де

- S – простір станів середовища

- Ai – агент
- $a \in A$ – дія агента
- $U(a, s)$ – функція корисності (utility) дії a в стані s
- $P(s'|s, a)$ – ймовірність переходу в стан s' після дії a зі стану s

- Метод рендерингу рішень на основі корисності застосовуються для моделювання раціональних агентів, які приймають рішення, максимізуючи свою корисність.

Методи обробки великих даних

- MapReduce застосовується для опрацювання та аналізу великих обсягів даних про соціальні мережі, даючи змогу масштабувати моделювання на великі мережі.

- Метод розподіленого обчислення використовуються для паралельного опрацювання даних і виконання моделювання на кількох вузлах.

Методи динамічного моделювання

- Метод зворотного зв'язку (Feedback Loops) використовуються для моделювання динамічних процесів у соціальних мережах, таких як зворотні зв'язки в поширенні інформації.

Циклічні зміни в графі станів: $s\_\{\mathrm{t}+1\}=\mathrm{f}(s\_t, I\_t)$

де:

- St – поточний стан агента чи мережі на момент часу t,
- It – інформаційний вплив (вхідний контент, сигнали, реакції),
- f – функція переходу до нового стану, яка враховує попередній стан та вплив.

- Метод скінченних автоматів: застосовується для моделювання станів агентів та їхніх переходів між цими станами.

Агенти переходять між станами згідно з правилами $\delta(s, a) \rightarrow s'$, де

- S – множини можливих станів агента (наприклад: «пасивний», «активний», «ретранслює інформацію», «видаляє допис»).

- A – множини дій або вхідних подій, які можуть спровокувати зміну стану.
- $\delta(s, a) \rightarrow s'$ – функція переходу, яка визначає, що при виконанні дії a з поточного стану s агент переходить у новий стан s'.

Кожен із цих методів може бути адаптований і використаний залежно від специфіки завдань, пов'язаних із моделюванням інформаційних операцій у соціальних мережах. Їх вибір і комбінація залежать від особливостей моделі та цілей дослідження.

Для агентного моделювання інформаційних операцій у соціальних мережах можна створити комбінацію методів, яка дасть змогу моделювати складні соціальні процеси, розповсюдження інформації та взаємодію агентів. Так, можемо розглядати наступні комбінації методів, які поєднують в собі різні аспекти агентної поведінки та динаміки соціальних мереж:

1) Метод поширення впливу + Метод ухвалення рішень

- Метод поширення впливу (Influence Maximization): цей метод застосовується для визначення ключових агентів (інфлюенсерів) у соціальній мережі, які здатні максимізувати поширення інформації. За допомогою цього алгоритму ідентифікуються вузли, які можуть ефективно впливати на більшу частину мережі.

- Метод Монте-Карло (MCMC). Після визначення інфлюенсерів раціонально застосовувати метод Монте-Карло для моделювання рішень агентів, ухвалених на основі ймовірнісних оцінок. Це дасть змогу оцінити, як інформація поширюватиметься через мережу з урахуванням непередбачуваності поведінки окремих агентів.

2) Еволюційні методи + Методи мережевого аналізу

- Генетичні методи: застосування цього методу підходить для оптимізації стратегій агентів, які беруть участь в інформаційних операціях. Він дасть змогу агентам адаптуватися та покращувати свої стратегії з плином часу, що особливо важливо для динамічних соціальних мереж.

- Метод виявлення спільнот (Louvain) для виявлення спільнот всередині соціальної мережі допоможе краще зрозуміти, як інформація поширюється в рамках кластерів і як ефективно націлюватися на ключові групи агентів.

3) Методи кластеризації + Методи динамічного моделювання

- Кластеризація методом K-Means застосовується для сегментації множини агентів на групи зі схожими характеристиками або поведінкою. Цей метод корисний для розуміння того, як різні типи агентів можуть реагувати на інформаційні операції.

- Метод зворотного зв'язку (Feedback Loops) слід використати для моделювання динамічних процесів у мережі, таких як зміна думок або адаптація агентів у відповідь на зміни в інформаційному середовищі. Цей метод дає змогу враховувати, як минула інформація впливає на майбутню поведінку агентів.

Ця комбінація методів забезпечує різнопланові підхід до агентного моделювання, враховуючи як стратегічну поведінку агентів, так і динамічну взаємодію в соціальних мережах. Вона дає змогу моделювати складні сценарії, як-от поширення дезінформації, вплив лідерів думок, динаміка зміни думок у мережі та адаптація агентів у реальному часі.

Для побудови агентної моделі, спрямованої на виявлення інформаційних операцій у соціальних мережах, запропоновано також поєднання одразу п’яти методів у визначеній послідовності з урахуванням їхньої інтеграції в загальну агентну модель. Кожен метод відповідатиме за певний аспект моделювання, і разом вони забезпечать всебічний і комплексний аналіз інформаційних операцій у соціальних мережах.

Запропонований метод реалізується як послідовний алгоритм, що охоплює весь цикл моделювання інформаційної операції – від ідентифікації впливових користувачів до симуляції динаміки поширення дезінформації з

урахуванням змін у поведінці агентів. Метод реалізується у п’ятьох ключових етапах:

1. Виявлення ключових агентів поширення інформації

Застосовується для визначення ключових агентів (інфлюенсерів) у соціальній мережі, здатних максимізувати поширення інформації.

Оскільки інформаційні операції часто залежать від ключових фігур, які можуть значно вплинути на всю мережу. Цей метод дає змогу визначити, які агенти можуть максимально ефективно поширювати інформацію.

Роль – визначення вузлів. На першому етапі модель визначає ключові вузли в соціальній мережі, які мають найбільший потенціал для поширення інформації. Ці вузли будуть пріоритетними агентами, через яких розпочнеться інформаційна операція.

Використаний метод: Influence Maximization.

2. Моделювання ймовірнісної реакції користувачів на контент

Застосовується для моделювання ухвалення рішень агентами, що ґрунтуються на ймовірнісних оцінках і впливі оточуючих.

У реальних соціальних мережах поведінка агентів часто невизначена і може залежати від безлічі факторів. Це дає змогу змоделювати цю невизначеність і оцінити, як інформація поширюватиметься за різних сценаріїв.

Після того як ключові вузли визначено, здійснюється моделювання ймовірнісні рішення агентів у мережі. Це дає змогу оцінити, як інформація поширюватиметься, враховуючи випадкові фактори та невизначеність у поведінці агентів.

Використаний метод: Монте-Карло (MCMC).

3. Адаптація стратегій поширення

Застосовується для покращення стратегій агентів у процесі інформаційних операцій.

Інформаційні операції динамічні, і агенти повинні адаптуватися до змін у мережі. Використаний метод: Генетичні алгоритми, які дають змогу агентам «еволюціонувати», покращуючи свої стратегії та адаптуючись до нових умов.

На цьому етапі модель використовує генетичні алгоритми для поліпшення стратегій агентів. Це може включати адаптацію до змін у мережі або розробку нових методів поширення інформації на основі реакції агентів.

4. Врахування структури соціальної мережі

Застосовується для ідентифікації спільнот і кластерів усередині соціальної мережі для більш точного моделювання поширення інформації.

Інформація в соціальних мережах часто поширюється через кластери або спільноти. Використаний метод: Louvain Clustering допомагає виявити ці кластери, що дає змогу моделювати поширення інформації з урахуванням структури мережі.

Цей метод допомагає ідентифікувати кластери та спільноти всередині мережі. Ці кластери можуть відігравати роль бар’єрів або каталізаторів поширення інформації. Модель враховуватиме структуру мережі та орієнтуватиметься на взаємодію між спільнотами.

5. Динамічне оновлення станів агентів

Застосовується для моделювання динамічних змін у поведінці агентів і поширенні інформації.

Інформаційні операції мають циклічний характер, де кожне нове повідомлення або дія може впливати на подальшу поведінку агентів. Зворотні зв'язки дають змогу враховувати ці зміни, роблячи модель реалістичнішою.

Зворотний зв'язок дає змогу моделі враховувати динамічні зміни, як-от зміна думок агентів або адаптація їхньої поведінки у відповідь на отриману інформацію. Цей компонент робить модель реалістичнішою і дає

змогу симулювати ефекти, які проявляються з плином часу. Використаний метод: Feedback Loops.

Математичний опис методу.

Розглянемо соціальну мережу як неорієнтований граф: $G = (V, E)$, де $V = \{v_1, v_2, \ldots, v_n\}$ – множина агентів (вузлів), $E \subseteq V \times V$ – множина зв'язків між ними. Знайдемо підмножину $S \subseteq V$ таких агентів, які забезпечують максимальне охоплення мережі в результаті поширення інформації:

$$S^* = arg_{\max} \{S \subseteq V, |S| \leq k\} \sigma(S)$$

де $\sigma(S)$ – функція охоплення (кількість активованих вузлів від множини S.

Моделювання ймовірнісної реакції: кожен агент v_i в момент часу t має стан $s_i(t) \in \{0, 1\}$, де 1 означає, що агент є учасником інформаційної операції в момент часу t, а 0 – ні. Ймовірність активації агента визначається за формулою:

$$P(s_i(T+1) = 1) = f(\sum w_{ji} \times s_j(t)), j \in N(i),$$

де f(x) – функція активації (сигмоїда або порогова функція), N(i) – множина сусідів агента i, w_{ji} – вага впливу агента j на агента i. Моделювання Монте-Карло дозволяє симулювати випадкові траєкторії поширення та оцінювати середні сценарії.

Генетичні алгоритми використовуються для адаптації стратегії агента. Кожен агент має стратегію θ_i, що впливає на здатність активувати інших з метою максимізації функції виграшу:

$$F_i(\theta_i) = \sigma_i(T) - C_i(\theta_i),$$

де $\sigma_i(T)$ – кількість успішно активованих агентів до моменту часу T, C_i – вартість інформаційної стратегії.

Виявлення спільнот: метою є максимізація модулярності Q – показника якості кластеризації:

$$Q = (1/(2m)) \times \Sigma\_\{i, j\}[A_{ij} - (k_i k_j / 2m)] \delta(c_i, c_j),$$

де A_{ij} – елемент матриці суміжності, k_i – ступінь вузла i, m – кількість ребер,

c_i – кластер вузла i, δ – функція Кронекера. Метод Louvain ітеративно об’єднує вузли у кластери, покращуючи Q.

Для моделювання динаміки станів агентів у часі використовується рекурсивне оновлення:

$$s_i\ (t+1) = f\big(s_i(t), I_i(t)\big),$$

де $I_i(t)$ – інформаційний вплив від інших агентів, що може бути зваженою сумою повідомлень або взаємодій. Цей підхід дозволяє враховувати ефект резонансу, повторного впливу, адаптації поведінки та інформаційного виснаження.

Приклад сценарію:

Початковий етап. Модель визначає ключових агентів з використанням алгоритму поширення впливу. Це задає стартові умови для інформаційної операції.

Поширення інформації. Метод Монте-Карло моделює, як інформація поширюватиметься через мережу, враховуючи ймовірності та випадкові ефекти. Одночасно, алгоритм Louvain допомагає зрозуміти, як інформація поширюється всередині та між спільнотами.

Адаптація та покращення стратегій. У процесі поширення інформації генетичні методи покращують стратегії агентів, адаптуючи їх до нових умов. Наприклад, агенти можуть змінювати свої стратегії на основі реакції інших агентів.

Зворотний зв'язок і динаміка. Методи зворотного зв'язку враховують зміни, що відбуваються в часі, як-от зміна громадської думки або вплив нових інформаційних подій.

Застосування всіх п'яти методів у визначеній послідовності дає змогу створити гнучку, адаптивну та динамічну модель, яка здатна імітувати складні процеси інформаційних операцій у соціальних мережах. Ці методи,

працюючи разом, створюють новий гібридний метод, що дає змогу враховувати різноманітні аспекти поведінки агентів, структуру мережі, імовірнісні ефекти та динамічні зміни, що робить модель реалістичнішою та потужнішою (рис. 2.2).

Обґрунтування вибору. Цей комплексний метод дає змогу створити модель, яка враховує як мікродинаміку поведінки окремих агентів, так і макродинаміку мережі загалом. Метод поширення впливу та виявлення спільнот допомагають зрозуміти, як інформація поширюється і через які вузли. Методи Монте-Карло і генетичний метод забезпечують гнучкість і адаптивність моделі, даючи їй змогу ефективно моделювати невизначеність і зміни в стратегіях агентів. Метод зворотного зв'язку додає важливий аспект динаміки, даючи змогу моделі враховувати циклічні зміни та адаптацію агентів у реальному часі. На рис. 2.2 продемонстровано рівень інтеграції комплексного методу в межах агентної моделі, де 0 – не інтегрований зовсім, а 10 – інтегрований в повній мірі.

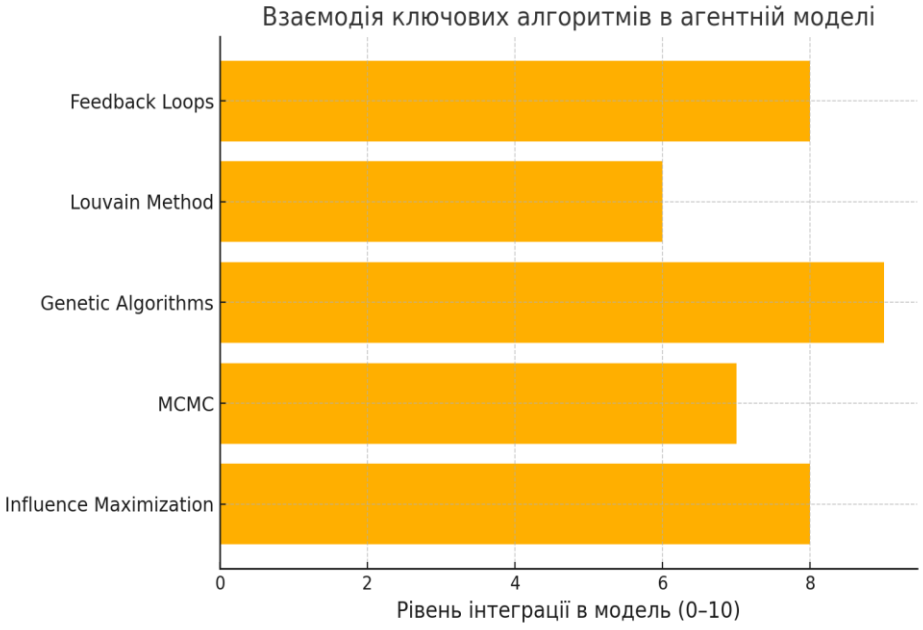

Рис. 2.2. Рівень інтеграції комплексного методу в межах агентної моделі для виявлення інформаційних операцій у соціальних мережах.

Ця комбінація робить модель комплексною і придатною для аналізу широкого спектра сценаріїв інформаційних операцій, включно з поширенням дезінформації, впливом лідерів думок, а також динамічною зміною думок і взаємодій усередині соціальної мережі.

2.3. Класифікація агентів та метод розрахунку коефіцієнтів їхнього впливу на соціальну мережу.

Зростаюче значення соціальних мереж у формуванні суспільного дискурсу пояснює підвищений інтерес до аналізу того, як відбуваються інформаційні впливи та поширення дезінформації в онлайновому середовищі. Актуальність таких досліджень зумовлюється двома основними чинниками. По-перше, використання ботів, тролів та інших інструментів для маніпулювання громадською думкою стало справжнім викликом для інформаційної безпеки, оскільки такі технології впливають на політичні процеси, громадську довіру та якість суспільних дискусій. По-друге, зростає кількість звичайних користувачів, які мимоволі поширюють неперевірену або маніпулятивну інформацію, посилюючи ефект дезінформаційних кампаній. За таких умов постає потреба у детальному аналізі динаміки поширення контенту з урахуванням різноманіття типів учасників соціальної мережі – від лідерів думок і звичайних користувачів до автоматизованих та деструктивних агентів.

Враховуючи важливість цього питання, актуальною є розробка методу розрахунку коефіцієнту впливу різних типів користувачів – агентів – на соціальну мережу.

У межах дослідження проведено аналіз чотирьох типів агентів і визначено їхні ключові характеристики, що визначають рівень впливу під час інформаційної операції, який, своєю чергою, є основним критерієм при побудові імітаційної моделі виявлення інформаційних операцій в соціальній мережі.

Аналізуючи типи віртуальних агентів в соціальних мережах в рамках побудови моделі, визначені такі:

- першоджерело – перший тип агентів, які публікують контент для подальшої популяризації;
- акаунти–боти – другий тип агентів (бот – це спеціальна програма, що виконує автоматично і за заданим розкладом певні дії через ті ж інтерфейси, що й звичайний користувач) – використовуються для штучного нарощування «лайків» чи коментарів з метою підняття рейтингу публікації серед користувачів мережі, дають змогу посилити вплив у інформаційному середовищі шляхом залучення нових цільових аудиторій (бот поширює новину, але майже нічого не змінює, він на відміну від троля є механічним, троль – креативним);
- акаунти-тролі – третій тип агентів – звичайна дійова особа, яка надає кольорового забарвлення новинам. Вони оперують великими групами і подають новину з різних ракурсів. За цим типом агентів можуть знаходитись блогери, лідери думок, які репостять «вірусний» контент на власні сторінки, тим самим одразу (в один клік) збільшуючи потенційні цільові аудиторії (перегляди, лайки, репости) в рази;
- четвертий тип агентів – реальні люди, які є потенційною цільовою аудиторію інформаційної операції, вони «споживають» контент та сприймають його достовірним, тобто підпадають під інформаційний та психологічний вплив і стають «інфікованими» даним контентом, вірять, що інформація правдива та популяризують її далі в мережі, базуючись на своїй вірі.

Передбачається, що агенти в соціальній мережі можуть

1) самозароджуватися;
2) породжувати нових агентів шляхом репостінгу (repost);
3) «вмирати» – зникати з простору агентів (припинити передавати контент);

4) отримувати лайки (like) від інших агентів.

Після появи «вірусного» контенту в акаунті першоджерела, різні типи агентів починають безперервно взаємодіють один з одним, та передавати інформацію (репост) за такими алгоритмами:

від одного агенту до іншого – взаємодія між четвертим типом агентів;

від одного агенту до групи агентів – взаємодія між третім та четвертим типом агентів, між першим та четвертим типом агентів та між другим та четвертим типом агентів;

від однієї групи агентів до іншої – взаємодія між другим типом агентів

Характер зв'язків між агентами може бути як прямим, так і зворотнім.

У такій системі рішення задачі можуть формуватися за рахунок взаємодії великої кількості агентів, що безперервно взаємодіють один з одним, а також формується колективна поведінка.

У результаті виділення типових агентів – акаунтів-користувачів – в соціальній мережі, виявлення закономірностей їхньої взаємодії та притаманних даним агентам характеристик, стає очевидним, що така умовна інформаційна система не належить до формальних моделей, є неоднорідною, а поведінка її елементів – акаунтів користувачів – нераціональною.

Метод розрахунку коефіцієнтів впливу різних типів агентів включає формування основних характеристик для кожного типу агенту, виявлення для кожного типу агенту самих значущих характеристик, які формують їхню модель поведінки в соціальних мережах, та на їхній основі математична модель коефіцієнту впливу.

Основні характеристики різних типів агентів.

Перший тип агентів – це лідери думок, які публікують контент для подальшої популяризації. Цьому типу притаманні такі характеристики як авторитетність, центральність, значимість думок, високий ступінь до впливу на аудиторію та високий ступінь прийняття рішень в умовах

невизначеності. Лідери думок публікують (генерують) власний контент, або використовують контент із зовнішнього джерела.

Indirect links (непрямі зв'язки): часто мають розгалужену «мережу впливу» через посередників, їхні публікації ретвітять/поширюють інші користувачі, які, у свою чергу, далі транслюють ці думки, що створює високий рівень непрямих зв'язків.

Frequency (частота взаємодій): зазвичай середня або висока, це спричинено кількістю регулярних публікацій та реакцією на запити аудиторії.

Stability (стабільність зв'язків): мають доволі стабільне коло підписників.

Multiplexity (множинність): висока ймовірність кількох рівнів контакту, тобто цей тип агентів може взаємодіяти з аудиторією одночасно в різних соцмережах (Twitter/X, Instagram, Facebook, YouTube). Мультиплексність часто висока.

Strength (сила зв'язку): має сильні зв'язки із «близьким оточенням» (команда, колеги), але з підписниками – «слабкі» або «помірні» зв'язки. Можна стверджувати про полярний розподіл сили зв'язків: мало дуже сильних, багато слабких.

Direction (напрямок): здебільшого односторонній у плані «фолловер → лідер думок» чи «лідер думок → аудиторія». Кількість людей, які читають лідера думок, значно перевищує кількість, за якими стежить він сам. Водночас, коли лідер думок згадує когось (відповідає), це створює спрямований канал впливу з високим резонансом.

Symmetry (симетрія): у звязках «лідера думок» і масової аудиторії асиметрія переважає: більшість зв'язків не є взаємними (follower→followed).

Другий тип агентів – це акаунти-боти (спеціальна програма, що виконує автоматично і за заданим розкладом певні дії через ті ж інтерфейси, що й

звичайний користувач). Використовуються для штучного нарощування «лайків» чи коментарів з метою підняття рейтингу публікації серед користувачів мережі, дають змогу посилити вплив у інформаційному середовищі шляхом залучення нових цільових аудиторій (бот поширює новину, але майже нічого не змінює, він на відміну від троля є механічним, троль – креативним).

Indirect links (непрямі зв'язки): можуть породжувати непрямі зв'язки, особливо якщо бот «цитує» чи поширює контент інших і таким чином запускає «ланцюжковий» ефект. Але часто ці зв'язки залишаються слабко вираженими або мають низьку довіру.

Frequency (частота): як правило, висока (або дуже висока) за рахунок автоматичного постингу великої кількості повідомлень, часто за шаблоном.

Stability (стабільність): діяльність бота може бути стабільною (довготривала й послідовна) або епізодичною (кампанійного типу). Однак стабільність особистих «зв'язків» у ботів низька, адже вони рідко формують тривалі чи «емоційні» зв'язки з реальними користувачами.

Multiplexity (множинність): як правило, низька, оскільки боти зазвичай працюють на одній або кількох пов'язаних платформах, але не схильні до багаторівневої взаємодії.

Strength (сила зв'язку): здебільшого слабкі зв'язки. Контакт із ботом не ґрунтується на довірі чи емоційній близькості, тож «сила» таких зв'язків незначна.

Direction (напрямок): Боти часто поширюють контент (outbound direction) і мають мало вхідних зв'язків. Водночас інші користувачі можуть підписуватися чи не підписуватися на бота, тож є асиметричний спрямований канал.

Symmetry (симетрія): здебільшого асиметрія – рідкісні випадки, коли бот «свідомо» читає (авторизує, відповідає) інших. Навіть якщо бот фолловить

когось, це зазвичай автоматизоване явище й не означає «справжнього» взаємного зв'язку.

Третій тип агентів – це акаунти-тролі – звичайна дійова особа, яка надає «кольорового забарвлення» публікаціям. Вони оперують великими групами і подають новину з різних ракурсів. За цим типом агентів можуть знаходитись блогери, лідери думок, які репостять «вірусний» контент на власні сторінки, тим самим одразу (в один клік) збільшуючи потенційні цільові аудиторії (перегляди, лайки, репости) в рази. Тролі за часту коментують контент, тим самим залучаються до активної багатосторонньої комунікації. Наявність специфічних соціальних норм відсутня, але наявна висока ігрова взаємодія агентів.

Indirect links (непрямі зв'язки): можуть виникати значні непрямі ефекти, оскільки тролі часто провокують конфлікти, які потім «відлунюються» через перепости інших. Втім, троль зазвичай свідомо не розвиває непрямі ланцюжки, та це може статись «автоматично» через обговорення.

Frequency (частота): середня або висока – тролі зазвичай дуже активні, але діяльність може бути нерівномірною (спалахи активності в певних темах).

Stability (стабільність): низька. Тролі часто змінюють теми, можуть переходити з одного каналу дискусії в інший, створюють нові акаунти. Стійких зв'язків із «жертвами» чи з аудиторією не підтримують.

Multiplexity (множинність): залежить від «стратегії» тролінгу – іноді це лише один майданчик, іноді – кілька (Twitter, Facebook, форуми). Проте емоційно глибоких чи комплексних зв'язків зазвичай немає.

Strength (сила зв'язку): переважно слабка, але з високим рівнем «емоційного збурення»; тобто троль може викликати сильну негативну реакцію, проте це не «сила зв'язку» у класичному розумінні довіри чи дружби.

Direction (напрямок): тролі найчастіше «нападають» або провокують (outbound direction), а інші реагують на них. Тому в них наявна значна асиметричність у комунікації.

Symmetry (симетрія): дуже рідко зустрічається симетрична взаємодія; зв'язки зазвичай односторонні (тролеві відповідають, але сам троль не прагне «порозуміння»). «Взаємне читання» може бути, якщо тролі об'єднуються в групу, але це швидше виняток.

Четвертий тип агентів – це реальні люди, які є потенційною цільовою аудиторію інформаційної операції, вони «споживають» контент та сприймають його достовірним, тобто підпадають під інформаційний та психологічний вплив і стають «інфікованими» даним контентом, вірять, що інформація правдива та популяризують її далі в мережі, базуючись на своїй вірі.

Indirect links (непрямі зв'язки): у типового користувача є зв'язки зі знайомими й друзями, які далі можуть бути пов'язані з іншими, тож непрямі ланцюжки можуть бути досить довгими (ефект «шести рукостискань»). Здебільшого помірна кількість непрямих зв'язків.

Frequency (частота): сильна варіативність від дуже низької (рідко пишуть) до досить високої (активні блогери). У середньому – помірна.

Stability (стабільність): зазвичай помірна. Основні дружні або родинні зв'язки доволі стабільні, але онлайнова активність може змінюватися з часом (хтось перестає користуватися соцмережею або заводить нові акаунти).

Multiplexity (множинність): у реальному житті люди взаємодіють і онлайн, і офлайн. Тож для близьких друзів чи колег множинність каналу висока. В середньому рівень мультиплексності цього типу агентів вищий, ніж у ботів, але нижчий, ніж у лідерів думок із багатьма медіаплатформами.

Strength (сила зв'язку): у більшості зв'язків із друзями, близькими знайомими – помірна або сильна. Із «випадковими» фолловерами чи

онлайн-знайомими – слабка. Тобто спостерігається полярне розподілення за силою зв’язку, але масштаби менші, ніж у лідерів думок.

Direction (напрямок): багато зв’язків є взаємними (undirected) або двосторонніми (друзі читають одне одного). Утім, бувають і односторонні стосунки (наприклад, коли хтось читає знайомого, а той не фолловить у відповідь).

Symmetry (симетрія): зазвичай відносно висока (друзі, родичі найчастіше «фоловлять» чи «дружать» одне з одним). Але симетричність не абсолютна – особливо якщо йдеться про підписки на відомих блогерів чи інфлюенсерів.

Таким чином емпіричним шляхом проаналізовано три варіанти розповсюдження контенту в соціальній мережі X (Twitter). Під час дослідження на основі запропонованих характеристик агентів визначено, які саме агенти і в який проміжок часу долучаються до розповсюдження визначеного контенту.

У результаті аналізу поширення інформації в соціальній мережі X (Twitter) визначено, що процес відбувається у три фази, залежно від часу, що минув із моменту публікації повідомлення.

Перша фаза охоплює перші 60 хвилин після публікації. У цей період поширення відбувається переважно серед підписників лідера думок, які складають його безпосередню аудиторію.

Друга фаза починається після першої години і триває до 10 годин після публікації. У цей період відбувається поділ між всіма агентами розповсюдження інформації. Поширення інформації в цей час визначається коефіцієнтами впливу кожного агента, що забезпечує експоненційне чи лінійне зростання охоплення.

Третя фаза настає після 10 годин до визначеного в дослідженні часу, у нашому випадку 24 години. Основну роль відіграють звичайні користувачі,

оскільки вплив ботів і тролів поступово зменшується і вже не має статистично значущого впливу на подальше поширення інформації.

Вибір основних початкових параметрів.

lom_people – змінна, яка відповідає значенню кількості підписників лідера думки;

lom_count – змінна, яка відповідає значенню кількості розповсюдження серед підписників лідера думки;

bot_count – змінна, яка відповідає значенню кількості розповсюдження завдяки ботам;

troll_count – змінна, яка відповідає значенню кількості розповсюдження завдяки тролям;

person_count – змінна, яка відповідає значенню кількості розповсюдження завдяки звичайним користувачам;

k_person – відсоток кількості звичайних користувачів з кількості підписників лідера громадської думки;

k_bot – відсоток кількості ботів з кількості підписників лідера громадської думки;

k_troll – відсоток кількості тролів з кількості підписників лідера громадської думки;

a – коефіцієнт, який відображає розповсюдження інформації від ботів на користувачів соціальної мережі у 2 фазі;

q –коефіцієнт, який відображає розповсюдження інформації від тролів на користувачів соціальної мережі 2 фазі;

b – коефіцієнт, який відображає розповсюдження інформації від звичайних користувачів на користувачів соціальної мережі;

v – коефіцієнт, який відображає розповсюдження інформації від ботів на користувачів соціальної мережі 3 фазі;

m – коефіцієнт, який відображає розповсюдження інформації від тролів на користувачів соціальної мережі 3 фазі.

Ця структура дозволяє чітко відмежувати етапи інформаційної динаміки та використовувати окремі математичні моделі для кожного з них.

Метод розрахунку коефіцієнтів впливу для різних типів агентів.

1. Лідери думок (Opinion Leaders).

Роль у соціальній мережі:

- Впливають на думку великої кількості підписників.
- Часто є експертами або авторитетами в певній тематиці.
- Генерують унікальний контент, що активно поширюється іншими користувачами.

Ключові характеристики:

1) Кількість підписників *lom_people* – чим більше аудиторія, тим більший вплив.

2) Рівень взаємодії з аудиторією *En* – середня кількість лайків, коментарів, репостів на одиницю контенту.

3) Частота публікацій *Ps* – середня кількість постів на добу.

4) Довжина життєвого циклу поста *Pl* – період активного обговорення (в годинах).

5) Коефіцієнт впливу α*alpha* – оцінка рівня довіри до контенту на основі взаємодій.

Для визначення кількості підписників, які фактично взаємодіють із контентом лідера думки, використовуємо наступну формулу, врахувавши коефіцієнт масштабування *K*:

$$lom\_count = lom\_people \times (1 - e\text{^}(-(Ps \times Pl \times En \times \alpha)\ /K))$$

Коефіцієнт впливу *l* лідера думок на користувачів в соціальної мережі визначаємо як:

$$l = lom\_coumt\ /\ lom\_people$$

2. Боти (Bots).

Роль у соціальній мережі:

- Автоматизовані акаунти, що генерують або поширюють

контент.

- Використовуються для масового розповсюдження інформації або дезінформації.
- Часто мають низьку взаємодію з аудиторією, але високу частоту публікацій.

Ключові характеристики:

1) Частота публікацій Pf – кількість постів у день (зазвичай висока).

2) Кількість репостів Nr – середня кількість репостів на день.

3) Коефіцієнт автоматизації β\beta – частка контенту, що є автоматично згенерованим.

4) Рівень взаємодії Li – середня кількість відповідей на коментарі (зазвичай низький).

5) Стійкість до блокування Br – оцінка ймовірності, що бот не буде видалений.

За ключовими характеристиками визначимо коефіцієнт впливу ботів a в окремо взятому посту. Кількість ботів на пряму залежить від рівня взаємодії Li, та визначається з кількістю однотипних коментарів Liz:

$$k\_bot = Li/Liz$$

Коефіцієнт впливу ботів a визначаємо як (розповсюджується на 2 фазу):

$$\alpha = Pf \times Nr \times \beta$$

Емпіричним шляхом встановлено, що кількість репостів Nr, які несуть дійсний інформаційний вплив Nrd на залучення аудиторії, становить 20%:

$$Nr = Nrd \times 20/100$$

На 3 фазі починається виявлення та блокування ботів, тому коефіцієнт впливу a змінюється на коефіцієнт впливу v:

$$v = \alpha \times Br$$

Коефіцієнт блокування залежить від часу та визначається за формулою:

$$Br(t) = exp(-Br(t-60)), t > 60$$

3. Тролі (Trolls).

Роль у соціальній мережі:

- Провокують конфлікти, дискредитують інформацію, поширюють дезінформацію.
- Орієнтовані на емоційні реакції інших користувачів.
- Мають середню або високу взаємодію через провокаційний контент.

Ключові характеристики:

1) Кількість конфліктних коментарів *Ncc* – кількість негативних або провокаційних коментарів.

2) Рівень залученості *Loi* – середня кількість реакцій на контент.

3) Частота атак *Af* – кількість провокаційних дій у день.

4) Тривалість активності *Ad* – середній час, протягом якого троль активний у мережі.

5) Коефіцієнт агресії *δ\delta* – рівень токсичності коментарів (оцінка за NLP-аналізом).

За ключовими характеристиками визначимо коефіцієнт впливу тролів q в окремо взятому посту. Кількість тролів на пряму залежить від кількості конфліктних коментарів *Ncc*, визначаємо, аналізуючи пост по його коментарям *Nccz*. Визначення агента-троля залежить від кількісті конфліктних або провокаційних коментарів:

$$k\_troll = Ncc / Nccz$$

Коефіцієнт впливу q тролів на користувачів в соціальної мережі визначаємо як (розповсюджується на 2 фазу):

$$q = Af \times Ad \times \delta$$

Ad залежить від часу та коефіцієнта впливу *k*:

$$Ad = t \times k$$

На 3 фазі суттєву роль відіграє рівень залученості *Loi* тролів, тому коефіцієнт впливу q змінюється на коефіцієнт впливу m:

$$m = q \times Loi$$

4. Звичайні користувачі (Regular Users).

Роль у соціальній мережі:

- Основна маса учасників, що пасивно або активно споживають контент.
- Можуть поширювати контент, але не впливають на широкий загал.

Ключові характеристики:

1. Кількість лайків та репостів *Nlr* – середня кількість взаємодій з контентом на день.
2. Рівень активності *Al* – кількість постів та коментарів на день.
3. Коефіцієнт впливу η*eta* – частка оригінального контенту у профілі.
4. Частота заходів в соцмережу Fs – середня кількість входів у день.
5. Індивідуальний коефіцієнт мотивації λ*lambd* – рівень зацікавленості користувача в участі в інформаційних операціях.

За ключовими характеристиками визначимо коефіцієнт впливу звичайних користувачів в окремо взятому посту. Кількість звичайних користувачів буде залишковою за виключенням кількості ботів та тролів, визначаємо аналізуючи пост по його коментарям:

$$k\_person = lom\_count - (bot\_count + trol\_count)$$

Коефіцієнт впливу b звичайних користувачів на інших учасників соціальної мережі враховуємо однаковим для всіх фаз та визначаємо як:

$$b = Nlr \times Al \times \eta \times Fs \times \lambda$$

Використовуючи наступні данні (рис.2.3) побудуємо графік коефіцієнтів впливу на розповсюдження інформації в соціальній мережі X

(Twitter) для кожного типу агента. Програмний код, написаний на мові програмування python, наведено в **Додатку 4**.

Для розрахунку коефіцієнтів впливу було використано наступні значення:

1) Коефіцієнта впливу лідера думок: *lom_people = 7000, Ps = 3, Pl = 5, En = 120, alpha = 0.1, K = 10;*

2) Коефіцієнта впливу ботів: *Pf = 5, Nrd = 20, beta = 0.00055, Br = 0.1;*

3) Коефіцієнта впливу тролів*: Af = 250, t = 600, k = 0.001, delta = 0.000114, Loi = 0.059;*

4) Коефіцієнта впливу звичайних користувачів: *Nlr = 17, Al = 6, eta = 0.0013, Fs = 5, lambd = 0.0009.*

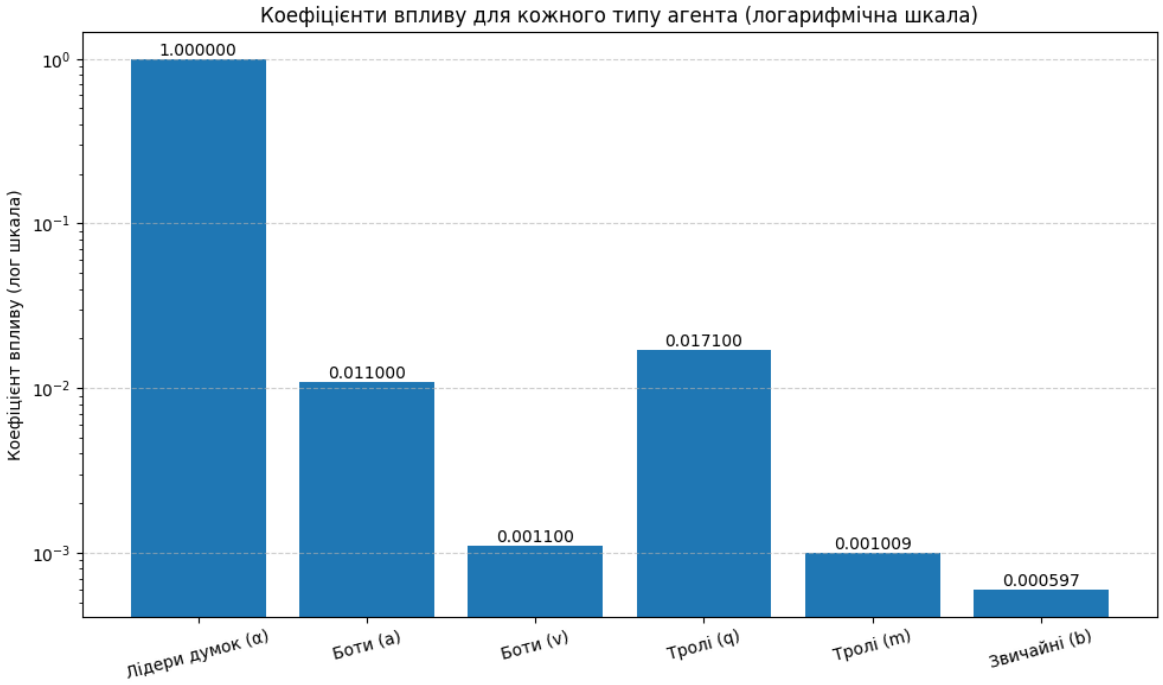

Рисунок 2.3 – Графік коефіцієнтів впливу кожного типу агента на розповсюдження інформації в соціальній мережі X (Twitter)

Вплив на користувачів здійснюється поетапно та залежить від першоджерела, а саме:

Лідери думок (негайне максимальне охоплення), рис. 2.4;

Боти (фаза 2) – автоматизована присутність (рис. 2.5);

Тролі (фаза 2) – високий емоційний вплив;

Боти/тролі (фаза 3) – вплив падає через блокування / зниження активності (рис. 2.6 та рис. 2.7);

Звичайні користувачі – мінімальний, довгостроковий вплив.

Проведемо моделювання змінюючи основні характеристики кожного типу агента, для знаходження більш значних та вагомих характеристик (рис. 2.4–2.7). Програмний код, написаний на мові програмування python, наведено в **Додатку 5**.

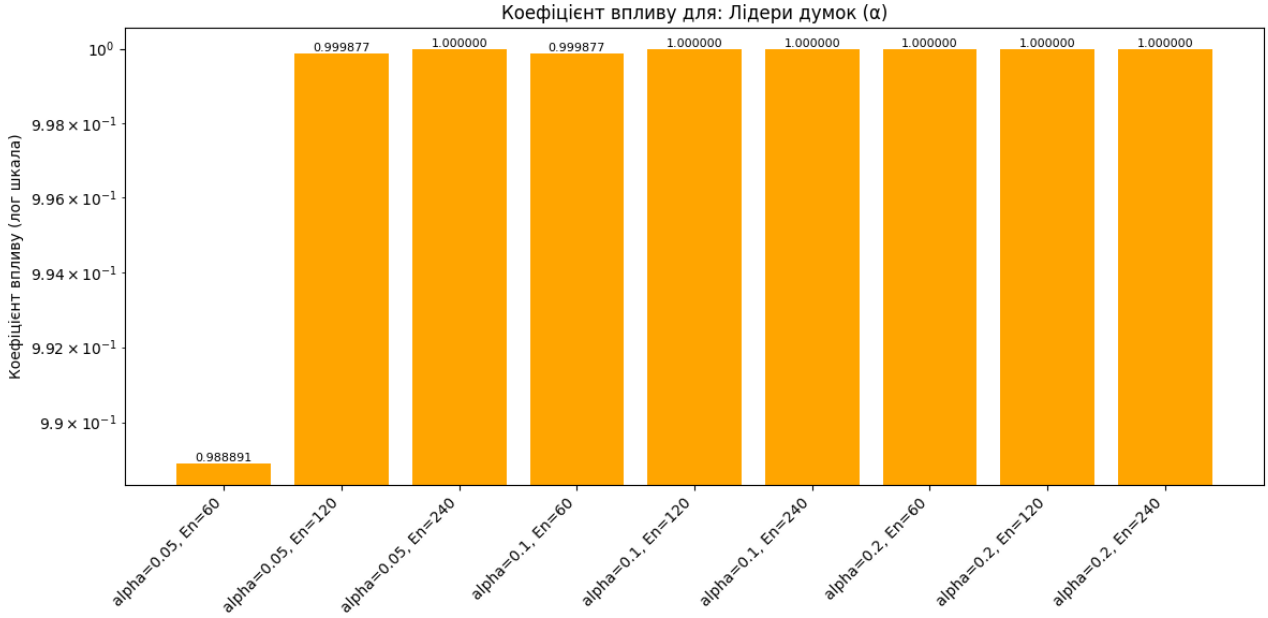

Рисунок 2.4 – Результати обчислення коефіцієнту впливу лідера думок при різних вхідних параметрах

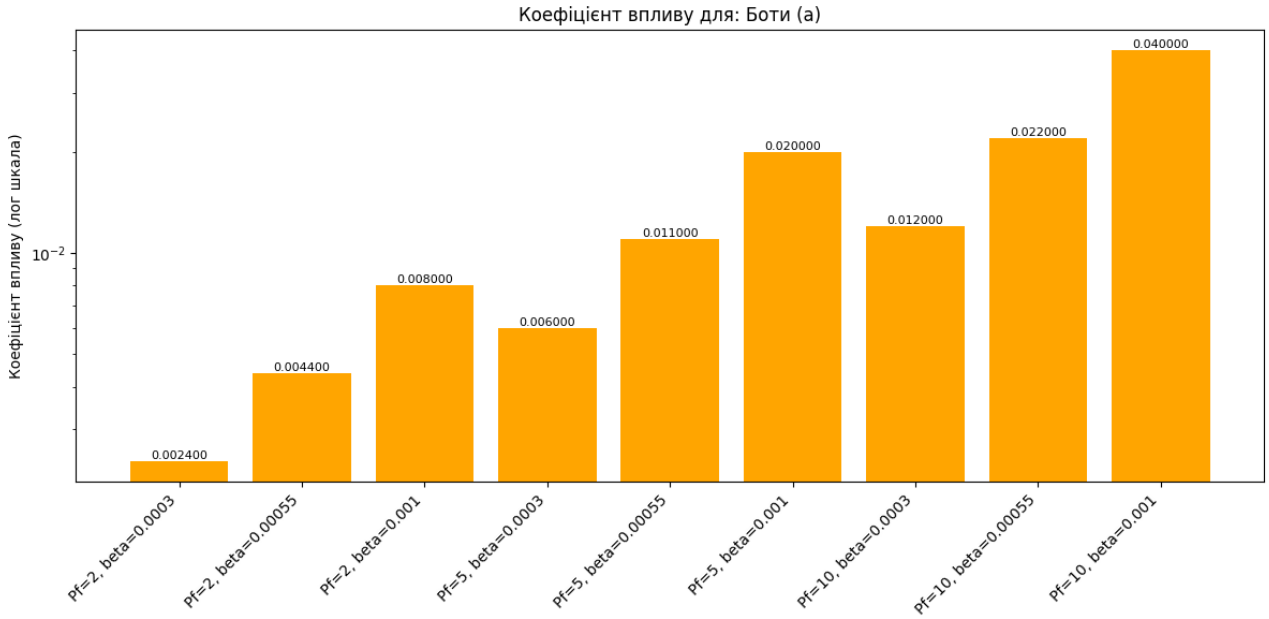

Рисунок 2.5 – Результати обчислення коефіцієнту впливу ботів при різних вхідних параметрах

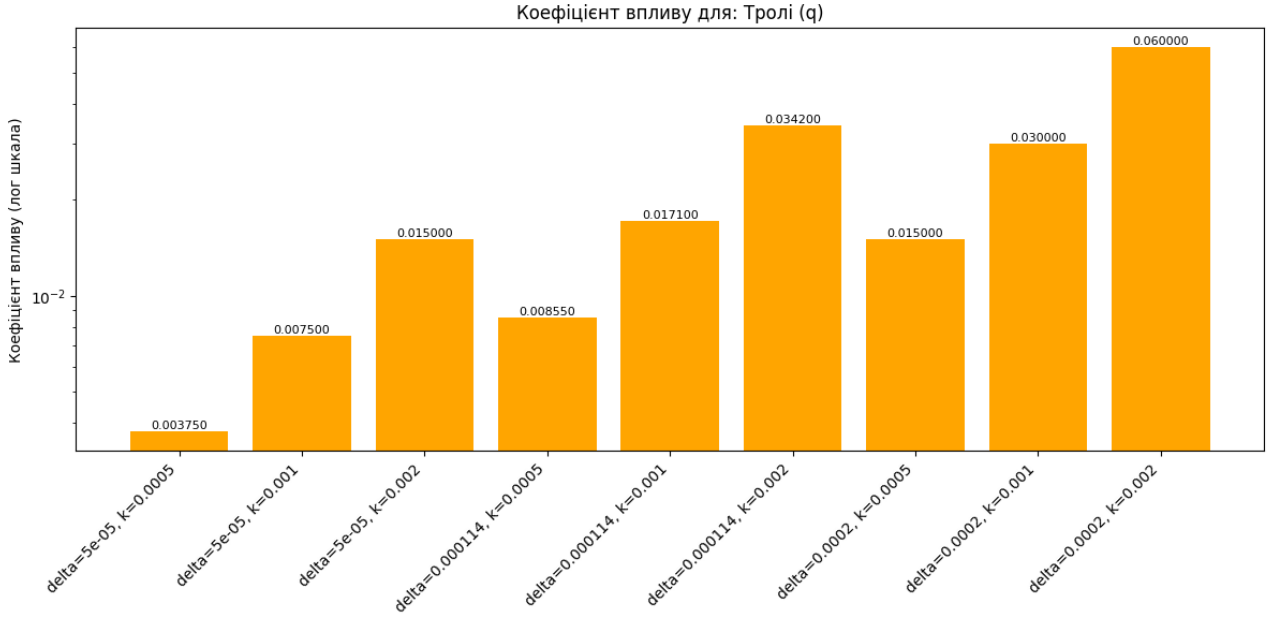

Рисунок 2.6 – Результати обчислення коефіцієнту впливу тролів при різних вхідних параметрах

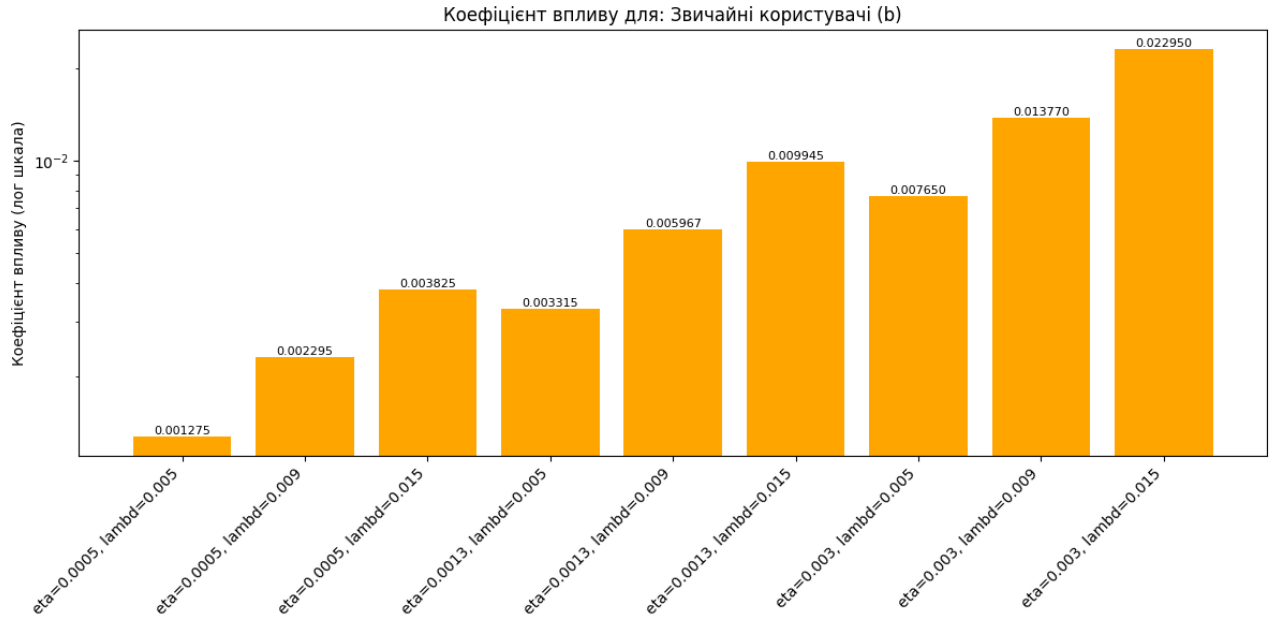

Рисунок 2.7 – Результати обчислення коефіцієнту впливу звичайних користувачів при різних вхідних параметрах

На основі моделей та обчислених коефіцієнтів можна зробити такі висновки:

1) **Лідери думок** l, ключові параметри: α (довіра), En (взаємодія). Висновок: навіть незначне збільшення α або En швидко доводить вплив до 1, тобто лідери думок досягають максимальної ефективності при середньому рівні активності та довіри. Чутливість висока лише при дуже низьких значеннях α/En, після чого графік «насичується». Найбільш вагомий параметр – En (взаємодія), але ефект значно підсилюється при довірі ($\alpha \geq 0.1$).

2) **Боти** a, ключові параметри: Pf (частота публікацій), β (автоматизація). Висновок: вплив ботів зростає лінійно при збільшенні Pf, а також помітно змінюється при навіть невеликих змінах автоматизації. Наприклад, перехід β з 0.0003 до 0.001 при фіксованому Pf створює зростання впливу ботів майже втричі. Найбільш вагомий параметр – β (автоматизація), оскільки він масштабує весь ефект.

3) **Тролі** q, ключові параметри: δ (агресія), k (коефіцієнт активності). Висновок: вплив тролів експоненційно зростає при збільшенні обох

параметрів. Найбільше значення q спостерігається при максимальному k і δ. Значення зростають від 0.0037 до 0.06 – майже в 16 разів у межах сценарію. Обидва параметри мають однакову чутливість, особливо у комбінації.

4) **Звичайні користувачі** b, ключові параметри: η (оригінальний контент), λ (мотивація). Висновок: лінійне зростання впливу, але він залишається низьким у порівнянні з іншими агентами. Найвищі значення досягаються лише при максимальному η та λ. Від 0.001 до 0.023 – ефект є, але «м'який». Найбільш вагомий параметр – λ (мотивація), що визначає готовність поширювати контент.

В табл. 2.1 наведено порівняння поведінкових характеристик, їхній вплив на ефективність агентів.

Таблиця 2.1

Найважливіші поведінкові характеристики агентів

№	Агент	Найважливіший параметр	Тип зростання	Коментар
1	Лідери думок	*En, α*	Швидке насичення	Достатньо середніх значень для максимуму
2	Боти	*β*	Лінійне/експоненційне	Залежить від ступеня автоматизації
3	Тролі	*δ, k*	Експоненційне	Вибуховий ріст при провокаціях
4	Звичайні користувачі	*λ*	Лінійне	Найменший вплив, але стабільний

Проведене дослідження дозволило здійснити формалізовану оцінку впливу різних типів агентів на поширення інформації в соціальній мережі X (Twitter). Було розроблено та застосовано метод розрахунку коефіцієнтів впливу з урахуванням поведінкових характеристик чотирьох типів агентів: лідерів думок, ботів, тролів і звичайних користувачів. Створено моделі та на

їхній основі та проведено симуляції впливу, що дозволило зробити наступні ключові висновки:

Лідери думок демонструють найвищий вплив уже на початку, що обумовлено довірою до них α та рівнем взаємодії En. Вплив насичується при середніх значеннях і швидко досягає максимуму.

Боти є ефективними у 2 фазі поширення. Їх вплив зростає лінійно або експоненційно при підвищенні автоматизації β та частоти публікацій Pf. У 3 фазі ефективність падає через блокування.

Тролі мають вибуховий емоційний вплив, особливо при високих значеннях агресії δ та активності k. Вони здатні швидко ескалувати ситуацію в інформаційному середовищі.

Звичайні користувачі мають мінімальний, але стабільний вплив, який нарощується в третій фазі. Важливими факторами є мотивація λ та присутність оригінального контенту η.

Проведений аналіз параметрів чутливості дозволив виокремити найбільш вагомі характеристики для кожного типу агентів та визначити їхній вплив на інформаційну операцію. Це дає змогу:

- здійснювати більш точне прогнозування динаміки поширення повідомлень;
- конструювати стратегії впливу з акцентом на потрібний тип агентів;
- розробляти сценарії інформаційних операцій з урахуванням фазової структури залучення аудиторії.

Висновок. Найбільшу ефективність в інформаційній операції демонструють агенти, що активні в перших двох фазах – зокрема, лідери думок, тролі та боти. Їхній вплив у комбінації є критичним для успішної реалізації інформаційної операції. За відсутності ботів і тролів ефективність значно знижується. Звичайні користувачі формують фонове, пасивне поширення, і можуть лише підсилювати ефект лідерів у пізні фази.

Висновки до Розділу 2.

1. Проведено аналіз переваг агентного моделювання для побудови моделі виявлення інформаційних операцій в соціальних мережах: будуються сценарії можливих варіантів розвитку подій у майбутньому, на підставі чого формуються, а потім відбираються стратегічні альтернативи, які працюють у кожному сценарії і служать підставою для прийняття рішень про вибір інтегрованої стратегії.
2. Розроблено комплексний метод, який дає змогу моделювати складні соціальні процеси, розповсюдження інформації та взаємодію агентів. Метод заснований на поєднанні методу поширення впливу (Influence Maximization) для визначення ключових агентів (інфлюенсерів) у соціальній мережі, методу Монте-Карло (MCMC) для моделювання ухвалення рішень агентами, генетичному методі для покращення стратегій агентів у процесі інформаційних операцій, методі виявлення спільнот (Louvain) для ідентифікації спільнот і кластерів усередині соціальної мережі для більш точного моделювання поширення інформації, методі зворотного зв'язку (Feedback Loops) для моделювання динамічних змін у поведінці агентів і поширенні інформації. Застосування всіх п'яти методів у визначеній послідовності дає змогу створити гнучку, адаптивну та динамічну модель, яка здатна імітувати складні процеси інформаційних операцій у соціальних мережах. Ці комбінації створюють можливості для аналізу широкого спектра сценаріїв інформаційних операцій, включно з поширенням дезінформації, впливом лідерів думок, а також динамічною зміною думок і взаємодій усередині

соціальної мережі. Даний метод буде застосовано при побудові агентної моделі.

3. Розроблено метод розрахунку коефіцієнту впливу чотирьох типів агентів на соціальну мережу, які будуть враховані при побудові агентної моделі. В рамках методу здійснено класифікацію агентів за рівнем впливу, виведено показники чотирьох типів агентів та визначено коефіцієнт впливу кожного типу агенту.

РОЗДІЛ 3. МОДЕЛЬ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ НА ОСНОВІ АГЕНТНОГО МОДЕЛЮВАННЯ

3.1. Середовища агентного моделювання

Для розуміння логіки процесів АМ бібліотеки агентного моделювання, повинні містити велику кількість прикладів симуляцій, щоб допомогти як початківцям, так і досвідченим користувачам.

Основна задача середовищ АМ полягає в тому, щоб спростити синтаксис і семантику програмування настільки, щоб зробити його доступним, надаючи дуже просту мову програмування, яка не вимагає знань з інформатики, і спрямований на залучення неспеціалістів (не вчених-моделювальників, а також науковців), щоб вони могли вивчати складні системи шляхом самостійного написання програм та/або проведення комп'ютерних симуляцій.

У зв'язку з тим, що агентний підхід виник в 90-х роках минулого століття в університетському середовищі США, досі більшість інструментів призначається для академічних і навчальних цілей, та не є комерційними продуктами в повній мірі [96-98].

Середовища АМ надають інфраструктуру та інструменти для розробки, візуалізації та аналізу агентних моделей. Вони різняться за можливостями, мовами програмування та інтерфейсами користувача. Проведено аналізі найвідоміших середовищ АМ:

1. NetLogo

Ця інформаційна система призначена для створення імітаційних моделей і технологій моделювання в суспільних науках. Це зручне середовище з відкритим вихідним кодом, відоме своєю простотою та універсальністю. Воно надає графічний інтерфейс і вбудовану мову програмування для розробки моделей. Дослідники можуть створювати

моделі для вивчення різних явищ, від екологічних систем до соціальної динаміки. призначена для моделювання ситуацій і феноменів, що відбуваються в природі та суспільстві. Зручний засіб для моделювання складних систем, що розвиваються в часі. NetLogo використовують для демонстрації мережевих феноменів і для моделювання соціальних феноменів у навчальних курсах з менеджменту [99].

2. Repast

Інструментарій для AOM на основі Java, який добре налаштовується і підходить для великомасштабних симуляцій. Він надає розробникам широкі бібліотеки та інструменти для побудови та аналізу агентних моделей у різних сферах. Оновлена версія Repast 3 містить три безкоштовні бібліотекі агентного моделювання з відкритим вихідним кодом - Repast J на основі Java, Repast .NET на основі C# та Repast Py на основі NQP (Not Quite Python). Об'єктно-орієнтоване проектування є важливим для забезпечення гнучкості як бібліотечних, так і користувацьких моделей. Використання шаблонів проектування корисне для покращення якості реалізації [100, 101].

3. General Purpose Simulation System World - GPSS World - загальноцільова система моделювання для побудови імітаційних моделей систем масового обслуговування, інформаційних процесів, моделей у мережі інтернет із застосуванням об'єктно-орієнтованого програмування. Даний програмний продукт дозволяє розробляти імітаційні моделі на мові програмування GPSS і підтримує широкі функціональні можливості: від використання вбудованих розподілів ймовірності до автоматичної генерації множинних експериментів, в тому числі для візуалізації та модельної оптимізації. На відміну від вищезгаданих систем система GPSS World не підтримує графічну реалізацію математичної моделі, тобто не містить вбудованих архетипів, за допомогою яких можна було б візуалізувати зв'язки між змінними моделі [102].

4. Arena

Комерційний продукт для імітаційного моделювання, створений компанією Systems Modeling Corporation мовою SIMAN. Дозволяє створювати віртуальні рухомі комп'ютерні моделі, за допомогою яких можна наочно уявити роботу багатьох реальних систем. Сфера основних застосувань системи - імітаційне моделювання виробничих технологічних процесів і операцій, складський облік, банківська діяльність, оптимізація обслуговування клієнтів у сфері послуг, транспортні завдання [103].

5. Plant Simulation Plant Simulation

Програмне середовище для імітаційного моделювання процесів, основною метою якого є оптимізація вхідних потоків, завантаження ресурсів, логістика, а також методи управління плануванням як окремих ліній і ділянок, так і цілого виробництва. Продукт має вбудовану мову програмування SimTalk. Продукт реалізує об'єктно-орієнтований підхід до реалізації імітаційних моделей. Побудова моделі проводиться в інтерактивному режимі за допомогою бібліотек типових елементів, що надаються. Крім базового набору об'єктів є спеціалізовані бібліотеки. Продукт підтримує необмежену ієрархію (вкладеність) моделей, тим самим надаючи користувачеві можливість створювати власні об'єкти і бібліотеки об'єктів. У моделі застосовуються об'єкти таких основних типів: матеріалопотік, інформаційний потік, рухомі об'єкти, призначений для користувача інтерфейс, ресурси та інструменти. Кожен об'єкт має власну поведінку і призначений для користувача інтерфейс для налаштування його параметрів. Plant Simulation дає змогу візуалізувати роботу моделей як у 2D, так і в 3D-режимі [104].

6. Swarm.

Вільний інструментарій з відкритим вихідним кодом з прив'язками як до Objective-C, так і до Java (Minar et al.1996). Swarm також використовує ліцензію GPL. Swarm спочатку розроблявся як програмний інструментарій для створення імітаційних моделей в галузі штучного життя (A-Life).

Програма надає користувачу гнучкий, вкладений підхід до моделювання взаємодій. [105].

7. MASON

Це безкоштовна бібліотека агентного моделювання з відкритим вихідним кодом, яка надає основні послуги, що можуть бути легко змішані з іншими бібліотеками. Ключова особливість полягає в тому, що бібліотеки мінімальні і добре поєднуються з бібліотеками сторонніх розробників. Тут реалізовано лише основні функції, щоб підвищити інтероперабельність і спростити навчання. Повне розділення між моделями, користувацькими інтерфейсами та офлайн-сховищем. Реалізована можливість створення і життездатності великої кількості агентів (наприклад, мільйони). Всі прогони моделі повинні є відтворюваними. Крім того, підтримуються контрольні точки (тобто збереження та відновлення прогонів моделі під час виконання) [106, 107].

8. Ascape

Це безкоштовна бібліотека агентного моделювання з відкритим вихідним кодом, яка представляє моделі у вигляді складної серії вкладених "сцен", населених агентами, чия поведінка реалізується за допомогою абстрактних правил. Автор моделі стверджує, що абстрагування складності є потужним способом зосередити зусилля з проектування та розробки. Вибіркову абстракцію слід використовувати, щоб забезпечити структуру для користувачів і зменшити складність користувацького коду. Абстракції повинні бути дуже ретельно продумані, щоб уникнути обмеження гнучкості [108, 109].

9. EcoLab

Універсальна бібліотека моделювання на основі агентів, написана мовами C++ та TCL/Tk. Також надаються стандартизовані моделі, з якими можна порівнювати бібліотеки агентного моделювання. Автор стверджує, що рефлексія має важливе значення для агентних моделей. Рефлексія - це

здатність досліджувати інформацію про тип об'єктів динамічно, тобто під час виконання програми. Динамічні вказівники, які автоматично відстежують такі об'єкти, як агенти, є важливими. Ці вказівники повинні автоматично відзначати тип об'єкта, що відстежується, і вказувати, чи було вивільнено посилання на об'єкт з пам'яті [110, 111].

10. AniLogic - розробка компанії XJTeknologies – є комерційним продуктом, який знайшов широке застосування серед користувачів.

Конкурентною перевагою AniLogic є підтримка всіх трьох парадигм імітаційного моделювання і можливість використання їх в рамках однієї моделі. Також AnyLogic відрізняє потужне продуктивне ядро, що дозволяє симулювати поведінку мільйонів агентів; багаті можливості для анімації і графічного опису моделі; підтримка різноманітних типів експериментів, включаючи аналіз чутливості, метод Монте-Карло, вбудований оптимізатор OptQuest; можливості інтеграції з базами даних, ERP і CRM системами; набір бібліотечних об'єктів з областей логістики, бізнес процесів, пішохідної динаміки.

При розробці агентной моделі в AnyLogic користувач вводить параметри агентів (це можуть бути люди, компанії, активи, проекти, транспортні засоби, міста, тварини і т.д.), визначає їх поведінку, поміщає їх в будь-яке навколишнє середовище, встановлює можливі зв'язки, після чого запускає моделювання. Індивідуальна поведінка кожного агента утворює глобальну поведінку системи, що моделюється [112]. Це використовувалось при в наукових дослідженнях та виявилося досить ефективним.

Нижче наведено порівняльну таблицю вищезазначених ПЗ, де серед іншого зазначені такі параметри як:

Free access: наявність ПЗ у безкоштовному доступі

Language: мова програмування, яка використовується для розробки програмного забезпечення.

Open-source software: програмне забезпечення з відкритим вихідним кодом.

GUI: наявність графічного інтерфейсу користувача.

Learning Curve: простота вивчення та використання програмного забезпечення.

Community Support: сила спільноти, яка надає допомогу, ресурси та розширення.

Advanced Features: додаткові функції або модулі, які виходять за межі базового агентного моделювання.

В табл. 3.1 наведено порівняльні характеристики середовищ АМ.

Таблиця 3.1

Порівняльні характеристики середовищ АОМ

Software	free access	Open-source software	Language	GUI	Learning Curve	Community Support	Advanced Features
1	2	3	4	5	6	7	8
NetLogo	+	+	Scala, Java	Yes	Low	Strong	HubNet, BehaviorSpace, GIS
Repast	+	+	Java, C#, Python	Yes	Moderate	Active	Repast Simphony, GIS
General Purpose Simulation System			GPSS	Yes	Low	Limited	Discrete-Event Simulation
Arena	-	-	SIMAN	Yes	Moderate	Active	Process Analysis, Simulation Optimization

1	2	3	4	5	6	7	8
Plant Simulation Plant Simulation	-	-	SimTalk	Yes	Moderate	Limited	Detailed Manufacturing Simulation
Swarm	+	+	Java	No	High	Limited	Spatial Analysis, Evolutionary Algorithms
MASON	+	+	Java	No	High	Active	Detailed Agent-Based Models
Ascape	+	+	Java	Yes	Moderate	Limited	Visualization, Social Network Analysis
EcoLab	-	-	C++, TCL/Tk	No	High	Limited	Ecological Modeling
AniLogic	+	-	Java SE	Yes	High	Strong	Visualization, Social Network Analysis, HubNet, BehaviorSpac, GIS, Ecological Modeling

Кожне програмне забезпечення має свої сильні сторони та сфери застосування. Деякі з них більш зручні у використанні завдяки потужній спільноті, тоді як інші пропонують розширені функції для конкретних галузей, таких як виробництво або екологічне моделювання.

Для подальшої побудови моделі та імітійних експериментів виявлення інформаційних операцій в соціальних мережах будуть використані деякі з вище зазначених середовищ, виходячи з їхніх функціональних можливостей та кількості типів агентів. Пропонуються нижче розглянути основні типи агентів, які залучені для розповсюдження контенту.

3.2. Модель на основі АМ з одним типом агентів.

Дана модель демонструє поширення інформації через соціальну мережу, її інтерпретація полягає в тому, що кожен вузол представляє собою окремого користувача – агента, що має зв'язки з іншими користувачами свого кола спілкування, і моделює поширення контенту через визначену мережу. В даній моделі вибрано один тип агенту – звичайний користувач мережі. Кожен агент (вузол) може перебувати в одному з трьох станів: синій – користувач, який «запостив» контент, червоний – користувач, який ознайомився з інформацією, сірий – користувач, який бачив, передав та більше не зацікавлений в даній інформації (Програмний код моделі надано в **Додатку 6**).

Позначимо кортеж параметрів моделі як: $P = (N, d, I_o, p_s, f_c, p_r, p_g, F(t))$

де:

- N – number-of-nodes – кількість початкових точок (вузлів у мережі);
- d – average-node-degree – середня кількість зв'язків між точками;
- I_o – initial-outbreak-size – початкова кількість носіїв інформації;
- p_s – virus-spread-chance – ймовірність поширення інформації;
- f_c – virus-check-frequency – частота перевірки на наявність інформації;
- p_r – recovery-chance – ймовірність "забуття" (втрати інформації);
- p_g – gain-resistance-chance – шанс появи резистентності до інформації (вузол стає «сірою точкою»);

- $F(t)$ – Network Status – функція, яка описує зміну кількості активних/інфікованих/резистентних точок у часі.

Проведемо декілька симуляцій з різними початковими параметрами. Це дасть можливість виявити, який параметр більш значний для поставленого завдання та залежності між точками.

В результаті проведених експериментів отримано наступні моделі:

1) Модель 1 (рис. 3.1)

$$P = (1000,6,343,0.014,4,0.028,1.0)$$

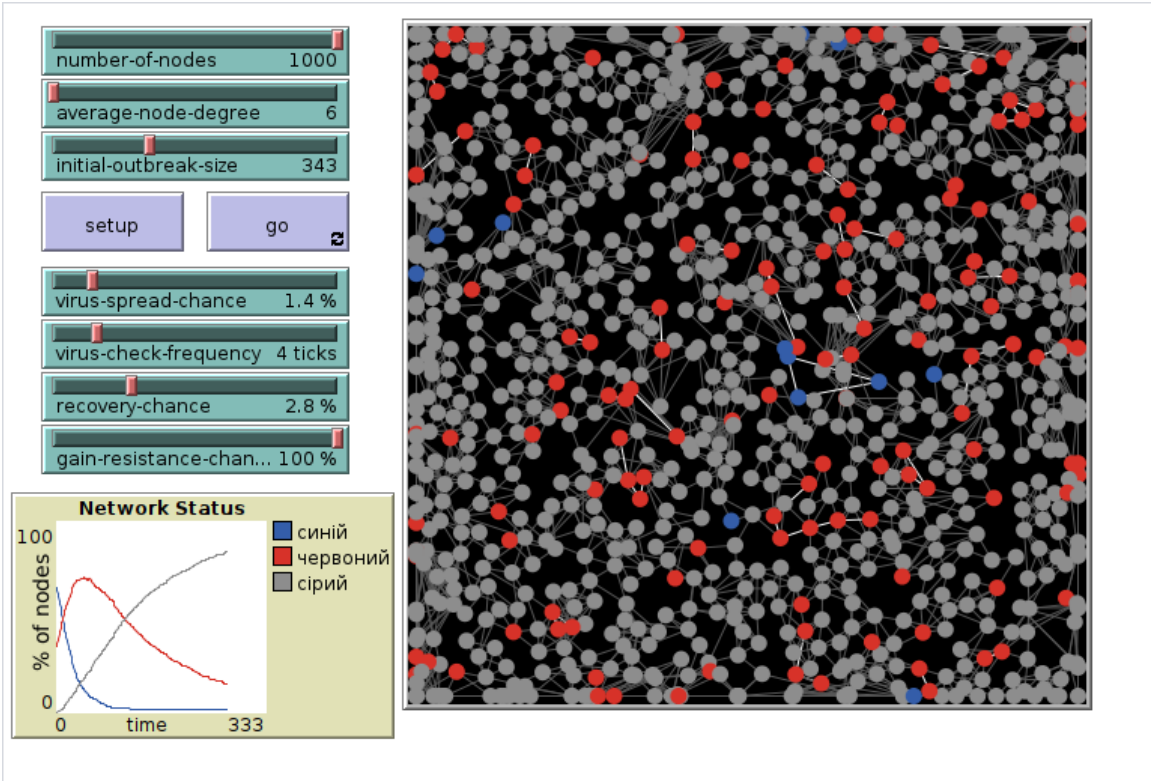

Рисунок 3.1 – Результат моделювання 1

Зміни, що відбуваються в моделі: початкова кількість поширення велика (343), усі агенти з часом отримують «опір» (gain-resistance-chance = 100%). Висновок: контент швидко поширюється, але через 100% опір інформація швидко зникає з мережі.

2) Модель 2 (рис. 3.2)

$$P = (1000,6,343,0.014,4,0.028,0.61)$$

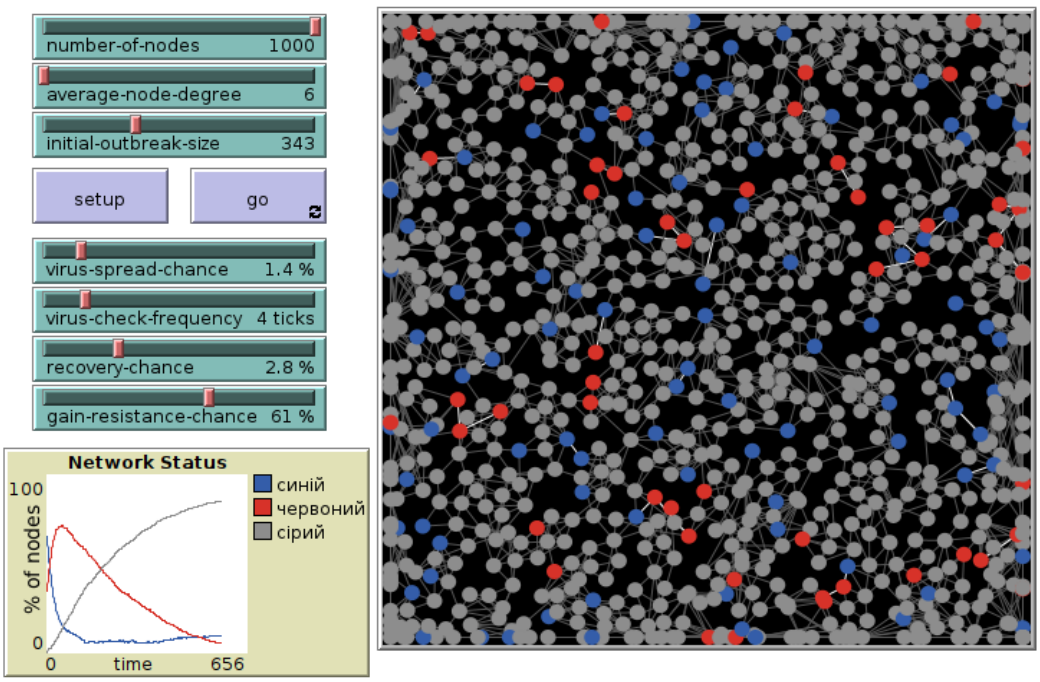

Рисунок 3.2 – Результат моделювання 2

Зміни, що відбуваються в моделі: зменшено опір до 61%, інші параметри збережені як при першому моделюванні. Висновок: зменшення опору дозволяє контенту циркулювати довше, зростає тривалість хвилі поширення.

3) Модель 3 (рис. 3.3)

$$P = (1000,6,1,0.014,4,0.01,0.61)$$

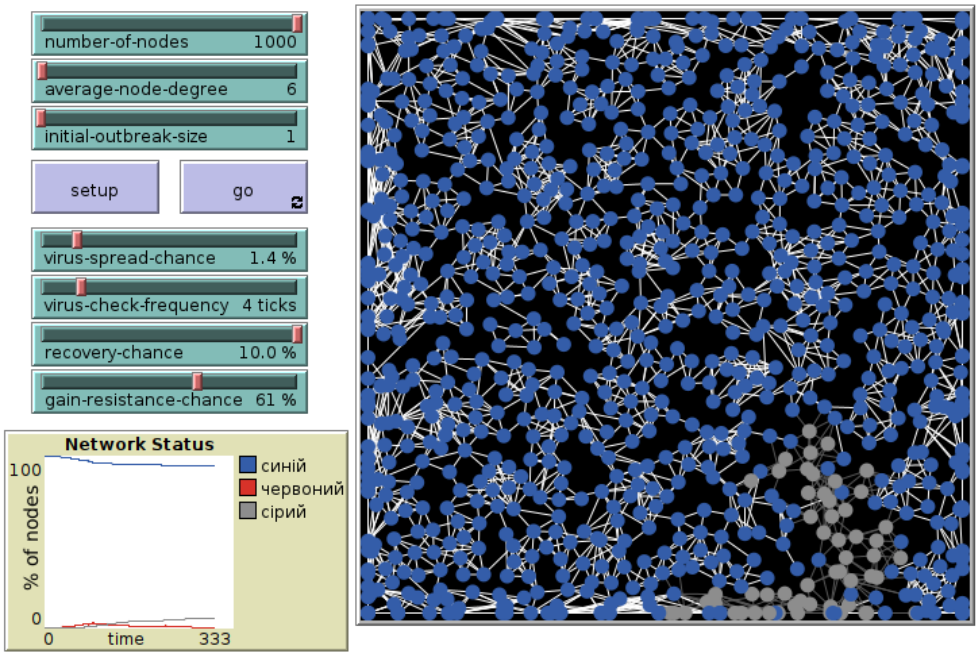

Рисунок 3.3 – Результат моделювання 3

Зміни, що відбуваються в моделі: початковий спалах – лише 1 агент; більший рівень забуття (10%) при опорі 61%. Висновок: з низьким стартом охоплення обмежене, але зменшений опір утримує інформацію довше в локальних групах.

4) Модель 4 (рис.3.4)

$$P = (1000,38,1,0.014,4,0.01,0.5)$$

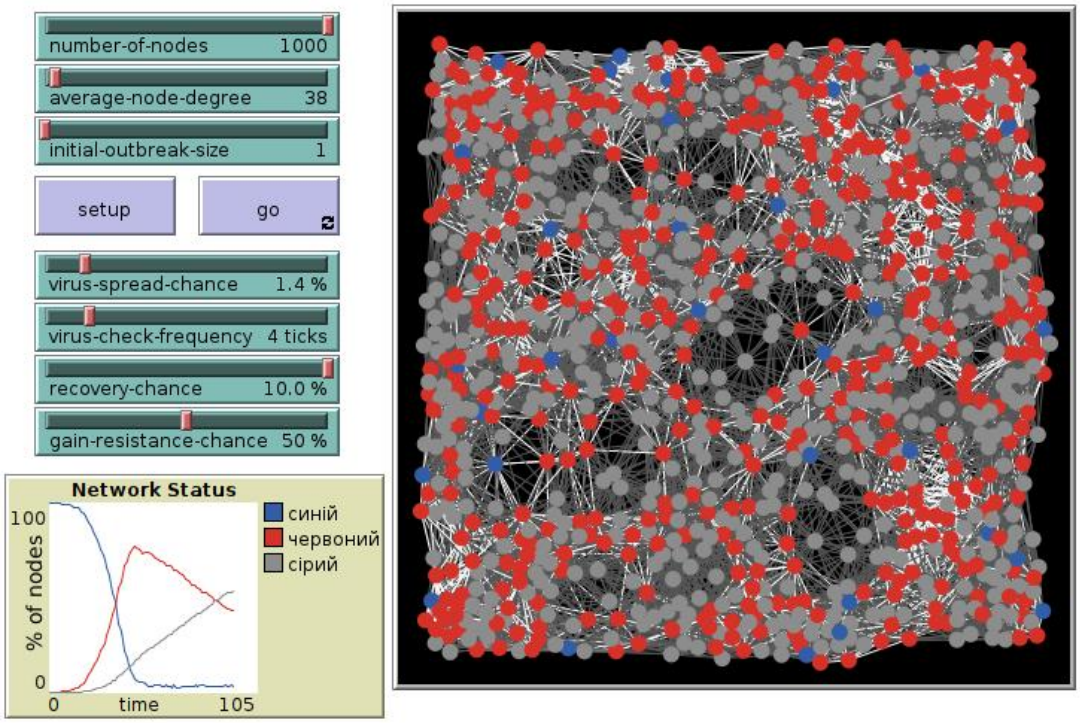

Рисунок 3.4 – Результат моделювання 4

Зміни, що відбуваються в моделі: збільшено середню кількість зв'язків (38), старт операції з 1 агента, опір становить 50%. Висновок: більша щільність зв'язків значно прискорює поширення навіть з мінімального початкового спалаху.

5) Модель 5 (рис. 3.5)

$$P = (1000,38,295,0.014,4,0.1,1.0)$$

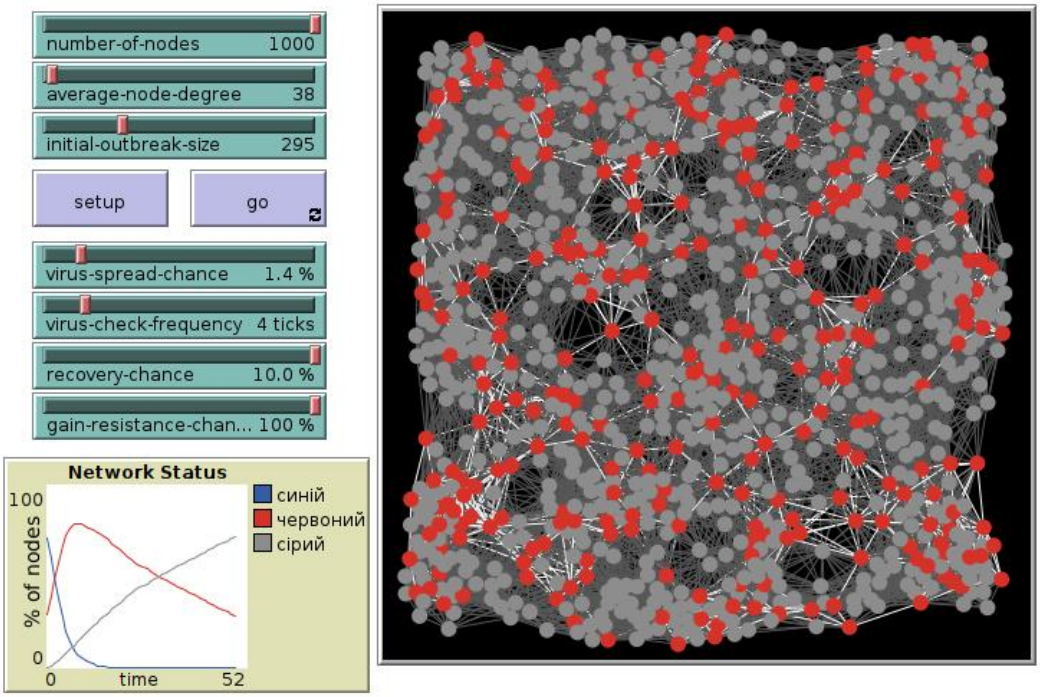

Рисунок 3.5 – Результат моделювання 5

Зміни, що відбуваються в моделі: велика кількість зв’язків (38) і високий старт (295), при максимальному опорі (100%). Висновок: дуже швидке охоплення, але повне згасання через повний опір.

6) Модель 6 (рис. 3.6)

$$P = (1000,234,90,0.014,4,0.1,1.0)$$

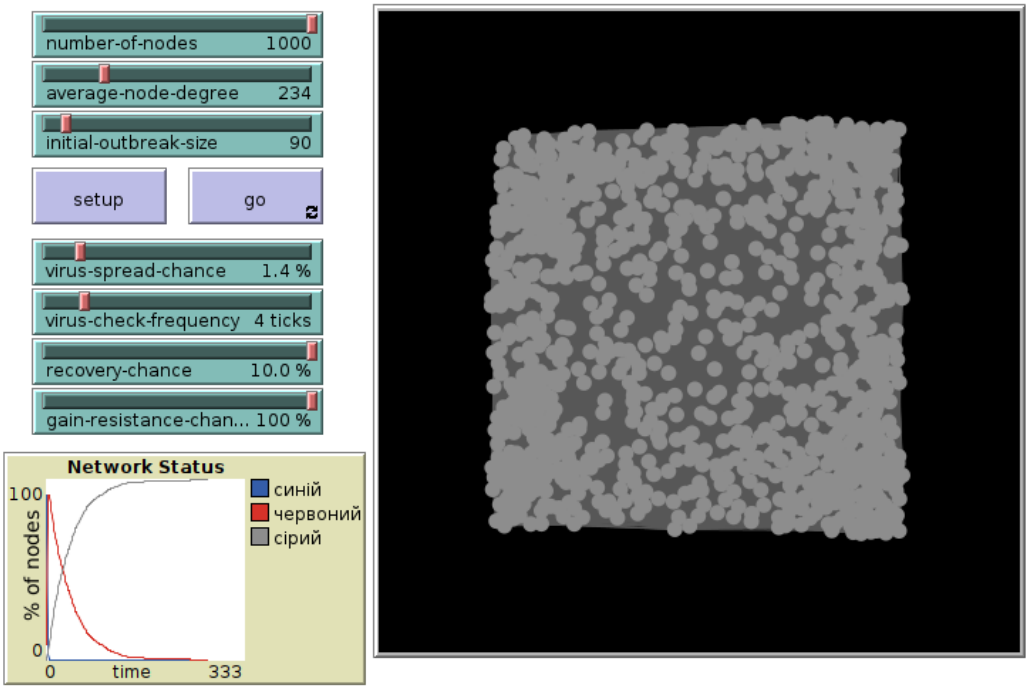

Рисунок 3.6 – Результат моделювання 6

Зміни, що відбуваються в моделі: дуже висока щільність зв’язків (234), старт з 90 агентів, опір максимальний, становить 100%. Висновок: миттєве розповсюдження з повним згасанням, модель показує межу максимальної швидкості поширення.

7) Модель 7 (рис. 3.7)

$$P = (1000,10,90,0.014,4,0.1,1.0)$$

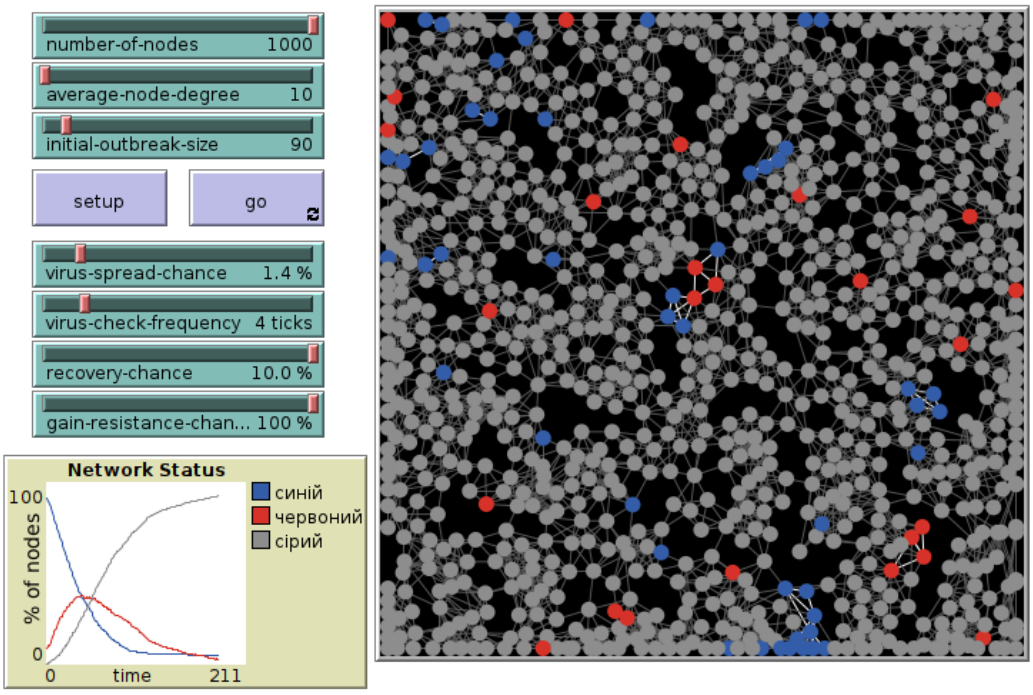

Рисунок 3.7 – Результат моделювання 7

Зміни, що відбуваються в моделі: середня кількість зв’язків (10), старт з 90 агентів, опір 100%. Висновок: поширення стабільне, але все одно швидко згасає через повний опір.

8) Модель 8 (рис. 3.8)

$$P = (300,2,4,0.1,2,0.002,1.0)$$

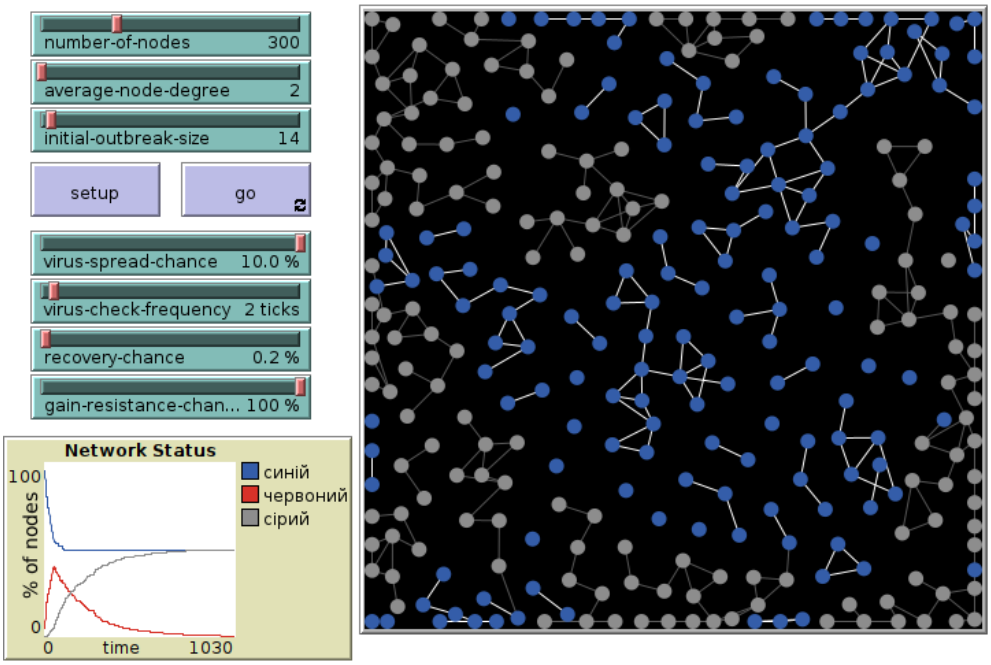

Рисунок 3.8 – Результат моделювання 8

Зміни, що відбуваються в моделі: мала мережа (300), низька щільність зв'язків (2), висока ймовірність поширення (10%), низький рівень забуття (0.2%), опір становить 100%. Висновок: невеликі та слабо зв'язані мережі з високим шансом передачі та низьким забуттям утримують інформацію значно довше.

Результатом такого експерименту розповсюдження контенту в однорідній соціальній мережі, тобто з одним типом агенту, є виявлення ключових параметрів для типу агенту – звичайний користувач, які мають бути враховані при виявлені інформаційних операцій.

3.3 Модель на основі АМ з чотирьох типів агентів.

Дана модель демонструє поширення інформації через соціальну мережу X (Twitter). Через програмні обмеження імітаційного середовища застосоване масштабування реальних значень, зменшених у 1000 разів для коректної роботи агентного моделювання. Модельна інтерпретація полягає в тому, що з'являється можливість відстежувати розповсюдження інформації від лідера громадської думки до звичайних користувачів цієї мережі та вплив інших суб'єктів розповсюдження – ботів та тролів.

1) **Lom** – лідер громадської думки (далі – ЛГД) – це особа або організація, яка має значний вплив на формування думок, поглядів та рішень у суспільстві. ЛГД користується високим авторитетом та довірою у певній сфері.

2) **Bot** (далі – бот) – це автоматизована програма або система, яка виконує певні завдання без участі людини. Боти можуть бути корисними інструментами для виконання рутинних завдань, таких як відповіді на повідомлення, аналіз даних або проведення пошуків. Вони можуть функціонувати як у відкритих середовищах (соціальні мережі, месенджери), так і в закритих (вебсайти, програми).

3) **Troll** (далі – троль) – це особа або група осіб, які навмисно провокують конфлікти, ображають інших користувачів або поширюють дезінформацію в інтернеті з метою дестабілізувати дискусії та викликати негативну реакцію. Тролі часто діють анонімно і використовують маніпулятивні техніки для досягнення своїх цілей.

4) **Person** (далі – звичайний користувач) – це людина, яка взаємодіє з певною системою, програмою чи платформою, користуючись її функціями або послугами. Користувачі можуть мати різний рівень технічної підготовки і виконувати різноманітні завдання, від перегляду контенту до створення інформації чи взаємодії з іншими користувачами.

Основні початкові параметри:

users – популяція агентів, що відповідає кількості переглядів посту на момент доби після публікації;

lom_people – параметр, що відповідає кількості підписників лідера громадської думки;

lom_count – змінна, яка відповідає значенню кількості розповсюдження серед підписників лідера громадської думки;

bot_count – змінна, яка відповідає значенню кількості розповсюдження завдяки ботам;

troll_count – змінна, яка відповідає значенню кількості розповсюдження завдяки тролям;

person_count – змінна, яка відповідає значенню кількості розповсюдження завдяки звичайним користувачам;

total_count – змінна, яка відображає кількість користувачів, яким доведена інформація у конкретний момент часу (сума lom_count, bot_count, troll_count, person_count);

tal_count – логарифмічна зміна, яка використовується для відображення загального росту кількості користувачів та активності системи користувачів, тролів та ботів у моделі. Він є метрикою, що відображає сумарну активність або значущість користувачів, включаючи їхній внесок у систему з часом;

k_person – відсоток кількості звичайних користувачів з кількості підписників лідера громадської думки;

k_bot – відсоток кількості ботів з кількості підписників лідера громадської думки;

k_troll – відсоток кількості тролів з кількості підписників лідера громадської думки;

a – коефіцієнт, який відображає розповсюдження інформації від ботів на користувачів соціальної мережі у 2 фазі;

q –коефіцієнт, який відображає розповсюдження інформації від тролів на користувачів соціальної мережі 2 фазі;

b – коефіцієнт, який відображає розповсюдження інформації від звичайних користувачів на користувачів соціальної мережі;

v – коефіцієнт, який відображає розповсюдження інформації від ботів та тролів на користувачів соціальної мережі 3 фазі;

tal_count_at_60 – змінна, яка відповідає значенню tal_count при time = 60 хвилин;

tal_count_at_600 – змінна, яка відповідає значенню tal_count при time = 600 хвилин;

tal_count_at_1440 – змінна, яка відповідає значенню tal_count при time = 1440 хвилин;

k1 – коефіцієнт, що використовується для зростання логарифмічного значення tal_count у другій фазі;

k2 – коефіцієнт, що використовується для зростання логарифмічного значення tal_count у третій фазі;

dynamicGrowth – подія, що описує поведінку даного моделювання.

Для побудови моделі були враховані дані із соціальної мережі X. Створено імітаційну модель інформаційної операції на основі залученості чотирьох типів агентів, та з урахуванням їхніх коефіцієнтів впливу (рис. 3.9).

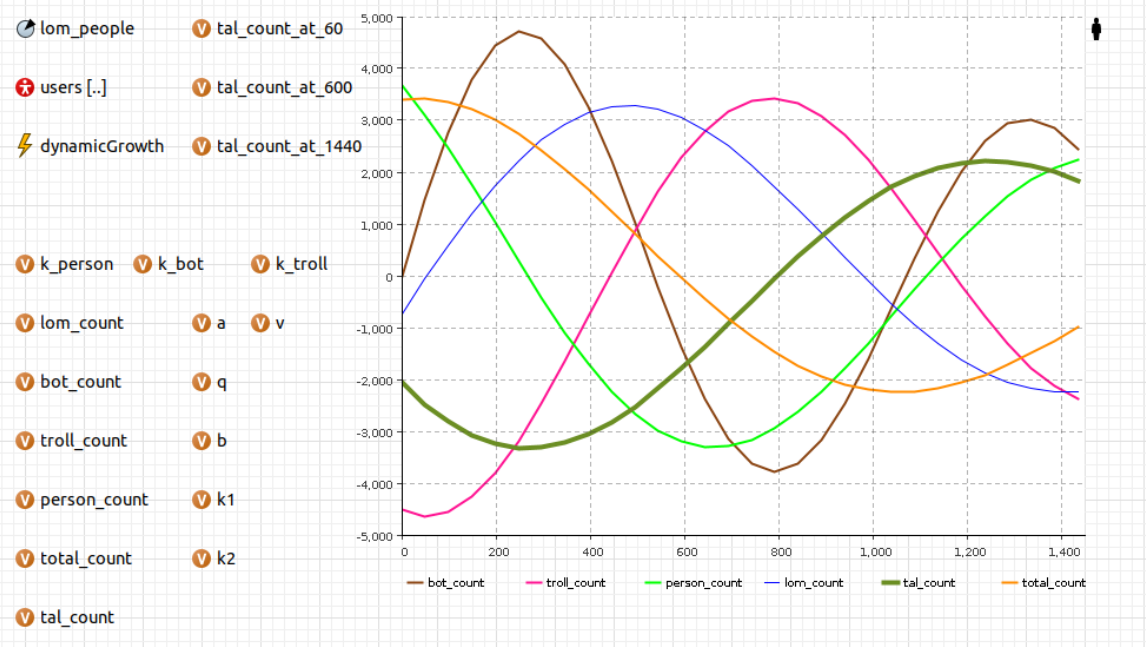

Рисунок 3.9 – Модель інформаційної операції

Провівши аналіз та методом експертних оцінок встановивши часову динаміку розповсюдження інформації в соціальній мережі X, дійшли висновку, що існують три етапи розповсюдження інформації від часу її публікації. На першому етапі інформація розповсюджується серед підписників ЛГД – це відбувається за перші 60 хвилин після часу публікації.

Експериментально було з'ясовано, що на другому етапі відбувається розділення всіх підписників на категорії: 20% становлять боти, 30% становлять тролі, 50% становлять звичайні користувачі. Приріст на другому етапі відбувається за рахунок коефіцієнтів впливу кожної з категорій. З дослідження було виявлено, що другий етап має вплив у перші 10 годин після публікації посту. Таким чином, другий етап у математичному розрахунку триває з 60 до 600 хвилин після публікації посту. Третій етап – це розповсюдження серед звичайних користувачів, оскільки вплив ботів та тролів нівелюється з часом і є не достатнім для подальшого врахування.

Математичний опис моделі.

Етап 1: Зростання за рахунок розповсюдження серед підписників ЛГД:

Формула для ЛГД (lom_count):

$$lom\_count = lom\_people \times time() \ /60$$

Це лінійна залежність, яка описує зростання кількості lom_people у перші 60 хвилин.

Формула для загальної кількості користувачів (total_count):

$$total\_count = lom\_count + bot\_count + troll\_count + person\_count$$

Формула є сумою всіх типів користувачів, включаючи ботів, тролів та звичайних користувачів.

Формула для tal_count:

$$tal\_count = lom\_people \times Math.log10(0.1 \times time() + 1)$$

Логарифмічна залежність описує зростання значення tal_count. Використання логарифму забезпечує уповільнене зростання, особливо на початку.

Етап 2: Підключення поширення від ботів, тролів і звичайних користувачів:

Формула для кількості ботів (bot_count):

$$bot\_count = (lom\_people \times k\_bot) \times \alpha \times (time() - 60)$$

Лінійне зростання ботів залежить від кількості lom_people та часу після 60 хвилин. Коефіцієнт k_bot визначає частку ботів, а коефіцієнт a відображає розповсюдження інформації від ботів на користувачів соціальної мережі.

Формула для кількості тролів (troll_count):

$$troll\_count = (lom\_people \times k\_troll) \times q \times (time() - 60)$$

Лінійне зростання тролів залежить від кількості lom_people та часу після 60 хвилин. Коефіцієнт k_troll визначає частку ботів, а коефіцієнт q відображає розповсюдження інформації від тролів на користувачів соціальної мережі.

Формула для кількості звичайних користувачів (person_count):

$$person\_count = (lom\_people \times k\_persom) \times b \times (time() - 60)$$

Звичайні користувачі додаються у другій фазі. Коефіцієнт b відображає розповсюдження інформації від звичайних користувачів на користувачів соціальної мережі.

Формула для tal_count:

$$tal\_count = k1 \times Math.log10(0.01 \times (time() - 60) + 1) + tal\_count\_at\_60$$

Логарифмічне зростання продовжується, при цьому додається значення tal_count після 60 хвилин, де початкове значення додається до зростання за логарифмом часу з моменту початку другої фази, що було зафіксовано на момент завершення першої фази.

Етап 3: Зміна впливу поширення від ботів, після завершення попередніх етапів:

Формула для кількості ботів (bot_count):

$$bot\_count = bot\_count + bot\_count \times v$$

Формула для кількості тролів (troll_count):

$$\text{troll\_count} = \text{troll\_count} + \text{troll\_count} \times \text{v}$$

Формула для кількості звичайних користувачів (person_count):

$$person\_count = person\_count + person\_count \times b$$

Після 600 хвилин кількість ботів, тролів та звичайних користувачів зростає експоненціально.

Формула для tal_count:

$$tal\_count = k2 \times Math.log10(0.01 \times (time() - 600) + 1) + tal\_count\_at\_600$$

Логарифмічна функція використовується для продовження зростання tal_count, де базовим значенням є tal_count_at_600 зафіксоване на момент завершення другої фази.

Модель комбінує лінійні та логарифмічні формули для опису поведінки різних типів користувачів на трьох фазах часу. Логарифмічні функції використовуються для моделювання уповільненого зростання tal_count, а лінійні та експоненціальні залежності забезпечують динаміку зростання кількості користувачів, ботів і тролів.

Опис моделі.

В даній моделі отримуємо сценарій розповсюдження інформаційної операції та візуальне відображення впливу різних типів користувачів на розповсюдження інформації (рис. 3.10).

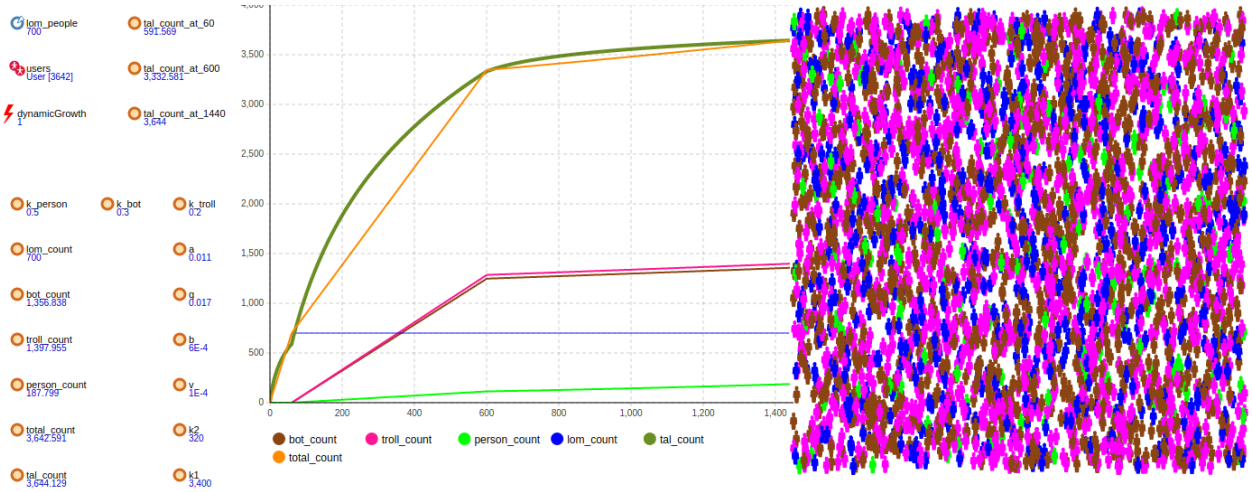

Рисунок 3.10 – Результат моделювання інформаційної операції

bot_count – коричневий колір;

troll_count – рожевий колір;

person_count – лаймовий колір;

lom_count – синій колір;

total_count – помаранчевий колір;

tal_count – зелений колір.

На графіку відображено зростання tal_count, яке відповідає розповсюдженню інформації з часом, також залежності впливу всіх типів агентів, які відіграють безпосередню роль в розповсюдженні інформації. На візуальному відображенні двомірної проекції зображено, який тип агентів має вплив на користувачів соціальної мережі відповідно до їх кольору.

Оскільки імітаційне середовище дає можливість проводити симуляцію в обмежених параметрах, тому вибрано масштабний коефіцієнт 1000, який не впливає на результати дослідження.

Проведено декілька модуляцій з різними початковими параметрами, що дало можливість встановити який параметр є більш значний для поставленого завдання. Код моделі наведено в **Додатку 7**.

В результаті проведених експериментів отримано наступні моделі:

Модель 1: Дана симуляція моделює поведінку розповсюдження проаналізованих постів (Рис. 3.11).

Основні параметри:

lom_people = 700;

k_person = 0.5;

k_bot = 0.3;

k_troll = 0.2.

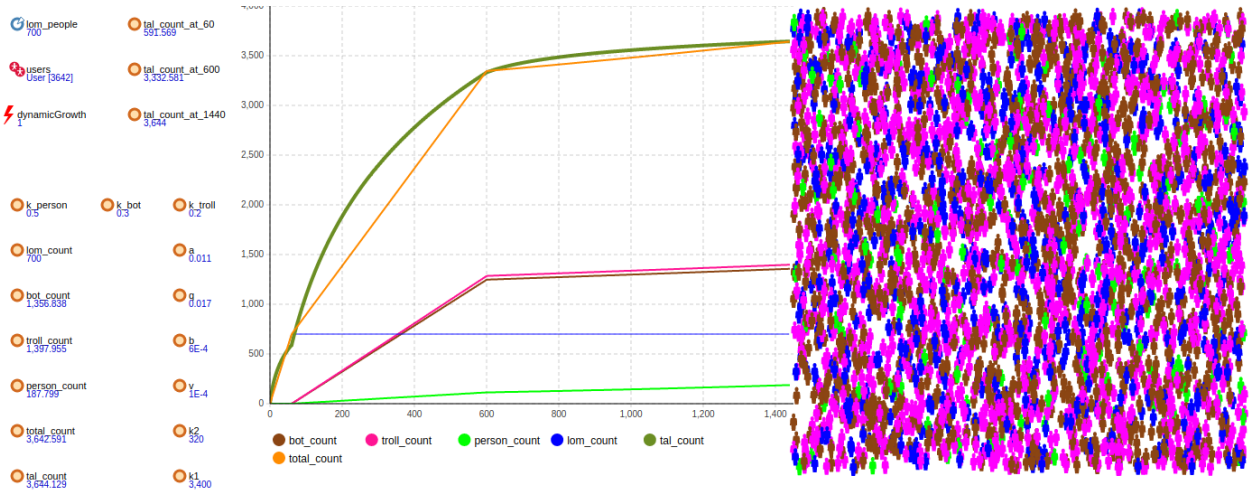

Рис. 3.11 – Результат моделювання_1

Зміни, що відбуваються в моделі: базові параметри – 700 підписників ЛГД, розподіл склав: 50% звичайні користувачі, 30% боти, 20% тролі. Висновок: поширення має збалансований внесок усіх категорій агентів, з помірним впливом ботів і тролів на ранніх етапах.

Модель 2: Дана симуляція моделює поведінку розповсюдження проаналізованих постів, збільшивши кількість підписників ЛГД (рис. 3.12).

Основні параметри:

lom_people = 2000;

k_person = 0.5;

k_bot = 0.3;

k_troll = 0.2.

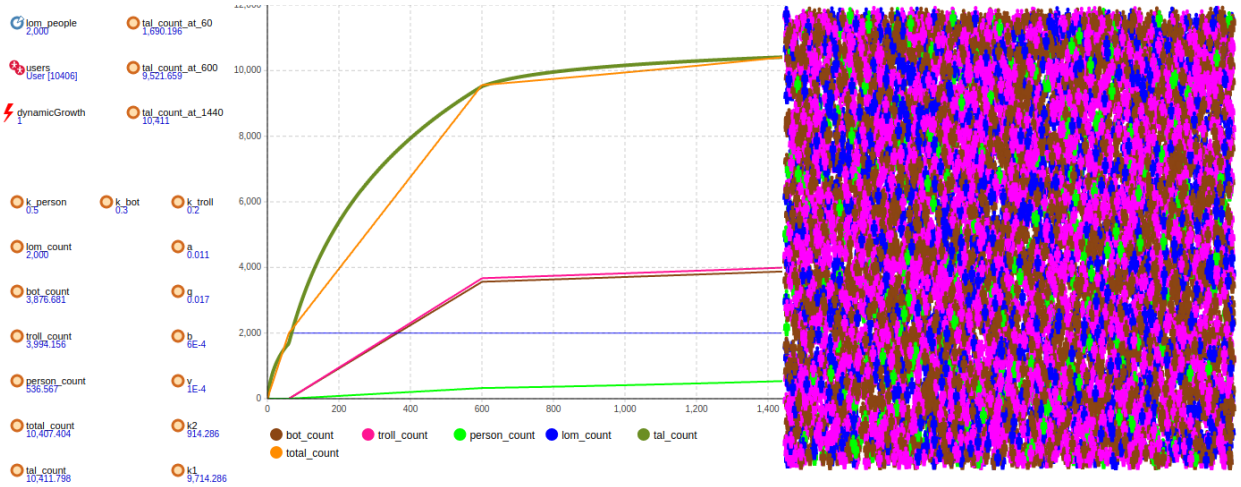

Рисунок 3.12 – Результат моделювання_2

Зміни, що відбуваються в моделі: кількість підписників ЛГД збільшено до 2000, інші показники незмінні. Висновок: значне зростання початкового охоплення, швидший вихід на високі значення total_count, збільшення впливу всіх груп.

Модель 3: Дана симуляція моделює поведінку розповсюдження проаналізованих постів при масштабному коефіцієнті 1000, зменшивши кількість підписників ЛГД (рис. 3.13).

Основні параметри:

lom_people = 200;

k_person = 0.5;

k_bot = 0.3;

k_troll = 0.2.

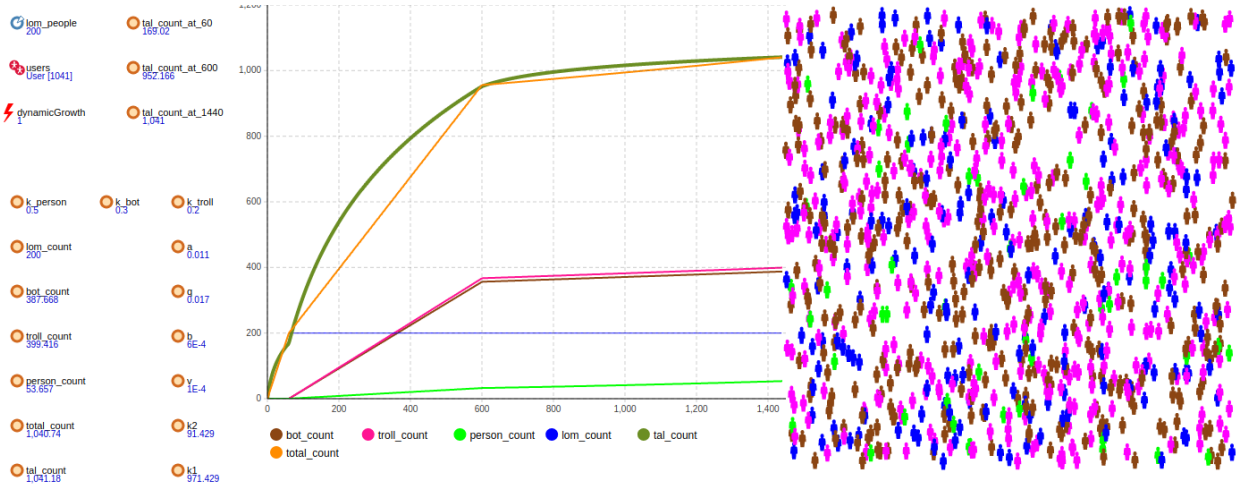

Рисунок 3.13 – Результат моделювання _3

Зміни, що відбуваються в моделі: кількість підписників ЛГД зменшено до 200, інші показники збережені. Висновок: менший старт знижує темпи та масштаби поширення, вплив ботів і тролів стає менш відчутним.

Модель 4: Дана симуляція моделює поведінку розповсюдження проаналізованих постів при масштабному коефіцієнті 1000, змінивши відношення кількості ботів і тролів (рис. 3.14).

Основні параметри:

lom_people = 700;

k_person = 0.5;

k_bot = 0.1;

k_troll = 0.4.

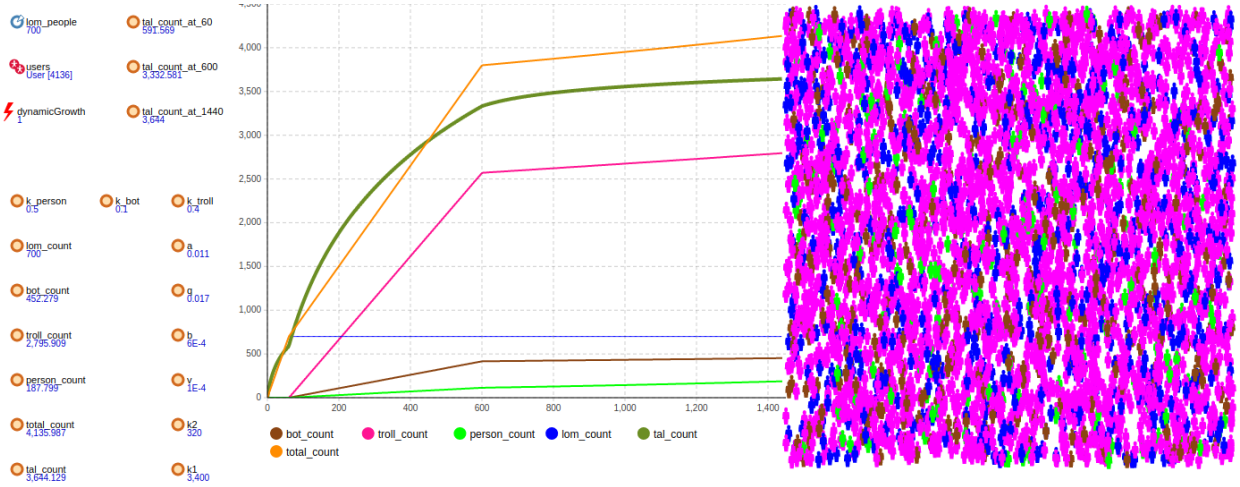

Рисунок 3.14 – Результат моделювання _4

Зміни, що відбуваються в моделі: зменшено частку ботів до 10% та збільшено частку тролів до 40%. Висновок: поширення більше зумовлене маніпулятивним впливом тролів, менший автоматизований вплив ботів.

Модель 5: Дана симуляція моделює поведінку розповсюдження проаналізованих постів при масштабному коефіцієнті 1000, змінивши відношення кількості ботів і тролів (Рис. 3.15).

Основні параметри:

lom_people = 700;

k_person = 0.5;

k_bot = 0.4;

k_troll = 0.1.

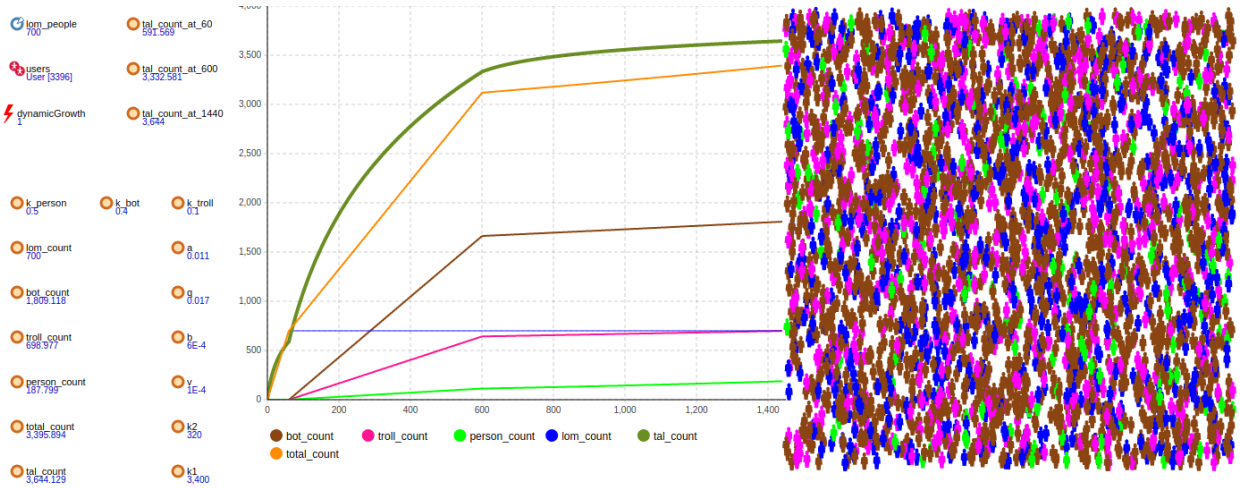

Рисунок 3.15 – Результат моделювання_5

Зміни, що відбуваються в моделі: збільшено частку ботів до 40%, зменшено частку тролів до 10%. Висновок: автоматизоване поширення пришвидшується, тролі мають мінімальний вплив, хвиля поширення коротша, але інтенсивніша.

Модель 6: Дана симуляція моделює поведінку розповсюдження проаналізованих постів при масштабному коефіцієнті 1000, змінивши відношення кількості ботів і тролів та звичайних користувачів (Рис. 3.16).

Основні параметри:

lom_people = 700;

k_person = 0.8;

k_bot = 0.1;

k_troll = 0.1.

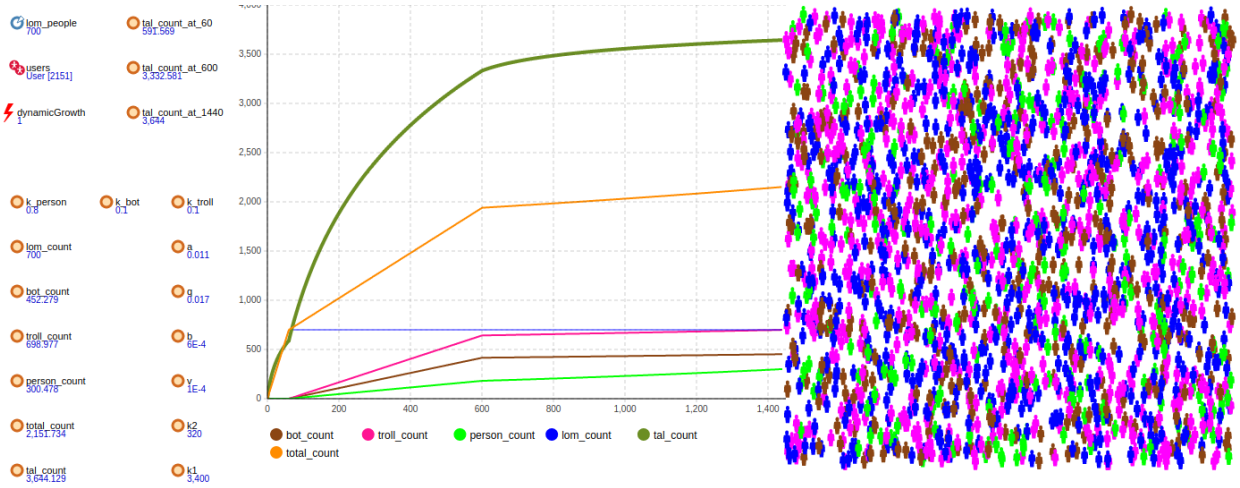

Рисунок 3.16 – Результат моделювання_6

Зміни, що відбуваються в моделі: збільшено частку звичайних користувачів до 80%, боти та тролі по 10%. Висновок: основний тягар поширення переходить до звичайних користувачів, що забезпечує більш природний і стабільний ріст охоплення.

Модель 7: Дана симуляція моделює поведінку розповсюдження проаналізованих постів при масштабному коефіцієнті 1000, при відсутності ботів та тролів (рис. 3.17).

Основні параметри:

lom_people = 700;

k_person = 1;

k_bot = 0;

k_troll = 0.

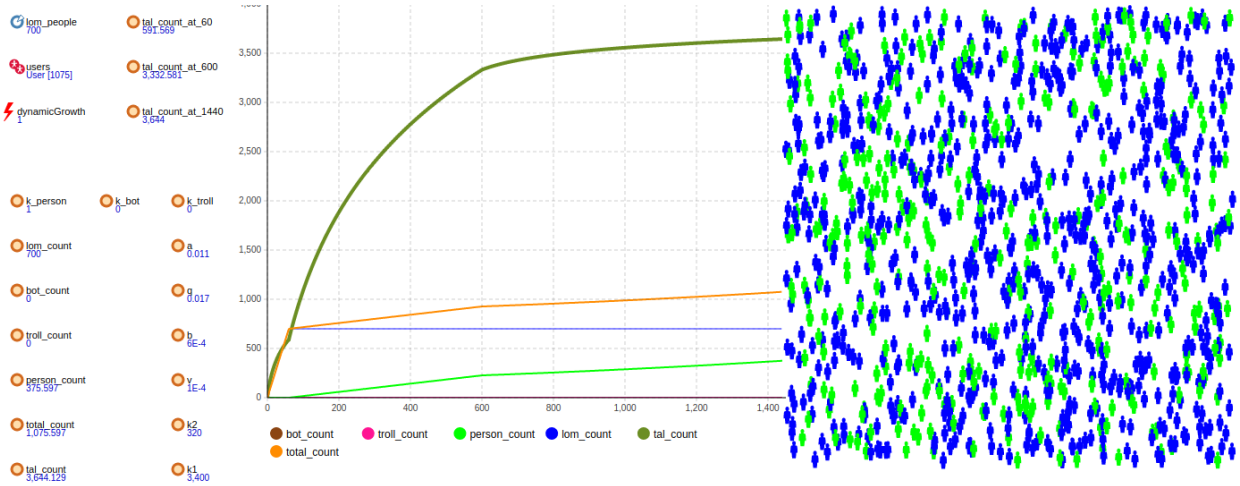

Рисунок 3.17 – Результат моделювання_7

Зміни, що відбуваються в моделі: відсутні боти та тролі, лише 100% звичайних користувачів. Висновок: поширення відбувається виключно органічним шляхом, темпи зростання повільніші, але довготривалі.

3.4. Обробка результатів імітаційних експериментів

Проаналізувавши моделі, отримані шляхом ряду імітаційних експериментів, можемо зробити наступні висновки.

Імітаційна модель з одним типом агентів, які мають однакові властивості та є звичайними користувачами, тобто потенційною цільовою аудиторією, яку використовують в проведенні інформаційних операцій, виявила такі залежності:

1) чим швидше йде розповсюдження (сплеск) інформації, тим швидше затухання;

2) основні параметри впливу average-node-degree та initial-outbreak-size: average-node-degree – чим більше зв'язків, тим швидше розповсюдження, initial-outbreak-size – в залежності від кількості зв'язків, втрата інтересу до інформації досить швидка;

3) якщо значення параметрів average-node-degree та initial-outbreak-size низькі, а значення параметру gain-resistance-chance достатньо високий, тоді інформація може не дійти до більшості зацікавлених користувачів.

Імітаційна модель на основі чотирьох типів агентів враховує різні стадії інформаційної операції та залучення агентів з різними характеристиками, тобто враховує діяльність першоджерел та так званих «каталізаторів» поширення інформаційного впливу в соціальній мережі. Після аналізу ряду постів було виявлено та обраховано певні закономірності, за результатами яких було проведено симуляції інформаційних операцій. На основі проведених симуляцій спостерігаємо вплив різних категорій та їх поведінку при розповсюдженні інформації в соціальній мережі X за добу (1440 хв.). Число ботів, тролів і звичайних користувачів обчислюється згідно з кількістю підписників та пов'язано з показником tal_count, де tal_count – логарифмічний показник успішної інформаційної операції, а порівняння показника tal_count з total_count дає змогу визначити її успішність. Таким чином спостерігаємо, що вплив тролів є найбільшим – при відсутності ботів та тролів або їх недостатній кількості ефективність інформаційної операції є низькою. Результати експерименту дають можливість оцінити операції по розповсюдженню інформації в соціальній мережі X.

3.5. Інформаційна технологія виявлення інформаційних операцій у соціальних мережах.

У результаті проведеного дослідження було створено інформаційну технологію, яка поєднує концептуальні, математичні та алгоритмічні підходи для моделювання та виявлення інформаційних операцій у соціальних мережах. Зокрема:

Сформовано класифікацію агентів, що діють у соціальних мережах, з виділенням чотирьох основних типів: звичайні користувачі, боти, тролі та лідери громадської думки, із визначенням їхніх метричних характеристик, таких як індекс активності, ступінь впливу, рівень мережевої центральності тощо.

Розроблено математичні моделі кожного типу агентів, у яких враховано коефіцієнт впливу як динамічний параметр, що визначає здатність агента поширювати інформацію в межах мережі. Ці моделі реалізовано в рамках агентного моделювання, що дозволяє відтворити процеси поширення контенту та вивчати поведінку інформаційних операцій.

Запропоновано комбінований метод оптимізації поведінки агентів та виявлення ключових структур, який реалізовано на основі інтеграції кількох алгоритмів із чітким визначенням їхньої ролі в загальній архітектурі технології:

Influence Maximization – використовується для визначення найбільш впливових агентів (інфлюенсерів), чия активність має потенціал для максимального охоплення інформаційним впливом у мережі. Цей компонент критично важливий для виявлення первинних вузлів поширення ІО.

Метод Монте-Карло (MCMC) – застосовується для моделювання ймовірнісної поведінки агентів в умовах інформаційної невизначеності, а також для оцінки потенційних сценаріїв розвитку інформаційної кампанії.

Цей підхід забезпечує стохастичну варіативність моделі, що наближає її до реального інформаційного середовища.

Генетичні алгоритми – впроваджуються як інструмент еволюційної стратегії впливу, зокрема для підбору параметрів агентів або виявлення ефективних комбінацій для поширення контенту. Вони забезпечують адаптивність системи до змін у мережевому середовищі.

Louvain clustering – використовується для виявлення спільнот (кластерів) у соціальній мережі, що дозволяє сегментувати аудиторію за принципом близькості, подібності або спільної поведінки. Це дає змогу таргетувати інформаційний вплив більш прицільно та ефективно, підвищуючи точність і результативність ІО.

Сформовано мультимодальну модель інформаційної операції, яка враховує різні типи інформаційного впливу (текст, візуальні матеріали, відео, емоційні тригери тощо) та особливості перетину каналів комунікації, що відповідає реальним умовам функціонування ІО у цифровому просторі.

На основі вищевикладеного можна стверджувати, що розроблена екосистема являє собою основу інформаційної технології для виявлення інформаційних операцій у соціальних мережах, а також для їхнього аналізу, моделювання та організації подальшої протидії. Вона забезпечує як симуляційне вивчення динаміки ІО, так і виявлення структурних та функціональних характеристик ворожих кампаній, що відкриває перспективи для її практичного використання в системах кіберзахисту, моніторингу інформаційного простору та підтримки рішень у сфері інформаційної безпеки (Рисунок 3.18).

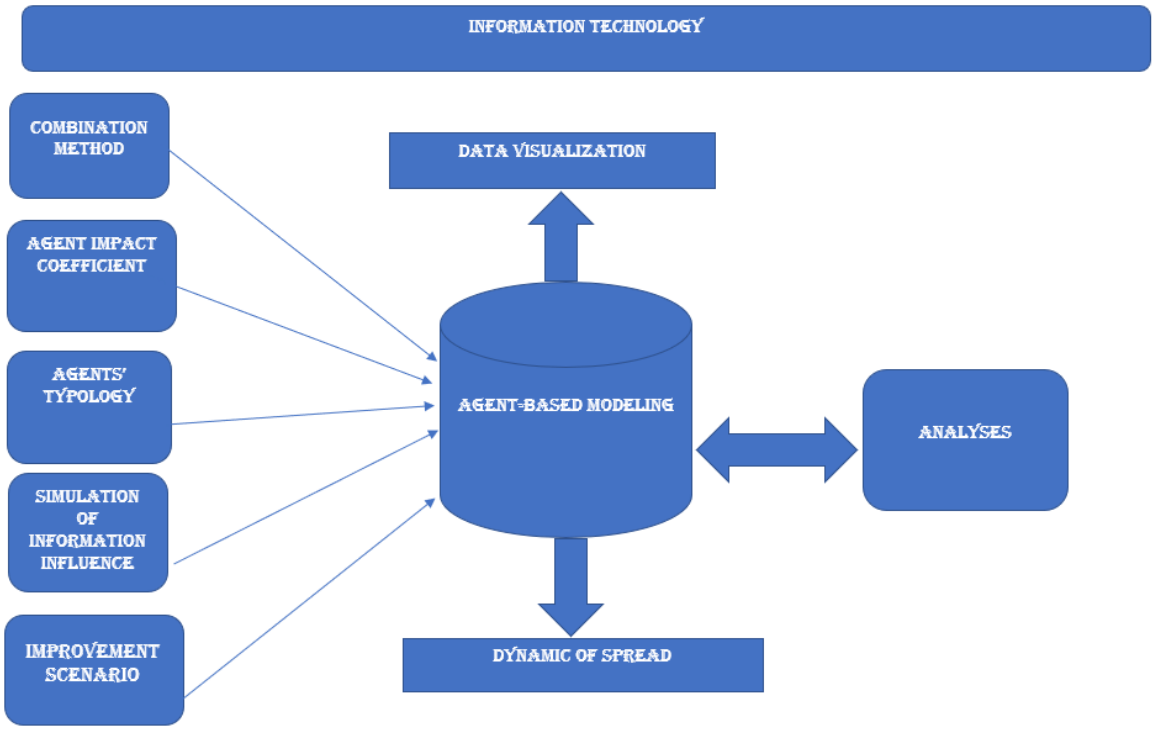

Рис. 3.18 Інформаційна технологія виявлення інформаційним операціям

Ключовими ознаками, що дозволяють вважати результати дослідження інформаційною технологією є:

1. Агентна модель виявлення інформаційних операцій в соціальних мережах включає чотири типи агентів (звичайні користувачі, боти, тролі та лідери громадської думки), які мають різну вагу впливу. Для кожного типу агентів визначено математичну модель, що відображає їхню участь у поширенні контенту.
2. Результати моделювання з одним типом агентів (тільки звичайні користувачі) показали такі закономірності:
   - Швидкий сплеск інформації веде до її швидкого згасання.
   - Параметри *average-node-degree* та *initial-outbreak-size* суттєво впливають на охоплення аудиторії.
   - За низьких значень цих параметрів та високого *gain-resistance-chance*, інформація не охоплює критичну масу користувачів.

3. Результати моделювання з чотирма типами агентів дозволили оцінити динаміку інформаційного впливу в реалістичнішому середовищі. Було створено і протестовано модель, яка включає близько 20 параметрів, таких як *lom_people*, *k_bot*, *k_person*, *tal_count*, *dynamicGrowth* тощо, що дозволяє моделювати багатофазну структуру інформаційних операцій. Було встановлено агентів з найбільшим впливом – тролів та ботів, а за відсутності яких ефективність інформаційних операцій значно зменшується.
4. Алгоритмічне ядро нової інформаційної технології включає інтеграцію комплексного методу:
    - Influence Maximization: визначення ключових агентів-інфлюенсерів.
    - MCMC: моделювання прийняття рішень з урахуванням невизначеності.
    - Генетичні алгоритми: покращення стратегій впливу.
    - Louvain: виявлення спільнот для таргетування.
    - Механізми зворотного зв'язку: адаптація стратегії впливу в реальному часі.

Мультимодальність запропонованої агентної моделі полягає у синтезі кількох підходів до імітаційного моделювання інформаційних операцій у соціальних мережах. У моделі одночасно враховано топологічні характеристики мережевої структури (структурний підхід), індивідуальні поведінкові особливості агентів (агентна парадигма), часову динаміку активності користувачів (динамічний підхід), а також соціальні реакції, що відображаються у зміні моделей взаємодії (соціологічний вимір). Такий комплексний підхід забезпечує високий рівень адекватності моделі для аналізу складних інформаційних процесів і дозволяє відтворювати ключові характеристики реальних інформаційних операцій.

Оцінка ІТ щодо виявлення елементів інформаційної операції.

Дозволяє виявляти типи учасників / акторів ІО в повній мірі за рахунок методу розрахунку коефіцієнту впливу чотирьох типів агентів (звичайні користувачі, боти, тролі, лідери думок). Також забезпечено виявлення впливових вузлів (лідерів думок) за рахунок компоненту Influence Maximization, який виявляє агентів з найбільшим впливом. Симуляційні експерименти моделюють хвилі поширення, включно з параметрами initial-outbreak, що створює можливість відслідковувати динаміку поширення контенту. Компонент Louvain дозволяє виявляти кластери для таргетингу, тобто цільові аудиторії/спільноти. Передбачено зворотний зв'язок та генетичні алгоритми, які задіяні в агентній моделі для адаптивних стратегій**.** Виявлені закономірностей швидкого зростання та згасання контенту (експерименти 1 типу). Враховуються параметри average-node-degree, спільноти, динаміка зв'язків.

В той же час інформаційна технологія не враховує типи контенту та наративи. В моделі не враховується вплив алгоритмів платформ та частково враховується координація дій ключових вузлів (відсутні прямі метрики координації ботів/тролів).

Сильні сторони ІТ:

- чітка ідентифікація агентів впливу та симуляція їхньої ролі;
- моделювання поширення інформації, включаючи ефект «порогу охоплення»;
- виявлення ключових спільнот у мережі для цільового впливу;
- використання зворотного зв'язку та оптимізації;
- аналіз впливу різних сценаріїв активності ботів і тролів на загальну ефективність операції.

Обмеження (можливі напрями розвитку):

- відсутність семантичного рівня (аналіз змісту наративів або фреймів);
- відсутнє врахування алгоритмів платформи, що підсилюють або пригнічують контент;

- обмежена обробка реальних даних (оскільки модель симуляційна).

Оцінка ефективності інформаційної технології щодо виявлення елементів інформаційних операцій у соціальних мережах.

Розроблена інформаційна технологія, що базується на агентному моделюванні, має комплексну архітектуру, реалізовану за модульним принципом, що забезпечує її гарантоздатність: відмова одного компонента (наприклад, модуля класифікації агентів або обробки графів) не призводить до повного виходу з ладу всієї системи. ІТ дозволяє відтворювати ключові характеристики ІО у соціальних мережах. Для оцінки її ефективності доцільно зіставити функціональні можливості ІТ із типовими структурними та динамічними елементами, що є характерними для ІО згідно з науковими дослідженнями [10, 12, 14, 15, 18].

На основі синтетичного підходу виокремлено 10 базових елементів інформаційних операцій, які найчастіше моделюються або виявляються у сучасних інформаційних системах. Проведено зіставлення цих елементів із функціональністю створеної ІТ:

Таблиця 3.2

Оцінка відповідності функціональності ІТ елементам ІО

№	Елемент інформаційної операції	Виявляється/моделюється в ІТ	Обґрунтування
1	Типи учасників (боти, тролі, інфлюенсери)	Так	Модель включає 4 типи агентів із різними коефіцієнтами впливу.
2	Виявлення інфлюенсерів	Так	Реалізовано через компонент *Influence Maximization*.
3	Координація дій агентів	Частково	Виявляється через динамічну поведінку, але без явної оцінки синхронності.
4	Динаміка поширення контенту	Так	Симуляційні експерименти першого типу моделюють динаміку охоплення.
5	Виявлення спільнот для таргетування	Так	Використано алгоритм *Louvain* для кластеризації мережі.

6	Семантична природа контенту (наративи, фрейми)	Ні	Наративний рівень не моделюється.
7	Стратегії впливу та адаптація	Так	Адаптивність забезпечується зворотним зв’язком, МСМС, генетичними алгоритмами.
8	Віральність, інформаційні сплески	Так	Зафіксовано короткочасні хвилі поширення інформації.
9	Алгоритмічне підсилення контенту	Ні	Алгоритми соціальних платформ не враховуються.
10	Мережеві ефекти / центральність	Так	Аналізується через параметри average-node-degree та інші метрики.

Таким чином, розроблене рішення є системним продуктом, який поєднує агентне моделювання, мережевий аналіз та симуляційні експерименти.

На основі отриманих результатів можна стверджувати, що сформовано архітектуру інформаційної технології для виявлення інформаційних операцій у соціальних мережах. Ця інформаційна технологія є уніфікованим інструментом для проведення експериментів, побудови симуляцій інформаційних операцій, виявлення ключових акторів впливу, та формування системи стратегічного реагування на основі даних. Технологія має потенціал для прикладного застосування в сфері національної інформаційної безпеки, інформаційної аналітики, стратегічних комунікацій та соціального моделювання.

Висновки до Розділу 3.

1. Проаналізовано середовища для агентного моделювання: здійснено порівняння сильних та слабких сторін, що надало можливість обрати середовища для подальшого створення агентних моделей з одним та чотирма типами агентів. Визначено 7 ключових параметрів, за якими здійснено порівняння обраних середовищ: Free access, Language, Open-source software, GUI,

Learning Curve, Community Support та Advanced Features. За зазначеними параметрами обрано два середовища для створення агентної моделі (NetLogo, AniLogic), які є у вільному доступі, мають високу підтримку спільноти, яка надає допомогу, ресурси та розширення, а також додаткові функції або модулі, які виходять за межі базового агентного моделювання.

2. Створено агентну модель виявлення інформаційних операцій в соціальних мережах. Проведено імітаційні експерименти в двох різних імітаційних середовищах, які демонструють розповсюдження контенту в однорідних та гетерогенних соціальних мережах. Так, досліджено основні показники, які впливають на динаміку поширення при участі тільки одного типу агенту – звичайного користувача, а також динаміку поширення контенту за участі чотирьох типів агентів, які були описані в цьому розділі. Визначена роль кожного типу агенту на зміну динамічних систем з урахуванням зміни їхніх показників впливу, виявлено та обраховано певні закономірності. Результати експерименту дають можливість виявляти інформаційні операції в соціальних мережах.
3. Створено інформаційну технологію, що, на відміну від інших, базується на агентній моделі з чотирма типами агентів, де агентами є різні типи користувачів із врахуванням їхнього коефіцієнту впливу; має комплексну архітектуру, яка дозволяє відтворювати ключові характеристики інформаційних операцій (ІО) у соціальних мережах. На основі синтетичного підходу виокремлено 10 базових елементів інформаційних операцій, які найчастіше моделюються або виявляються у сучасних аналітичних системах. Проведено зіставлення цих елементів із функціональністю створеної ІТ. Описано її сильні сторони та обмеження, що може бути подальшими напрямками досліджень та розвитку ІТ. До сильних

сторін можемо віднести чітку ідентифікацію агентів впливу та симуляцію їхньої ролі, моделювання поширення інформації, включаючи ефект «порогу охоплення», виявлення ключових спільнот у мережі для цільового впливу, використання зворотного зв’язку та аналіз впливу різних сценаріїв активності ботів і тролів на загальну ефективність операції. До обмежень – відсутність семантичного рівня (аналіз змісту наративів або фреймів) та відсутність врахування алгоритмів платформи, що підсилюють або пригнічують контент.

РОЗДІЛ 4. ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В СОЦІАЛЬНИХ МЕРЕЖАХ

У цьому розділі представлено результати впровадження інформаційної технології, що базується комплексному методі виявлення інформаційних операцій, методі розрахунку коефіцієнту впливу агентів та агентній моделі. Інформаційна технологія дозволяє виявляти, моделювати та аналізувати інформаційні операції, які реалізуються через онлайн-платформи шляхом поширення контенту між користувачами різних типів (звичайні користувачі, боти, тролі, лідери думок).

Для проведення реальних експериментів використано моніторингову систему, в якій окремим модулем інтегровано зазначені методи та моделювання.

Для отримання первинних дата-сетів використано систему моніторингу соціальних мереж «CAPSMI» (рис. 4.1.)

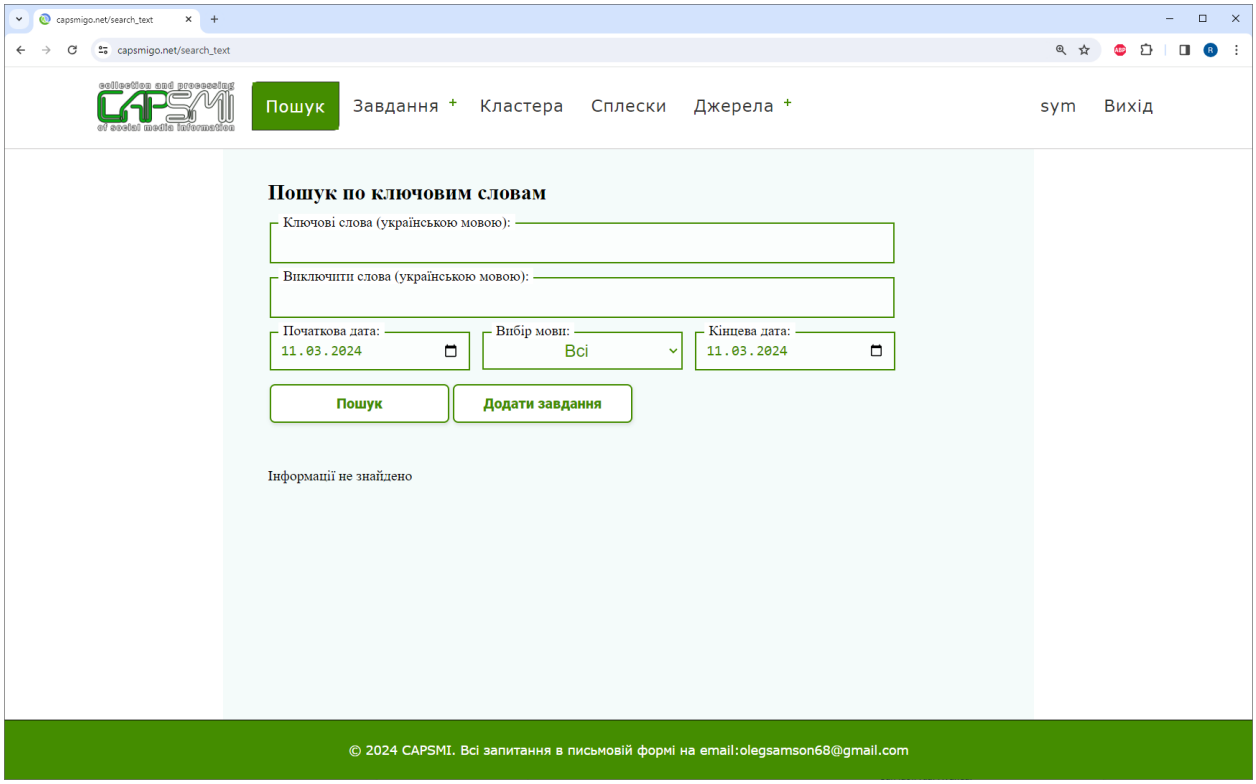

Рисунок 4.1. Інтерфейс моніторингової системи «CAPSMI»

Дана моніторингова система вирішує завдання із пошуку контенту щодо досліджуваної тематики або для отримання актуальної інформації щодо інформаційних сплесків в режимі реального часу із соціальних мереж.

4.1. Формування дата-сетів та первинна обробка даних

З метою забезпечення повноцінного функціонування інформаційної технології, орієнтованої на виявлення інформаційних операцій у соціальних мережах, на початковому етапі було реалізовано модуль збору та збереження контенту, що формує первинний масив даних для подальшого аналізу.

Для зберігання отриманої інформації застосовано реляційну базу даних PostgreSQL. Взаємодія з базою реалізована за допомогою мови програмування Python з використанням ORM (Object-Relational Mapper) Peewee, що дозволяє створювати та визначати структуру таблиць, здійснювати запити та маніпуляції з даними у зручному об'єктно-орієнтованому стилі. Створено основну таблицю бази даних під назвою «1_text», яка акумулює текстовий контент, зібраний із соціальних мереж, із прив’язкою до метаінформації, що має аналітичну цінність для дослідження динаміки поширення інформації.

Структура таблиці включає такі ключові поля:

- id_text – первинний ключ, який однозначно ідентифікує кожен запис.
- text – текстова частина повідомлення, що є об’єктом контентного аналізу.
- id_lang – ідентифікатор мови повідомлення.
- post_date – дата і час публікації, що дозволяє формувати часові ряди поширення.
- source_id, post_id – ідентифікатори джерела і публікації відповідно.
- parent_text_id – батьківський ідентифікатор, дозволяє будувати деревоподібні структури (наприклад, коментарі до оригінального посту).

- source, type – тип джерела та категорія контенту (наприклад, допис, коментар, репост).
- Метрики взаємодії (views, likes, comments, reposts) – ключові показники соціальної активності, які використовуються при оцінці впливу.

Також передбачено поле update_at для фіксації моменту останнього оновлення запису. Для забезпечення цілісності даних реалізовано індексацію за комбінацією полів source_id та post_id, що дозволяє уникати дублювання контенту при багаторазовому зборі з одного джерела.

Ця структура є основою формування дата-сетів для подальших обчислювальних експериментів, зокрема для навчання моделей, виявлення аномалій, побудови мережевих графів взаємодії та тестування алгоритмів інформаційного впливу (рис. 4.2).

class **A_texts**(BaseModel):

```
class A_texts(BaseModel):
    id_text = PrimaryKeyField(null=False)
    text = TextField(null=True)
    id_lang = IntegerField(null=False)
    post_date = DateTimeField(default=datetime.datetime.now, index=True)
    source_id = BigIntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    post_id = BigIntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    parent_text_id = BigIntegerField(
        index=True, null=True, constraints=[SQL("DEFAULT 0")]
    )
    source = IntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    type = IntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    update_at = DateTimeField(default=datetime.datetime.now())
    views = IntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    likes = IntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    comments = IntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    reposts = IntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])

    class Meta:
        db_table = "1_text"
        indexes = ((("source_id", "post_id"), True),)
```

Рисунок 4.2. – Модель бази даних контенту.

4.2. Формування бази даних акаунтів

У рамках системи збору контенту реалізовано окрему таблицю акаунтів «1_sources», яка містить детальну інформацію про джерела публікацій, зокрема ідентифікатори користувачів або акаунтів, що є носіями

інформаційного впливу в соціальних мережах. Ця база виконує функцію довідника метаінформації про облікові записи, що дозволяє ідентифікувати поведінкові та структурні характеристики джерел контенту.

Використання цієї бази даних дає змогу поєднувати інформацію з текстових публікацій із соціальними та технічними атрибутами користувача, що істотно підвищує точність виявлення аномалій, бото- та троль-поведінки, а також інфлюенсерів.

Основні поля таблиці включають:

- id – первинний ключ таблиці.
- id_source – унікальний ідентифікатор джерела (користувача або сторінки).
- name, screen_name – текстові назви акаунта або каналу; використовуються для виводу та ідентифікації джерела у візуалізаціях.
- followers – кількість підписників, що використовується як одна з ключових метрик оцінки рівня впливу джерела.
- favourites – кількість вподобаних публікацій користувача, як індикатор активності.
- friends – кількість взаємодій або підписок, що характеризує ступінь соціальної інтегрованості акаунта.
- last_update_date – дата останнього оновлення профілю; дозволяє фіксувати активність джерела в динаміці.
- last_download_post_id – технічний параметр, що вказує на останнє зібране повідомлення, з метою уникнення дублювання повідомлень при оновленнях.
- status – індикатор активності або валідності джерела в межах системи.
- source – код платформи (наприклад, 1 – Telegram, 2 – Facebook, 3 – X.com), що дає змогу аналізувати мережеву приналежність джерела.

- rules – класифікатор типу агента, що задається на основі обчислень:
    - 0 – звичайний користувач,
    - 1 – лідер громадської думки (ЛГД),
    - 2 – троль,
    - 3 – бот.

Це поле є критичним для подальшого формування агентної моделі, оскільки забезпечує класифікацію агентів в інформаційній технології.

- lang – мова облікового запису; використовується для фільтрації та аналізу контенту за мовними ознаками.

Аналітична роль таблиці бази даних «1_sources» полягає в забезпеченні зв'язку між контентом (таблиця «1_text») та його автором, що дозволяє:

- ідентифікувати авторів інформаційних вкидів,
- аналізувати впливові акаунти за кількісними показниками (followers, activity),
- будувати мережі взаємодії між джерелами та контентом,
- проводити класифікацію акаунтів для включення в агентну модель з відповідним коефіцієнтом впливу.

Таким чином, таблиця «1_sources» формує структурну основу для побудови поведінкової та типологічної моделі агентів у межах всієї інформаційної технології (рис. 4.3.).

```
class A_sources(BaseModel):
    id = PrimaryKeyField(null=False)
    id_source = BigIntegerField(index=True, null=True, constraints=[SQL("DEFAULT 0")])
    name = CharField(max_length=255, index=True, default='')
    screen_name = CharField(max_length=255, index=True, default='')
    followers = BigIntegerField(default=0)
    favourites = BigIntegerField(default=0)
    friends = BigIntegerField (default=0)
    last_update_date = DateTimeField(default=datetime.datetime.now, index=True)
    last_download_post_id = IntegerField(default=0)
    status = IntegerField(default=0)
    source = IntegerField (default=0)
    rules = IntegerField (default=0)
    lang = IntegerField (default=0)

    class Meta:
        db_table = '1_sources'
```

Рис. 4.3. Модель бази даних акаунтів

Ідентифікація типів агентів та визначення коефіцієнта впливу.

Після формування таблиць «1_text» та «1_sources», що акумулюють контентну та структурну інформацію про активність у соціальних мережах, наступним логічним кроком стало застосування методу ідентифікації типів агентів, кожному з яких призначається коефіцієнт впливу, який відображає їхню роль у поширенні інформації в мережі.

Для цього використано поле rules таблиці «1_sources», у якому реалізовано класифікацію агентів згідно з методом, розробленим на основі типових патернів поведінки та мережевих показників. Згідно з цією класифікацією, агенту присвоюється значення від 0 до 3, що відповідає його типу.

Таблиця 4.1.

Значення типів агентів

Значення rules	**Тип агента**	**Характеристика**
0	Звичайний користувач	Обмежений вплив, мінімальна кількість зв’язків, низький рівень взаємодії
1	Лідер громадської думки	Високий авторитет, значна кількість підписників, активна взаємодія

2	Троль	Помітна активність у вигляді коментарів, конфліктогенна риторика
3	Бот	Системна, шаблонна активність; неавтентичні патерни публікацій

Нижче надається візуалізація розподілу агентів за типами, яка ілюструє результати класифікації в БД таблиці «1_sources». Вона демонструє домінування звичайних користувачів, а також присутність специфічних агентів – лідерів думок, тролів і ботів – які відіграють ключову роль у моделюванні інформаційних операцій (рис. 4.4).

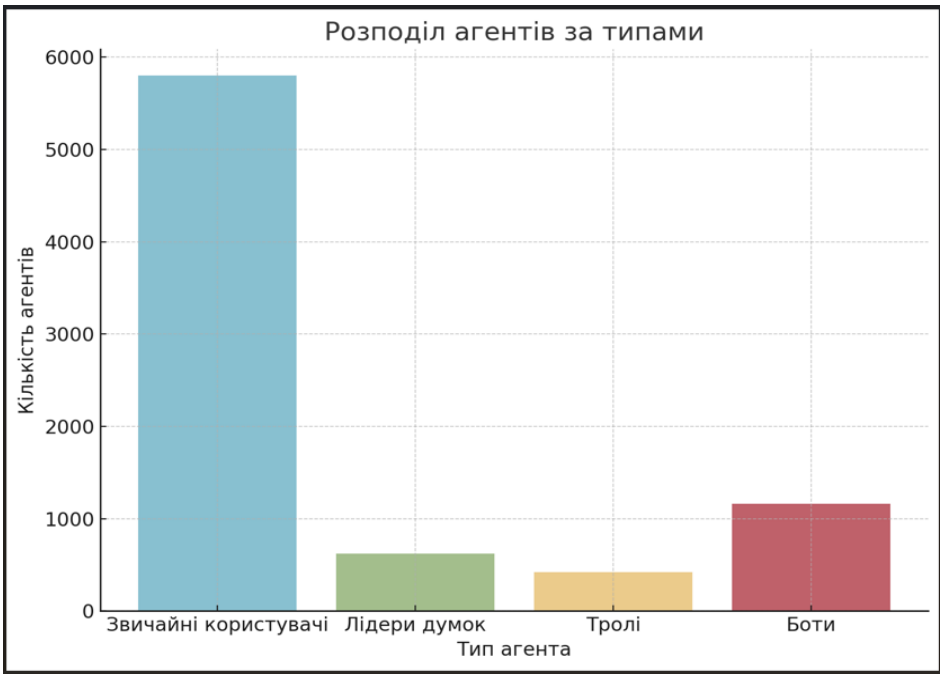

Рисунок 4.4. Розподіл агентів за типами

4.3 Аналіз мережі розповсюдження контенту від лідера громадської думки

Для дослідження характеру поширення інформаційного повідомлення, опублікованого акаунтом типу «лідер (громадської) думки» (ЛГД), було сформовано вибірку підписників і послідовників, які

взаємодіяли з цим постом. Дані сформовано шляхом виконання SQL-запиту, що об’єднує таблиці БД «1_text» і «1_sources», з умовою, що post_id або parent_text_id дорівнюють ідентифікатору базового повідомлення ЛГД (post_id = 194792778407053820) (рис. 4.5).

Ключові параметри стовбців запиту:

- screen_name – ідентифікатор облікового запису користувача (поширювача або коментатора).

- rules – тип агента за шкалою 0–3 (звичайний користувач, ЛГД, троль, бот).

- followers, favourites, friends – числові метрики, які дозволяють оцінити рівень мережевого охоплення і соціальної взаємодії користувача.

- text – вміст поширеного або коментованого повідомлення, що дозволяє виявляти семантичну схожість та узгодженість меседжів.

- post_date – час публікації або реакції на оригінальний пост, що використовується для побудови часових профілів поширення.

- views, likes, comments, reposts – інтерактивні метрики, що дозволяють оцінити ступінь зворотного зв’язку й загальне охоплення повідомлення.

Query Query History

```
1  SELECT T2.screen_name, T2.rules, T2.followers, T2.favourites,T2.friends, T1.text, T1.post_date, T1.views, T1.likes,T1.comments, t1.reposts
2  FROM public."1_text" AS T1 INNER JOIN public."1_sources" AS T2 ON T1.source_id = T2.id_source
3  WHERE post_id = 1947927784007053820
4  UNION
5  SELECT T2.screen_name, T2.rules, T2.followers, T2.favourites,T2.friends, T1.text, T1.post_date, T1.views, T1.likes,T1.comments, t1.reposts
6  FROM public."1_text" AS T1 INNER JOIN public."1_sources" AS T2 ON T1.source_id = T2.id_source
7  WHERE parent_text_id = 1947927784007053820
```

ata output Messages Notifications

	screen_name character varying (255)	rules integer	followers bigint	favourites bigint	friends bigint	text text	post_date timestamp without time zone	views integer	likes integer	comments integer	reposts integer
4	Candace Carboni	3	2492	28285	7502	@MyLordBebo Speaking of genocide	2025-07-23 18:11:42	22	0	0	0
5	Karen	0	873	5821	609	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	873	0	0	0
6	Mustafa Akkilic	0	200	44075	853	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	200	0	0	0
7	MTG	0	206	20923	650	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	206	0	0	0
8	🇹🇴🇲 寿	0	2188	394962	4439	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	2188	0	0	0
9	Mr.Limping	0	571	23114	1005	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	571	0	0	0
0	天鹭城	0	567	40698	645	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	567	0	0	0
1	Rehman Khalid	0	364	27456	590	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	364	0	0	0
2	silvain	3	141	24094	1227	@MyLordBebo Just remember that if the proc...	2025-07-23 11:10:23	148	1	0	0
3	Seroga 🐐	3	23	4401	67	@MyLordBebo Zelensky dictator	2025-07-23 11:33:32	92	1	1	0
4	Gatis Brediks	3	72	1651	126	@MyLordBebo They are free people and they c...	2025-07-23 12:48:42	90	1	0	0
5	Talidari	0	72	957	2	@MyLordBebo devil? Guess they didn't get the...	2025-07-23 22:27:32	15	1	0	0
6	RvE	3	270	8118	716	@MyLordBebo Now the right translation, pleas...	2025-07-23 11:02:59	132	2	0	0
7	Grammar Killer	3	29	3708	17	@MyLordBebo I don't buy these protests, they ...	2025-07-23 11:05:12	388	2	1	1
8	The Political Poet	0	314	200	169	@MyLordBebo It is insane what is happening i...	2025-07-23 11:00:34	308	3	2	0
9	DQ 🛵🛵🌀🏌	3	12669	354108	7670	@MyLordBebo Is Lord Bobo lying about transl...	2025-07-23 14:03:46	70	3	1	0
0	Bob Bear	3	254	4065	458	@MyLordBebo now they see it?... after the jun...	2025-07-23 11:06:09	143	3	0	0
1	CHECK OUT THE TAVİSTOCK İNSTİTUTE	3	934	5972	361	@MyLordBebo Yes, Zelensky, the revolution is ...	2025-07-23 12:42:02	184	4	1	0
2	Tapio Ylipuranen	3	3261	62175	1914	@MyLordBebo Russian propaganda	2025-07-23 12:57:17	188	4	1	1
3	Lord Bebo	1	691234	30349	268	"Zelensky is the devil" – Ukrainian protesto...	2025-07-23 10:52:29	26603	973	49	257

Рисунок 4.5. Вибірка підписників та послідовників ЛГД

Аналітичні висновки:

Повідомлення було репліковано щонайменше 20 різними обліковими записами, з яких частина має ознаки ботів (низький рівень підписників і високий рівень автоматизованої активності).

Зміст переважної більшості реакцій ідентичний або близький до оригінального повідомлення, що свідчить про координоване поширення меседжу з однаковим наративом – у даному випадку, спрямованим на дискредитацію політичного лідера.

Виявлено кілька ключових облікових записів, що мають значну кількість підписників (понад 100 тис., наприклад, GEROMAN – time will tell з 301,199 підписниками), що потенційно є вторинним ЛГД.

Більшість реакцій зосереджені протягом короткого проміжку часу (інтервал до 1 години), що вказує на віральний характер поширення (рис. 4.6).

Рис. 4.6. Фрагмент хронології реакцій на контент

Формування такої бази даних дозволяє кількісно описати охоплення інформаційної операції, побудувати графи взаємодій, виявити вузли впливу та оцінити ступінь когерентності інформаційного наративу в мережі. Отримані дані також можуть бути використані для класифікації агентів на основі поведінкових ознак, застосування кластеризаційних алгоритмів, а також візуалізації каскаду поширення контенту.

На основі обробки метаданих з таблиць БД «1_text» і «1_sources», а також візуального аналізу даних, було сформовано вибірку активності користувачів, які поширили або відреагували на пост, опублікований ЛГД. Для кожного користувача обчислено індекс взаємодії як суму трьох основних метрик: likes, comments, reposts (рис. 4.7).

```
1  SELECT screen_name, followers,favourites, friends,rules FROM public."1_sources" WHERE source=3 and status =1
```

Data output | Messages | Notifications

	screen_name character varying (255)	followers bigint	favourites bigint	friends bigint	rules integer
1	Lord Bebo	691234	30349	268	1
2	-- GEROMAN -- time will tell - 👀 --	301199	677794	3219	1
3	Polak Potrafi	43998	41719	45760	2
4	酒本正夫	27374	152583	861	2
5	Frontier Art	20701	67212	22113	2
6	Grok 4 Game Coding	19786	8861	389	2
7	Doodles 🇺🇸🐕	19767	1148998	13172	2
8	Lee is back	17106	713993	16840	2
9	Patria Grande	15650	964	15848	2
10	DQ 🚲🚲🌍🎖️	12669	354108	7670	3
11	Denis Z 🇷🇺	10545	157261	9756	2
12	Hermann	10452	281690	3726	2
13	Suse🦋🇩🇪🦋❎	9506	533531	8066	2
14	Sunshine Sunnybunz	7315	46737	4557	2
15	De opiniemaker	7220	13813	1272	2
16	Брат Иоанн ☦ 🇷🇺	5904	130267	2819	2
17	BlokkiMedia	5518	2921	1517	2
18	WPR	4803	29511	6721	3
19	Total	4771	1040878	2025	2
20	New Joseph World	4432	28068	6328	2
21	O PLANETA DOS MACACOS (1968)	4103	133510	3883	2

Рисунок 4.7. – Вибірка активності користувачів

На основі параметрів followers, favourites, friends та класифікаційного індексу rules було побудовано вибірку акаунтів з джерела X (відповідно до source=3), які мають активний статус (status=1). Ця вибірка охоплює представників трьох типів агентів**:**

- Лідери думок (rules=1) – акаунти з високим охопленням і стійкою присутністю в мережі;
- Тролі (rules=2) – часто активні, з великим числом реакцій і друзів, однак з підозрілою динамікою поведінки;
- Боти (rules=3) – акаунти з автоматизованими характеристиками, зокрема типовими патернами «підписки-без підписників» або надвисокою кількістю лайків.

Таблиця 4.2.

Структура даних та характеристика ролей агентів

Тип агента	Кількість	Характерні ознаки (за БД)
ЛГД (rules = 1)	2 акаунти (Lord Bebo, GEROMAN)	Від 300 тис. підписників, потужна база вподобань

Тролі (rules = 2)	29 акаунтів	Значна активність, високе співвідношення «favourites/followers», часто багатомовні
Боти (rules = 3)	26 акаунтів	Низький рівень друзів, нестандартні імена, автоматизовані дії

Аналітичні висновки.

Lord Bebo і -- GEROMAN -- демонструють високий рівень охоплення (691,234 і 301,199 підписників відповідно) та є ключовими ЛГД у вибірці.

Більшість акаунтів мають ознаки когерентної поведінки: схожі вподобання, однотипні зв'язки, специфічну часову активність.

Тролі, такі як Patria Grande, Lee is back, Doodles тощо, мають величезну кількість уподобань (до 1 млн), що вказує на високу емоційну або маніпулятивну залученість.

Акаунти з правилами 3 (наприклад, WPR і DQ) демонструють автоматизовану поведінку, що типово для бот-мереж, орієнтованих на посилення інформаційних повідомлень.

На графіку хронології реакцій спостерігається пікове навантаження у вузькому часовому вікні (10:52–11:03), що підтверджує віральну природу поширення контенту. Подібна концентрація активності є типовою для скоординованих інформаційних вкидів.

Таблиця 4.3.

Топ-3 користувачів за індексом взаємодії

Користувач	Followers	Likes
Lord Bebo	691,234	973
Bob Bear	1560	2
Tapio	320	4

Лідером впливу очікувано виступає сам акаунт ЛГД – Lord Bebo, що зібрав понад 1200 одиниць взаємодії. Решта користувачів мають порівняно низькі показники, що вказує на централізований характер джерела впливу.

Загальне охоплення аудиторії поста (тобто сумарна кількість підписників усіх користувачів, які лайкнули, прокоментували або поширили повідомлення) становила 991000 користувачів.

Ця вибірка є основою для:

формування агентного шару моделі, з чіткою диференціацією типів агентів;

розрахунку коефіцієнтів впливу, залежно від типу агента (наприклад, ЛГД має коефіцієнт 1.0, бот – 0.2);

ініціалізації початкових вузлів у графі поширення контенту в симуляціях;

виявлення аномалій або когерентних операцій у системі моніторингу.

4.4. Інтеграція аналітичних алгоритмів та побудова топології інформаційної операції

Після здобування та структурування даних у таблицях БД «1_text» та «1_sources», наступним кроком було здійснено інтегрування аналітичних алгоритмів, які забезпечують обробку, виявлення аномалій і моделювання інформаційних впливів у соціальних мережах. Для цього було реалізовано окремі програмні модулі, що працюють із зібраними даними у зв’язці з агентною моделлю.

Основні компоненти інтеграції:

- Дані з вибірки «1_text» та «1_sources» передаються до аналітичного ядра, де формуються агенти, яким присвоюються:
  - тип (звичайний користувач / бот / троль / ЛГД) – на основі поля rules;
  - індекси активності та впливу – з метаданих (followers, likes, reposts, views);
  - текстова поведінка – з таблиці «1_text».

- Алгоритм Louvain clustering застосовується до взаємозв’язків між джерелами, побудованих за принципом: «джерело *A* взаємодіє з джерелом *B*, якщо коментує або поширює його контент».
- Influence Maximization використовується для ідентифікації найбільш значущих агентів у мережі – з урахуванням динаміки поширення інформації та історії взаємодій.
- MCMC-моделювання виконується для прогнозування ймовірнісних сценаріїв розвитку інформаційної кампанії в умовах невизначеності даних або неповного охоплення.
- Генетичні алгоритми дозволяють покращити структуру взаємодії агентів та налаштування моделі (наприклад, порогів передачі інформації, рівня довіри, реакцій на меседж).

Інтеграція комплексного методу реалізована у вигляді модульної обчислювальної системи, що дозволяє масштабувати модель відповідно до обсягу даних і характеру дослідження.

Формування структури агентів для симуляцій

Для моделювання ІО в соціальних мережах кожен обліковий запис із таблиці 1_sources інтерпретується як агент із набором властивостей:

Таблиця 4.4

Атрибут агента	Джерело	Призначення в моделі
agent_id	id_source	Унікальний ідентифікатор
agent_type	rules	Тип агента (0–3)
followers	followers	Коефіцієнт охоплення
activity	likes, comments, reposts (агреговано)	Визначає частоту участі в ІО
language	lang	Визначає цільову аудиторію
platform	source	Дає змогу враховувати особливості платформи

content	Зв'язок через post_id в 1_text	Формує поведінковий профіль агента

Наступним етапом функціонування системи моніторингу є аналіз поширення окремих інформаційних повідомлень, ініційованих ключовими агентами – зокрема, лідерами громадської думки (ЛГД). Використовуючи створені таблиці «1_text» та «1_sources», система дозволяє автоматично ідентифікувати пости, що були опубліковані акаунтами з параметром rules = 1, тобто класифікованими як ЛГД.

Для кожного такого повідомлення система виконує такі аналітичні кроки:

1. Визначення первинного поста від ЛГМ за параметром post_id у таблиці 1_text.
2. Ідентифікація поширення повідомлення шляхом виявлення:
    - репостів або коментарів із відповідним parent_text_id,
    - користувачів, які здійснили ці дії,
    - подальших реакцій (лайки, коментарі, поширення) на дочірні пости.
3. Агрегація реакцій користувачів, які включають:
    - загальну кількість лайків (likes) – як індикатор позитивного зворотного зв’язку;
    - репости – як тригери подальшого каскаду поширення;
    - коментарі – як індикатор когнітивної залученості аудиторії.

Ця логіка дозволяє розрахувати охоплення інформаційної операції як кількість унікальних користувачів, які взаємодіяли з повідомленням напряму чи опосередковано. При цьому загальна кількість лайків слугує емпіричною мірою зворотного зв’язку аудиторії, що є ключовим фактором у підсиленні вірального ефекту контенту.

На основі зібраних взаємодій побудовано граф поширення інформаційного повідомлення, де:

- вузли відповідають окремим агентам (користувачам),
- ребра – актам взаємодії (репост, лайк, коментар),
- напрямок ребра – вказує, від кого і до кого поширюється вплив.

Побудована топологія дозволяє:

- визначити ключові вузли (hubs) – агентів, через яких проходить найбільша кількість зв’язків, тобто локальних центрів впливу;
- виявити сегментовану цільову аудиторію, яку можна інтерпретувати як кластер впливу на основі спільних реакцій;
- провести оцінку глибини та ширини каскаду поширення, що вказує на ефективність операції у часово-просторовому вимірі.

На рисунках 4.8 а-б представлено структурну топологію поширення конкретного повідомлення, яке було ініційоване акаунтом, ідентифікованим як лідер громадської думки (ЛГД) на основі розробленої агентної моделі. Цей граф був автоматично згенерований модулем в системі моніторингу, де відбувається інтеграція наукових результатів у вигляді:

- класифікації агентів за типами;
- обрахунку коефіцієнтів впливу;
- побудови агентної моделі розповсюдження контенту;
- візуалізації мережевої активності навколо інформаційної операції.

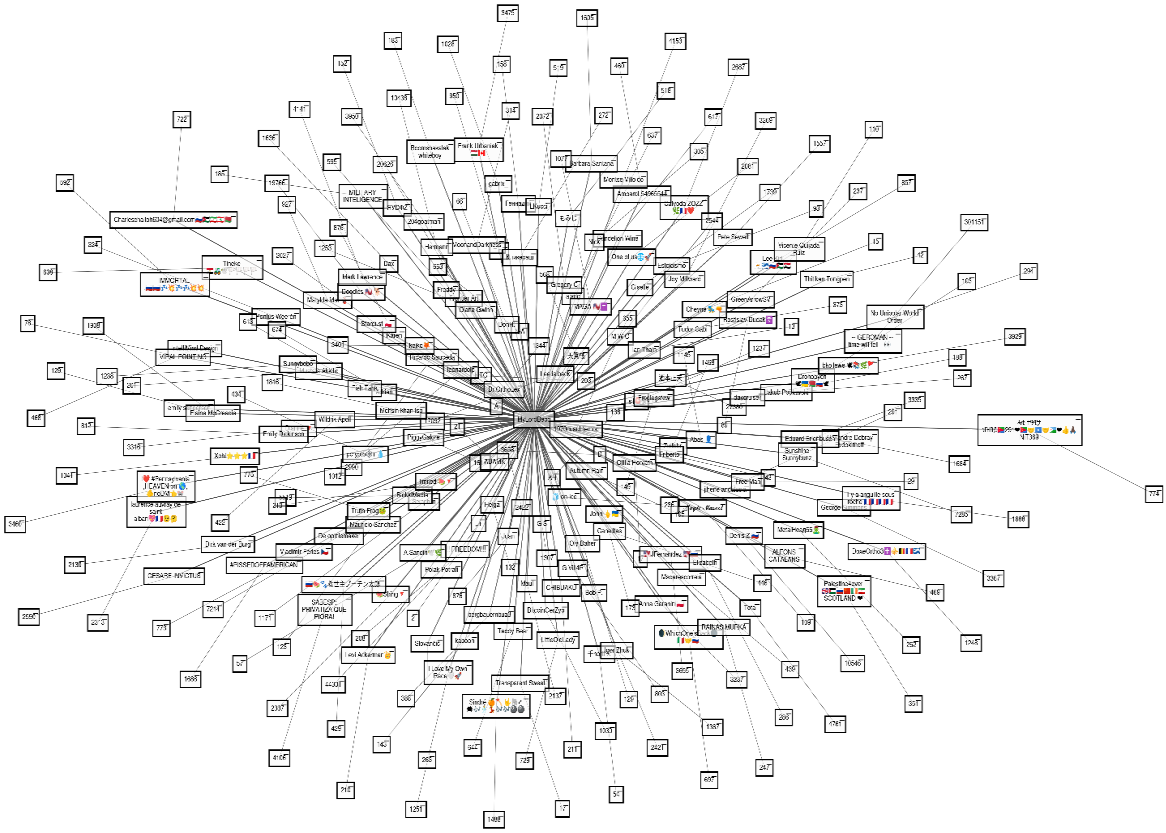

Рисунок 4.8-а. – Структурна топологія поширення повідомлення

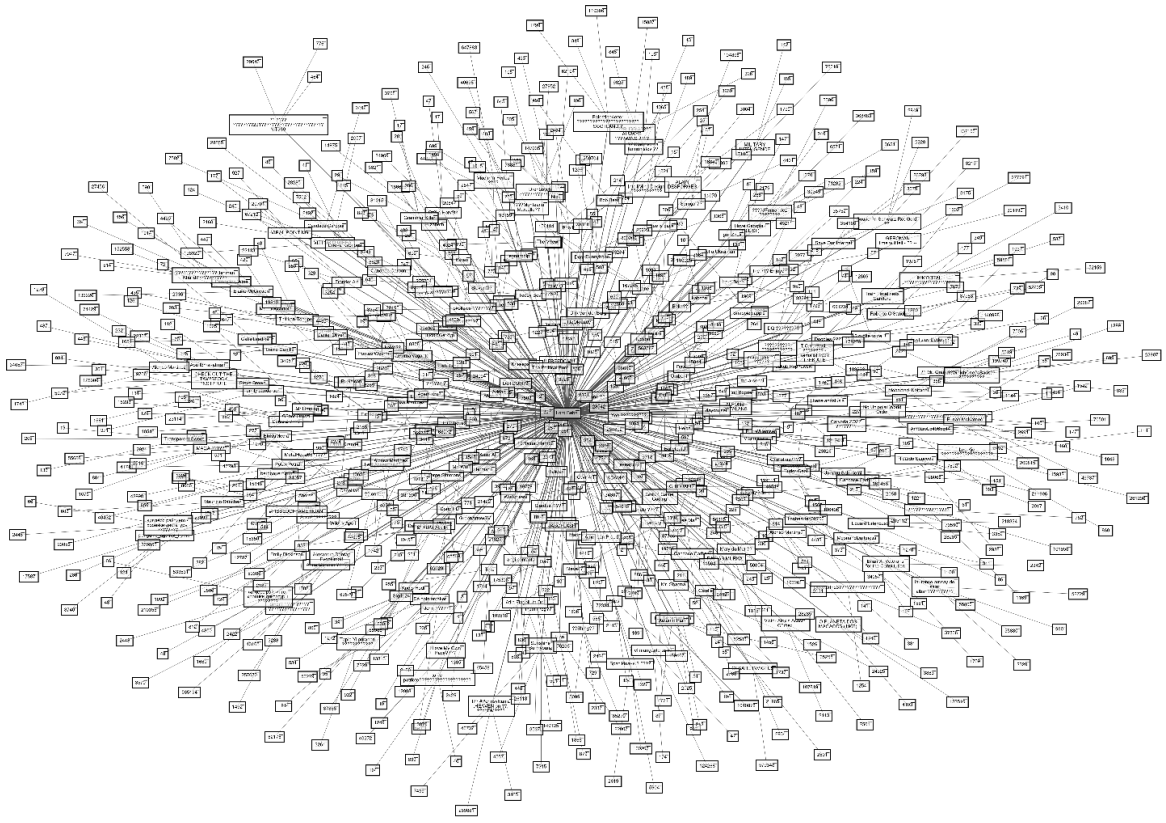

Рисунок 4.8-б. – Структурна топологія поширення повідомлення

Ключові характеристики візуалізованої структури:

- Центральний вузол – акаунт ЛГД, який ініціював повідомлення.
- Вузли першого рівня – прямі поширювачі або взаємодіючі користувачі (репости, лайки, коментарі).
- Вузли другого рівня – користувачі, що взаємодіяли з поширеними копіями повідомлення (вторинне охоплення).
- Ребра – орієнтовані зв’язки передачі інформації (від кого – до кого), які фіксуються в системі моніторингу.

Цей граф є результатом впровадження алгоритму зворотного зв'язку, де агрегуються дії аудиторії (лайки, репости, коментарі), і формується мережа поширення**.**

Модуль використовує ці дані для:

- оцінки впливу повідомлення;
- ідентифікації ключових вузлів за критеріями центральності;
- визначення охоплення цільової аудиторії;
- побудови прогнозу подальшого поширення.

Зв’язок із науковими результатами:

1. Візуалізація реалізована як впровадження агентної моделі інформаційних операцій у реальному середовищі.
2. Кожен вузол містить тип агента (rules), обрахований коефіцієнт впливу та параметри активності (виведені з таблиці «1_sources»).
3. Мережа формувалась на основі даних, зібраних системою моніторингу в БД PostgreSQL за допомогою ORM Peewee, з подальшою обробкою Python-модулями.

Таким чином, система дозволяє не лише фіксувати факт активності ЛГД у межах інформаційної операції, але й кількісно оцінити реакцію аудиторії, побудувати агентні моделі поширення та виявити ключові маршрути трансляції контенту, що є критичним для раннього виявлення ймовірної інформаційної операції.

Висновки до Розділу 4

1. Перевірено працездатність методів та моделі, інтегрованих у інформаційну технологію: реалізовано впровадження агентної моделі, що включає чотири типи агентів із розрахунком коефіцієнтів впливу; протестовано комплексний метод (Influence Maximization, MCMC, Genetic Algorithms, Louvain Clustering) у рамках єдиної технологічної архітектури.
2. Реалізовано метод розрахунку коефіцієнту впливу типів агентів у соціальних мережах на основі метаінформації про акаунти. Метод передбачає врахування визначених параметрів (кількість підписників, уподобань, друзів, активність), що дозволяє класифікувати користувачів на лідерів громадської думки, ботів, тролів і звичайних користувачів, та враховує їхній вплив на розповсюдження контенту. Ідентифікований тип зберігається у відповідному полі rules таблиці БД «1_sources» та використовується в подальшому моделюванні.
3. Протестовано інтеграцію методів у модуль системи моніторингу, зокрема обробку структурованих даних про публікації, їх взаємодії, джерела та користувачів. Це дало змогу формувати агентні структури, виявляти типи агентів та генерувати вхідні дані для симуляцій інформаційних операцій.
4. Отримано в результаті обробки даних:
   - структуру агентної моделі розповсюдження контенту від ЛГД із визначенням ключових вузлів впливу;
   - візуалізацію топології взаємодій користувачів;
   - обчислення загального охоплення (991000 потенційних користувачів);
   - автоматизовану класифікацію акаунтів та виявлення ознак скоординованої активності.

5. Підтверджено прикладну ефективність розробленої інформаційної технології: система дозволяє здійснювати ідентифікацію початкового джерела повідомлення, моделювати його поширення, виявляти цільову аудиторію, розраховувати охоплення та структурувати взаємодії в межах інформаційної операції.

ВИСНОВКИ

1. Проведений аналіз існуючих методів та імітаційних моделей в контексті моделювання інформаційних операцій в соціальних мережах та визначено їхні обмеження інноваційними контекстами, обмеження при аналізі складних взаємодій, забезпеченні реалізації, в передбаченні тривалих процесів, а також складність для опису складних мережевих структур, та неврахування соціального контексту. При цьому показано, що парадигма агентного моделювання дає змогу моделювати складні та багатошарові взаємодії агентів (користувачів), враховуючи їхню поведінку, адаптацію до змін, соціальні впливи та поширення інформації. Запропоновано агентне моделювання як метод імітаційного моделювання для інформаційних операцій в соціальних мережах, який досліджує поведінку децентралізованих автономних агентів. Наведено основні переваги даного методу: будуються сценарії можливих варіантів розвитку подій у майбутньому, на підставі чого формуються, а потім відбираються стратегічні альтернативи, які працюють у кожному сценарії і служать підставою для прийняття рішень про вибір інтегрованої стратегії. Описано основні середовища для побудови імітаційних моделей. Наведені їх переваги та недоліки, здійснено порівняння можливостей. Визначено 7 ключових параметрів, за якими здійснено порівняння обраних середовищ: Free access, Language, Open-source software, GUI, Learning Curve, Community Support та Advanced Features. За зазначеними параметрами обрано два середовища для створення агентної моделі (NetLogo, AniLogic), які є у вільному доступі, мають високу підтримку спільноти, яка надає допомогу, ресурси та розширення, а також додаткові функції або модулі, які виходять за межі базового агентного моделювання.

2. Розроблено комплексний метод, який дає змогу моделювати складні соціальні процеси, розповсюдження інформації та взаємодію агентів. Метод заснований на поєднанні методу поширення впливу (Influence Maximization) для визначення ключових агентів (інфлюенсерів) у соціальній мережі, методу Монте-Карло (MCMC) для моделювання ухвалення рішень агентами, генетичному методі для покращення стратегій агентів у процесі інформаційних операцій, методі виявлення спільнот (Louvain) для ідентифікації спільнот і кластерів усередині соціальної мережі для більш точного моделювання поширення інформації, методі зворотного зв'язку (Feedback Loops) для моделювання динамічних змін у поведінці агентів і поширенні інформації. Застосування всіх п'яти методів у визначеній послідовності дає змогу створити гнучку, адаптивну та динамічну модель, яка здатна імітувати складні процеси інформаційних операцій у соціальних мережах. Ці комбінації створюють можливості для аналізу широкого спектра сценаріїв інформаційних операцій, включно з поширенням дезінформації, впливом лідерів думок, а також динамічною зміною взаємодій усередині соціальної мережі.
3. У межах дослідження запропоновано чотири типи агентів, визначено їхні ключові характеристики, що визначають рівень впливу під час інформаційної операції, який, своєю чергою, є основним критерієм при побудові імітаційної моделі поширення контенту в соціальній мережі. Виведено показники чотирьох типів агентів та визначено коефіцієнт впливу кожного типу агенту. Розроблено методи розрахунку коефіцієнту впливу чотирьох типів агентів на соціальну мережу.

4. Розроблено модель на основі агентного моделювання розповсюдження контенту в соціальних мережах для виявлення інформаційних операцій, проведено симуляційні експерименти в двох різних імітаційних середовищах для моделей з одним типом агентів та для моделей з чотирма типами агентів для виявлення інформаційних операцій в соціальних мережах.
5. Сформовано архітектуру інформаційної технології для виявлення інформаційних операцій у соціальних мережах, що базується на агентному моделюванні, має комплексну архітектуру, яка дозволяє відтворювати ключові характеристики інформаційних операцій (ІО) у соціальних мережах. На основі синтетичного підходу виокремлено 10 базових елементів інформаційних операцій, які найчастіше моделюються або виявляються у сучасних аналітичних системах. Проведено зіставлення цих елементів із функціональністю створеної ІТ. Описано її сильні сторони та обмеження, що може бути подальшими напрямками досліджень та розвитку ІТ.
6. Удосконалено систему моніторингу інформаційних загроз в соціальних мережах шляхом імплементації методу розрахунку коефіцієнту впливу агентів на основі метаінформації акаунтів, реалізовано класифікацію користувачів і забезпечено збереження результатів у базі даних. Інтеграція компонентів у модуль системи моніторингу дозволила обробляти структуровані дані, будувати модель поширення контенту, візуалізувати топологію взаємодій, класифікувати акаунти та виявляти ознаки скоординованої активності. Загальне охоплення інформаційного впливу, згідно з результатами симуляції, становило понад 991 тис. користувачів. Отримані результати підтверджують прикладну ефективність запропонованої інформаційної технології, що забезпечує

виявлення джерел інформаційного впливу, моделювання його розповсюдження, ідентифікацію цільової аудиторії та структуризацію взаємодій у межах інформаційної операції.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Конституція України [Електронний ресурс]. – 1996. – Режим доступу до ресурсу: https://www.president.gov.ua/documents/constitution.

[2] Tunstall T. How social network structure impacts the ability of zealots to promote weak opinions. Phys. Rev. E. 2025. V. 111, N2. 024311. – Режим доступу до ресурсу: https://doi.org/10.1103/PhysRevE.111.024311..

[3] «СТРАТЕГІЯ інформаційної безпеки [Електронний ресурс] – 2020 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/685/2021#n14.

[4] Литвиненко О. В. Інформаційні впливи та операції: теорет.-аналіт. нариси / О. В. Литвиненко. – К. : Нац. ін-т стратегічних досліджень, 2003. – 239 с. – (Сер. Нац. безпека; Вип. 6).

[5] Панченко В. М. Інформаційні операції в системі стратегічних комунікацій, Стратегічні пріоритети. Серія : Політика. 2016. № 4. С. 72-79.

[6] Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. К. : Інтертехнологія, 2009. 164 с.

[7] Панченко В. М. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. Інформація і право. 2014. № 3(12). С. 13-16.

[8] Коваленко Є.В., Плетньов О.В. Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). Київ : Нац. акад. СБУ, 2019. С. 58–59.

[9] Онищенко О. С., Горовий В. М., Попик В. І. та ін. Тенденції впливу глобального інформаційного середовища на соціокультурну сферу. Київ: НАН України: Нац. б-ка України ім. В. І. Вернадського, 2013. 224 с.

[10] Starbird, K. (2019). Disinformation and the unwitting amplifier: Analyzing narratives in the 2016 presidential election. *Harvard Kennedy School Misinformation Review*. Режим доступу до ресурсу: https://doi.org/10.37016/mr-2019-01

[11] Петренко, І. І. (2020). Інформаційні війни: методи та засоби впливу. Інформаційна безпека людини, суспільства, держави, 3(28), 45–52.

[12] Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe report DGI(2017)09. Режим доступу до ресурсу: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[13] Бех, В. П., Дудко, Л. В. (2019). Соціальні мережі як інструмент інформаційної війни: виклики для України. Науковий вісник Міжнародного гуманітарного університету, (38), 89–93. Режим доступу до ресурсу: http://www.vestnik-humanities.mgu.od.ua

[14] Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1-2), 4–37. Режим доступу до ресурсу: https://doi.org/10.1080/01402390.2014.977382

[15] Данько, С. І. (2021). Інформаційні операції в соціальних мережах: механізми реалізації. Інформація і право, (3), 27–33. Режим доступу до ресурсу: https://ipi.org.ua

[16] NATO Strategic Communications Centre of Excellence. (2016). *Social Media as a Tool of Hybrid Warfare*. Режим доступу до ресурсу: https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/119

[17] Prier, J. (2017). Commanding the trend: Social media as information warfare. *Strategic Studies Quarterly*, *11*(4), 50–85. Режим доступу до ресурсу: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf

[18] Лепський, В. Є. (2020). Системна парадигма інформаційної безпеки: концептуальні засади. Збірник наукових праць «Інформація і право», (2), 7–15. Режим доступу до ресурсу: https://ipi.org.ua

[19] Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., ... & Winkelman, Z. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe*. RAND Corporation. Режим доступу до ресурсу: https://www.rand.org/pubs/research_reports/RR2237.html

[20] Durkheim E. Suicide: A Study In Sociology. Free Press: Reissue edition, 1997. 416 p.

[21] Levine D. N. Georg Simmel on Individuality and Social Forms (Heritage of Sociology Series). Chicago : University of Chicago Press, 1972. 412 p.

[22] Spencer H. The man versus the state. Carmel : Liberty Fund Inc.,1982. 550 p.

[23] Moreno J. L. Who Shall Survive? Foundations of Sociometry, Group Psychotherapy and Sociodrama. Boston : Beacon House, 1953. 763 p.

[24] Barnes J. A. Class and committees in a Norwegian Island Parish // Human Relations. –1954. V. 7. – P. 39–58.

[25] Granovetter Mark. Society and Economy: Framework and Principles. Boston : Harvard University Press, 2017. 256 p.

[26] Freeman Linton C. The Development of Social Network Analysis: A Study in the Sociology of Science. New York : Empirical Press, 2004. 218 p.

[27] Burt Ronald S. StructuralHoles: The Social Structure of Competition. - Doson : Harvard University Press. 1995. 323 p.

[28] Галіч Т. О. Соціальні Інтернет-мережі та віртуалізація суспільного життя. Соціологія майбутнього: науковий журнал з проблем соціології молоді та студентства. 2010. Вип. 1. С. 145-152.

[29] Онищенко О., Горовий В., Попик В. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства : монографія. НАН України, Нац. б-ка України ім. В.І. Вернадського. Київ, 2014. 260 с.

[30] Nicole B. Ellison Social Network Sites: Definition, Histori and Scholarship. Available: Режим доступу до ресурсу: https://www.danah.org/papers/JCMCIntro.pdf.

[31] Пінчук О. П. Історико-аналітичний огляд розвитку соціальних мережних технологій і перспектив їх використання у навчанні, Інформаційні технології і засоби навчання, 2015, Том 48, №4 ст.17-19.

[32] Wellman B., Haythornthwaite C. A. The Internet in Everyday Life. Oxford : Blackwell Publishing, 2002, 588 p.

[33] Brass, Daniel J, 'A Social Network Perspective on Human Resources Management', Networks in the Knowledge Economy (New York, 2003; online edn, Oxford Academic, 12 Nov. 2020), Режим доступу до ресурсу: https://doi.org/10.1093/oso/9780195159509.003.0019, accessed 10 Apr. 2025.

[34] Niketna Vivek, Evan Clark Social network analysis as a new tool to measure academic impact of physicians Laryngoscope Investig Otolaryngol 2025 Jan 7;10(1):e70060. doi: 10.1002/lio2.70060

[35] Johan Koskinen, Tom A B Snijders Multilevel longitudinal analysis of social networks Journal of the Royal Statistical Society Series A: Statistics in Society, Volume 186, Issue 3, July 2023, Pages 376–400, https://doi.org/10.1093/jrsssa/qnac009

[36] Introduction to Social Capital Theory, Social Capital Research v1.0 (August 2018). First version published with online course; 51 pages.

[37] Ronald S. Burt, Giuseppe Soda Network Capabilities: Brokerage as a Bridge Between Network Theory and the Resource-Based View of the Firm, Volume 47, Issue 7 https://doi.org/10.1177/0149206320988764

[38] Антибот: як протидія інформаційним маніпуляціям, Інтерньюз Україна, Режим доступу до ресурсу: https://internews.ua/uk/opportunity/antybot-notes.

[39] Российские медики в Италии и «коронавирусная» пропаганда, Голос Америки, [Електронне джерело] – Режим доступу: https://www.golosameriki.com/a/russia-state-media-use-the-medical-convoy-to-italy-for-anti-western-propaganda/5346046.html.

[40] Chi-Jen Lin. Assignment Problem for Team Performance Promotion under Fuzzy Environment // Hindawi Publishing Corporation. Mathematical Problems in Engineering. 2013. 10 p. Available: http://dx.doi.org/10.1155/2013/791415.

[41] Бадризлов В.А., В'язня В.В. Оцінка ефективності поширення інформації в соціальних мережах з використанням імітаційного моделювання // Креативна економіка. - 2018. - Том 12. - №9. - С.1359-1372.

[42] Федонюк А.А., Деякі аспекти моделювання соціальних мереж, 2014. Режим доступу до ресурсу: http://science.lp.edu.ua/sites/default/files/Papers/plugin-56_33.pdf..

[43] Чураков А. Н. Анализ социальных сетей // СоцИс. 2001. № 1. С. 109–121.

[44] Батура Т. В. Модели и методы анализа компьютерных социальных сетей, Программные продукты и системы. 2013. No 3, С. 131-133.

[45] Charu C., Social network data analytics. 2011, 520 p.

[46] Hanneman, Robert A. and Mark Riddle. Introduction to social network methods. Riverside, CA: University of California, Riverside, 2005. 322 p.

[47] Wiedermann, M., Smith, E. K., Heitzig, J., & Donges, J. F. (2020). A network-based microfoundation of Granovetter's threshold model for social tipping. *Scientific Reports*, 10, Article 11202. https://doi.org/10.1038/s41598-020-67102-6

[48] Kempe, D., Kleinberg, J., & Tardos, É. (2003). *Maximizing the spread of influence through a social network*. In *Proceedings of the 9th ACM SIGKDD*, 137–146. https://doi.org/10.1145/956750.956769

[49] Acemoglu, D., & Ozdaglar, A. (2011). Opinion dynamics and learning in social networks. *Dynamic Games and Applications*, 1(1), 3–49.

[50] Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

[51] Newman, M. E. J. (2002). Spread of epidemic disease on networks. *Physical Review E*, 66, 016128.

[52] Castellano, C., Fortunato, S., & Loreto, V. (2009). Statistical physics of social dynamics. *Reviews of Modern Physics*, 81(2), 591–646.

[53] Flache, A., & Macy, M. W. (2011). Small worlds and cultural polarization. *Journal of Mathematical Sociology*, 35(1–3), 146–176.

[54] Pemantle, R. (2007). A survey of random processes with reinforcement. *Probability Surveys*, 4, 1–79.

[55] Epstein, J. M. (2007). *Generative Social Science: Studies in Agent-Based Computational Modeling*. Princeton University Press. https://doi.org/10.1515/9781400842872

[56] Молодецька-Гринчук К. В. Методологія побудови системи забезпечення інформаційної безпеки держави в соціальних інтернет сервісах// Дисертаційна робота, 2017, С. 3

[57] Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання // Монографія, К.:Інтертехнологія, 2009. С. 12-14.

[58] Гончар М., Горбач В., Пінчук А. Російський спрут у дії. Кейс «Україна», на основі досліджень експертної групи під егідою Центру глобалістики «Стратегія XXI» за підтримки Міжнародного Фонду «Відродження», 2020р. ст. 67-77.

[59] Додонов В. О., Ланде Д. В., Путятін В. Г., Мультиагентний підхід до моделювання інформаційно-аналітичної системи/ Інформаційно-аналітичні системи обробки даних, 2016, Т. 18, № 2. С. 22- 24.

[60] Додонов А. Г., Ландэ Д. В., Додонов В. А., Распознавание информационных операций: мультиагентный подход, Open Semantic Technologies for Intelligent System.

[61] Chi-Jen Lin. Assignment Problem for Team Performance Promotion under Fuzzy Environment // Hindawi Publishing Corporation. Mathematical Problems in Engineering. 2013. 10 p. [Електронне джерело] Режим доступу: http://dx.doi.org/10.1155/2013/791415.

[62] Федонюк А. А. Деякі аспекти моделювання соціальних мереж. 2014 [Електронне джерело] Режим доступу: http://www.irbis-nbuv.gov.ua/FVNULPICM_2014_783_56.pdf.

[63] Hanneman, Robert A. and Mark Riddle. Introduction to social network methods. - Riverside, CA : University of California, Riverside, 2005. 322 p.

[64] Бутвін Б. Л., Штифурак Ю. М. Методичні засади дослідження складних динамічних систем на основі агентного моделювання // Матеріали VII міжнародної наукової конференції «Актуальні проблеми забезпечення кібербезпеки та захисту інформації». 2021. С. 8-10.

[65] Dante Sblendorio Agent-based Modeling in NetLogo [Електронне джерело] – Режим доступу: https://sweetcode.io/agent-based-modeling-netlogo/ (дата звернення 21.05.2025).

[66] de Arruda, H.F., Silva, F.N., Comin, C.H., Amancio, D.R., da Costa, L.F. Connecting network science and information theory. Physica A: Statistical Mechanics and its Applications. 2019. 515. P.641–648.

[67] Handbook of Communication for Development and Social Change. Ed. Servaes, J. Springer Nature Singapore Pte Ltd, 2020. 1506 p.

[68] Shyian, A., Nikiforova, L. Model for New Innovation Knowledge Spreading in Society. Lecture Notes on Data Engineering and Communications Technologies, 2024, 195, pp. 97–116.

[69] Shao C., Ciampaglia G.L., Varol O., et al. The spread of low-credibility content by social bots. Nat Commun. 2018. Vol. 9. Article 4787. doi:10.1038/s41467-018-06930-7.

[70] Ross B., Pilz L., Cabrera B. et al. Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks. European Journal of Information Systems. 2019. Vol. 28(4). P. 394–412. doi:10.1080/0960085X.2018.1560920.

[71] Del Vicario M., Bessi A., Zollo F., et al. The spreading of misinformation online. Proceedings of the National Academy of Sciences. 2016. Vol. 113(3). P. 554–559. doi:10.1073/pnas.1517441113.

[72] Bail C.A., Argyle L.P., Brown T.W., et al. Exposure to opposing views on social media can increase political polarization. Proceedings of the National Academy of Sciences. 2018. Vol. 115(37). P. 9216–9221. doi:10.1073/pnas.1804840115.

[73] Pranav Goel, Jon Green, David Lazer, Philip Resnik.Mainstream News Articles Co-Shared with Fake News Buttress Misinformation Narratives. arXiv, 2023. 2308.06459. 86 с. https://doi.org/10.48550/arXiv.2308.06459.

[74] Songhui Yue, Jyothsna Kondari, Aibek Musaev, Randy K. Smith, Songqing Yue. Using Twitter Data to Determine Hurricane Category: An Experiment. arXiv, 2023. 2308.05866. 9 с. https://doi.org/10.48550/arXiv.2308.05866.

[75] Iknoor Singh, Carolina Scarton, Xingyi Song, Kalina Bontcheva. Finding Already Debunked Narratives via Multistage Retrieval: Enabling Cross-Lingual, Cross-Dataset and Zero-Shot Learning. arXiv, 2023. 2308. 05680. 11 с. https://doi.org/10.48550/arXiv.2308.05680.

[76] Julia Mendelsohn, Sayan Ghosh, David Jurgens, Ceren Budak. Bridging Nations: Quantifying the Role of Multilinguals in Communication on Social Media. arXiv, 2023. 2304.03797. 17 с. https://doi.org/10.48550/arXiv.2304.03797.

[77] Abiola Akinnubi, Nitin Agarwal. Deliberative Democracy, Perspective from Indo-Pacific Blogosphere: A Survey. arXiv, 2023. 2304.04126. 25 с. https://doi.org/10.48550/arXiv.2304.04126.

[78] Mihaela Curmei, Andreas Haupt, Dylan Hadfield-Menell, Benjamin Recht. Towards Psychologically-Grounded Dynamic Preference Models. RecSys '22: Proceedings of the 16th ACM Conference on Recommender Systems. September 2022. Pages 35–48.

[79] Malhotra N. K. Marketing Research: An Applied Orientation. London, Pearson, 2009. 900 p.

[80] Москотіна, Р. Агентно-орієнтоване моделювання як різновид імітаційного моделювання. Актуальні проблеми соціології, психології, педагогіки. 2017 №3-4 (34-35) Соціологічні науки. [Електронний ресурс] // https://core.ac.uk/download/pdf/229855815.pdf

[81] Москотіна, Р. Агентно-орієнтоване моделювання та соціологія: точки перетину. Соціологічні студії, 1(14), 2019, 38–44. Режим доступу: DOI: https://doi.org/10.29038/2306-3971-2019-01-38-44

[82] Мельников В.В., Агентна модель процесів управління інноваційних кластерів. Науковий вісник Міжнародного гуманітарного університету, 2015. Режим доступу: http://www.vestnik-econom.mgu.od.ua/journal/2015/14-2015/72.pdf

[83] Гужва В. М. Агентно-орієнтоване моделювання економічних процесів і систем. Бізнесінформ № 6 ’2011. Режим доступу: https://www.business-inform.net/export_pdf/business-inform-2011-6_0-pages-95_99.pdf

[84] Примостка А. О. Концептуальні засади агентно-орієнтовного моделювання Науковий вісник Ужгородського національного університету Випуск 11 • 2017 124-129

[85] Грушецький А. М. Агентне моделювання: основні ідеї і перспективи. Наукові записки. Том 161. Соціологічні науки, 2014. Режим доступу: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0196c219-1768-4d64-bc43-388133fa629c/content

[86] Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences, 99*(suppl_3), 7280–7287. https://doi.org/10.1073/pnas.082080899

[87] Ahrweiler, P., Gilbert, N., & Pyka, A. (2015). Simulating knowledge dynamics in innovation networks (KDIN): An agent-based model approach. *Computational and Mathematical Organization Theory, 21*(1), 1–26. https://doi.org/10.1007/s10588-014-9174-8

[88] Miller, J. H., & Page, S. E. (2007). *Complex adaptive systems: An introduction to computational models of social life*. Princeton University Press.

[89] Epstein, J. M. (2006). *Generative social science: Studies in agent-based computational modeling*. Princeton University Press.

[90] Grimm, V., & Railsback, S. F. (2005). *Individual-based modeling and ecology*. Princeton University Press.

[91] Tesfatsion, L., & Judd, K. L. (Eds.). (2006). *Handbook of computational economics: Agent-based computational economics* (Vol. 2). Elsevier.

[92] Macal, C. M., & North, M. J. (2010). Tutorial on agent-based modeling and simulation. *Journal of Simulation*, 4(3), 151–162. https://doi.org/10.1057/jos.2010.3

[93] Epstein, J. M. (2009). Modelling to contain pandemics. *Nature*, 460(7256), 687. https://doi.org/10.1038/460687a

[94] Perez, L., & Dragicevic, S. (2009). An agent-based approach for modeling dynamics of contagious disease spread. *International Journal of Health Geographics*, 8(1), 50. https://doi.org/10.1186/1476-072X-8-50

[95] Rand, W., & Rust, R. T. (2011). Agent-based modeling in marketing: Guidelines for rigor. *International Journal of Research in Marketing*, 28(3), 181–193. https://doi.org/10.1016/j.ijresmar.2011.04.002

[96] Railsback, S. F., & Grimm, V. (2019). *Agent-based and individual-based modeling: A practical introduction* (2nd ed.). Princeton University Press.

[97] Wilensky, U., & Rand, W. (2015). *An introduction to agent-based modeling: Modeling natural, social, and engineered complex systems with NetLogo*. MIT Press.

[98] Macal, C. M., & North, M. J. (2014). Introductory tutorial: Agent-based modeling and simulation. In *Proceedings of the 2014 Winter Simulation Conference* (pp. 6–20). IEEE. https://doi.org/10.1109/WSC.2014.7019764

[99] Wilensky, U., & Rand, W. (2015). *An Introduction to Agent-Based Modeling: Modeling Natural, Social, and Engineered Complex Systems with NetLogo*. MIT Press.

[100] North, M. J., Collier, N. T., & Vos, J. R. (2006). *Experiences Creating Three Implementations of the Repast Agent Modeling Toolkit*. ACM Transactions on Modeling and Computer Simulation, 16(1), 1–25. https://doi.org/10.1145/1122012.1122013

[101] North M, Collier N, Ozik J: Complex adaptive systems modeling with Repast Simphony [Електронний ресурс] // Springer, 2013 Режим доступу: https://casmodeling.springeropen.com/articles/10.1186/2194-3206-1-3

[102] Schriber, T. J., & Brunner, D. T. (2006). *Inside Discrete-Event Simulation Software: How It Works and Why It Matters*. In *Proceedings of the 2006 Winter Simulation Conference* (pp. 1–15). IEEE. https://doi.org/10.1109/WSC.2006.322942

[103] Altiok, T., & Melamed, B. (2007). *Simulation Modeling and Analysis with Arena*. Elsevier.

[104] Siemens Digital Industries Software. (2020). *Tecnomatix Plant Simulation Help Manual*. Retrieved from https://docs.sw.siemens.com

[105] Minar, N., Burkhart, R., Langton, C., & Askenazi, M. (1996). *The Swarm simulation system: A toolkit for building multi-agent simulations*. Working Paper 96-06-042, Santa Fe Institute. Режим доступу до ресурсу: https://www.santafe.edu/research/results/working-papers/swarm-simulation-system

[106] Railsback, S. F., & Grimm, V. (2019). *Agent-Based and Individual-Based Modeling: A Practical Introduction* (2nd ed.). Princeton University Press.

[107] Luke, S. (2020). *The MASON simulator: Architecture, applications, and research directions*. George Mason University. Режим доступу до ресурсу: https://cs.gmu.edu/~eclab/projects/mason/

[108] Parker, J. (2001). *Ascape: Agent-based modeling platform for social science research*. Center on Social and Economic Dynamics, The Brookings Institution. Режим доступу до ресурсу: https://www.brookings.edu/research/ascape/

[109] Railsback, S. F., & Grimm, V. (2019). *Agent-Based and Individual-Based Modeling: A Practical Introduction* (2nd ed.). Princeton University Press.

[110] Railsback, S. F., & Grimm, V. (2019). *Agent-Based and Individual-Based Modeling: A Practical Introduction* (2nd ed.). Princeton University Press.

[111] Standish, R. K. (2008). *EcoLab: Agent-based modeling for C++ programmers*. In Proceedings of the 2008 International Conference on Complex Systems. Режим доступу до ресурсу: http://parallel.hpc.unsw.edu.au/rks/ecolab.html

[112] Grigoryev, I. (2016). *AnyLogic in three days: A quick course in simulation modeling*. The AnyLogic Company.

[113] Christian J. E., Andrew T. Crooks Castle Principles and Concepts of Agent-Based Modelling for Developing Geospatial Simulations UCL Centre for Advanced Spatial Analysis Paper 110 - Sep 06

[114] Miles T. Parker What is Ascape and Why Should You Care? Journal of Artificial Societies and Social Simulation vol. 4, no. 1, [Електронний ресурс] // Режим доступу: https://www.jasss.org/4/1/5.html>

[115] Russell K. Standish and Richard Leow EcoLab: Agent Based Modeling for C++programmers High Performance Computing Support Unit University of New South Wales, Sydney 2052, Australia February 1, 2008 [Електронний ресурс] // Режим доступу: http://parallel.hpc.unsw.edu.au/ecolab

[116] Christophe Le Page, Nicolas Becu, Pierre Bommel and x`François Bousquet Participatory Agent-Based Simulation for Renewable Resource Management: The Role of the Cormas Simulation Platform to Nurture a Community of Practice Journal of Artificial Societies and Social Simulation 15 (1) 10 [Електронний ресурс] // Режим доступу: https://www.jasss.org/15/1/10.html

[117] Social Media, Disinformation and Electoral Integrity: IFES Working Paper, 2019, International Foundation for Electoral Systems. [Електронний ресурс] // Режим доступу: https://www.ifes.org/sites/default/files/migrate/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019_0.pdf

[118] #LightOnZelenskyyOff. Чому не всі вкиди російських ІПСО варто розвінчувати, «Громадянська мережа ОПОРА», 2022, [Електронний ресурс] // Режим доступу: https://www.oporaua.org/polit_ad/lightonzelenskyyoff-chomu-ne-vsi-vkidi-rosiiskikh-ipso-varto-rozvinchuvati-24371

ЗАСТУПНИК СЕКРЕТАРЯ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50

ДОВІДКА

про впровадження наукових досліджень аспіранта Національного університету «Чернігівська політехніка» ВАСИЛЬЄВОЇ Ольги Олександрівни у сфері забезпечення інформаційної безпеки держави

Наукові результати отримані ВАСИЛЬЄВОЮ Ольгою Олександрівною в ході проведення наукового дослідження на тему «Інформаційна технологія виявлення інформаційних операцій в соціальних мережах на основі агентного моделювання».

Метою дисертаційного дослідження є підвищення рівня інформаційної безпеки за рахунок розробки методів та моделі виявлення інформаційних операцій у соціальних мережах на основі агентного моделювання.

В рамках дослідження вирішено актуальне наукове завдання з розробки архітектури інформаційної технології для виявлення інформаційних операцій у соціальних мережах кіберпростору, елементи якої дозволяють здійснювати детекцію та маркування різних типів агентів, а також вимірювати їхній вплив на поширення контенту за рахунок застосування методу коефіцієнту впливу, а також формувати бази даних різних типів користувачів – агентів – соціальних мереж для відслідковування їхньої активності та в подальшому організації протидії інформаційним операціям проти України. Застосування комплексного методу дає можливість побудови топології мережі поширення контенту та визначення кількісних показників залученої цільової аудиторії,

Апарат РНБО України
№ 2121/25-03/2-25 від 24.07.2025

часові показники та ключові вузли в топології, що дозволяє ідентифікувати чи є дана операція успішною.

Ця інформаційна технологія є уніфікованим інструментом для проведення експериментів, побудови симуляцій інформаційних операцій та формування системи стратегічного реагування на основі даних. Технологія має потенціал для прикладного застосування в сфері інформаційної безпеки, інформаційної аналітики, стратегічних комунікацій та соціального моделювання.

Отримані результати наукових досліджень сприятимуть реалізації державної політики з питань національної безпеки в інформаційній сфері, в частині що стосується виявлення деструктивних антиукраїнських кампаній в медійному просторі.

Заступник Секретаря
Ради національної безпеки
і оборони України **Андрій КОНОНЕНКО**

Вих. №435/25
від 29.07.2025

ЗАТВЕРДЖУЮ
Генеральний директор
ТОВ «НВЦ «ІНФОЗАХИСТ»
Ярослав КАЛІНІН
"29" 07 2025 року

АКТ

про впровадження наукових результатів, що отримані аспірантом Національного університету «Чернігівська політехніка» ВАСИЛЬЄВОЮ Ольгою Олександрівною при виконанні дисертаційної роботи на здобуття ступеня доктора філософії

Комісія у складі:

Голова комісії – генеральний директор ТОВ «НВЦ «ІНФОЗАХИСТ» – Ярослав КАЛІНІН.

Члени комісії:

- директор виконавчий ТОВ «НВЦ «ІНФОЗАХИСТ» доктор технічних наук професор – Ігор БУТКО;
- асистент генерального директора ТОВ «НВЦ «ІНФОЗАХИСТ» – Дар'я СУШКО.

розглянула реалізацію наукових результатів, отриманих ВАСИЛЬЄВОЮ Ольгою Олександрівною в ході проведення наукового дослідження на тему «Інформаційна технологія виявлення інформаційних операцій в соціальних мережах на основі агентного моделювання».

Комісія встановила:

1. Під час проведення наукових досліджень з розробки інформаційної технології виявлення інформаційних операцій в соціальних мережах на основі агентного моделювання особисто ВАСИЛЬЄВОЮ О.О.:

– запропоновано модель та її програмну реалізацію виявлення інформаційних операцій в соціальних мережах на основі агентного моделювання, яка функціонує, на відміну від існуючих, орієнтуючись на функціонування різних типів агентів – користувачів, таких як лідери думок, акаунти-боти, акаунти-тролі та звичайні користувачі;

– запропоновано метод розрахунку коефіцієнту впливу різних типів користувачів на розповсюдження контенту під час виявлення інформаційної операції в соціальних мережах.

2. Отримані наукові результати дозволяють:

виявляти ознаки інформаційних операцій у соціальних мережах шляхом застосування розробленої агентної моделі, яка моделює динаміку розповсюдження контенту з урахуванням взаємодії між різнотипними типами агентів (лідерами думок, бот-акаунтами, тролями та звичайними користувачами), що істотно розширює можливості аналізу соціальних мереж у режимі реального часу;

оцінювати інформаційний вплив користувачів шляхом упровадження методу кількісного розрахунку їхнього впливу на поширення контенту, що забезпечує точну ідентифікацію структурно-важливих агентів мережі, які є критичними для детекції та нейтралізації організованих інформаційних впливів, зокрема в рамках координації інформаційних атак чи кампаній дезінформації.

Економічний ефект від впровадження не розраховувався у зв'язку з науковим призначенням результатів.

Акт складено для представлення в спеціалізовану вчену раду та не є основою для виплати винагороди за впровадження та інших авторських винагород.

Голова комісії:

Генеральний директор
«ТОВ «НВЦ «ІНФОЗАХИСТ» Ярослав КАЛІНІН

Члени комісії:

Директор виконавчий
ТОВ «НВЦ «ІНФОЗАХИСТ»
доктор технічних наук
професор Ігор БУТКО

Асистент генерального директора
ТОВ «НВЦ «ІНФОЗАХИСТ» Дар'я СУШКО

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного університету
«Чернігівська політехніка»,
кандидат технічних наук, доцент
Анатолій ПРИСТУПА
«30» 06 2025 р.

АКТ
впровадження результатів дисертаційного дослідження
Васильєвої Ольги Олександрівни
«Інформаційна технологія виявлення інформаційних операцій в соціальних мережах на основі агентного моделювання»
на здобуття наукового ступеня доктора філософії

Комісія у складі:
голова комісії – директор навчально-наукового інституту електронних та інформаційних технологій, к.е.н., доцент Базилевич Володимир Маркович, члени комісії – керівник служби захисту інформації, ст. викладач кафедри кібербезпеки та математичного моделювання, Семендяй Сергій Матвійович, к.т.н., доцент кафедри кібербезпеки та математичного моделювання Петренко Тарас Анатолійович, розглянувши матеріали дисертаційної роботи Васильєвої Ольги Олександрівни склала цей акт про те, що в освітній процес кафедри кібербезпеки та математичного моделювання до робочих програм навчальних дисциплін освітніх програм «Кібербезпека» зі спеціальності F5 «Кібербезпека за захист інформації» для першого (бакалаврського) та другого (магістерського) рівня вищої освіти впроваджено наступні результати:

Назва освітніх компонент	*Науковий результат*
1.Методи моделювання та оптимізації процесів в сфері захисту інформації; 2.Інформаційно-психологічне протиборство; 3.Соціальна інженерія.	- метод агентного моделювання на основі різних типів агентів для виявлення інформаційних операцій в соціальних мережах; - метод розрахунку коефіцієнту впливу чотирьох типів агентів на соціальну мережу під час проведення інформаційної операції та математичні моделі для кожного типу агенту; - набір алгоритмів із визначеним сценарієм моделювання для забезпечення комплексного аналізу інформаційних операцій у соціальних мережах.

Голова комісії Володимир БАЗИЛЕВИЧ
Члени комісії: Сергій СЕМЕНДЯЙ
Тарас ПЕТРЕНКО

Програмний код для побудови графіку коефіцієнтів впливу кожного типу агента

```
import matplotlib.pyplot as plt
import numpy as np

def influence_lom(F: float, Ps: float, Pl: float, En: float, alpha: float, K: float) -> float:
    """
    Вплив лідерів думок:
        lom = F * (1 - e^(-(Ps * Pl * En * alpha) / K))
    """
    return F * (1 - np.exp(-(Ps * Pl * En * alpha) / K))

def influence_bot(Pf: float, Nr_real: float, beta: float, Br: float) -> tuple[float, float]:
    """
    Вплив ботів:
        a = Pf * Nr * beta, де Nr = Nr_real * 0.2
        v = a * Br
    """
    Nr = Nr_real * 0.2
    a = Pf * Nr * beta
    v = a * Br
    return a, v

def influence_troll(Af: float, t: float, k: float, delta: float, Loi: float) -> tuple[float, float]:
    """
    Вплив тролів:
        Ad = t * k
        q = Af * Ad * delta
        m = q * Loi
    """
    Ad = t * k
    q = Af * Ad * delta
    m = q * Loi
    return q, m

def influence_person(Nlr: float, Al: float, eta: float, Fs: float, lambd: float) -> float:
    """
    Вплив звичайних користувачів:
        b = Nlr * Al * eta * Fs * λ
    """
    return Nlr * Al * eta * Fs * lambd
```

```
# === Вхідні параметри ===
F = 7000          # кількість підписників
Ps = 3            # частота публікацій
Pl = 5            # цикл життя поста
En = 120          # рівень взаємодії
alpha = 0.1       # довіра
K = 10            # коеф. кореляції

Pf = 5            # публікації ботів на день
Nr_real = 20      # репости реальні
beta = 0.00055 # автоматизація
Br = 0.1          # стійкість до блокування

Af = 250          # частота атак тролів
t = 600           # час у хвилинах
k = 0.001         # активність тролів
delta = 0.000114 # агресія тролів
Loi = 0.059     # залученість

Nlr = 17          # лайки/репости зв. користувачів
Al = 6            # активність
eta = 0.0013      # оригінальний контент
Fs = 5            # заходи в соцмережу
lambd = 0.0009    # мотивація

# === Розрахунок коефіцієнтів ===
lom = influence_lom(F, Ps, Pl, En, alpha, K) / F
a, v = influence_bot(Pf, Nr_real, beta, Br)
q, m = influence_troll(Af, t, k, delta, Loi)
b = influence_person(Nlr, Al, eta, Fs, lambd)

# === Вивід чисел (опціонально)
print(f"Лідери думок (lom/F): {lom:.9f}")
print(f"Боти (a): {a:.9f}, (v): {v:.9f}")
print(f"Тролі (q): {q:.9f}, (m): {m:.9f}")
print(f"Звичайні користувачі (b): {b:.9f}")

# === Побудова графіка ===
agents = ['Лідери думок (α)', 'Боти (a)', 'Боти (v)', 'Тролі (q)', 'Тролі (m)', 'Звичайні (b)']
values = [lom, a, v, q, m, b]

plt.figure(figsize=(10, 6))
bars = plt.bar(agents, values, log=True)
plt.ylabel("Коефіцієнт впливу (лог шкала)")
```

```
plt.title("Коефіцієнти впливу для кожного типу агента (логарифмічна шкала)")
plt.xticks(rotation=15)
plt.grid(True, axis='y', linestyle='--', alpha=0.6)

# Значення над стовпцями
for bar in bars:
    yval = bar.get_height()
    plt.text(bar.get_x() + bar.get_width() / 2.0, yval, f'{yval:.6f}', va='bottom', ha='center')

plt.tight_layout()
plt.savefig("моделювання.png")
```

Додаток 5

Програмний код для розрахунку коефіцієнтів впливу агентів при різних вхідних параметрах

```
import matplotlib.pyplot as plt
import numpy as np
from itertools import product

# === Функції впливу ===
def influence_lom(F: float, Ps: float, Pl: float, En: float, alpha: float, K: float) -> float:
    return F * (1 - np.exp(-(Ps * Pl * En * alpha) / K)) / F

def influence_bot(Pf: float, Nr_real: float, beta: float, Br: float) -> tuple[float, float]:
    Nr = Nr_real * 0.2
    a = Pf * Nr * beta
    v = a * Br
    return a, v

def influence_troll(Af: float, t: float, k: float, delta: float, Loi: float) -> tuple[float, float]:
    Ad = t * k
    q = Af * Ad * delta
    m = q * Loi
    return q, m

def influence_person(Nlr: float, Al: float, eta: float, Fs: float, lambd: float) -> float:
    return Nlr * Al * eta * Fs * lambd

# === Сценарії ===
scenarios = [
    {
        "title": "Лідери думок",
        "label": "Лідери думок (α)",
        "func": lambda p: influence_lom(**p),
        "params": {"F": 7000, "Ps": 3, "Pl": 5, "En": 120, "alpha": 0.1, "K": 10},
        "vary": {"alpha": [0.05, 0.1, 0.2], "En": [60, 120, 240]}
    },
    {
        "title": "Боти",
        "label": "Боти (a)",
        "func": lambda p: influence_bot(**p)[0],
        "params": {"Pf": 5, "Nr_real": 20, "beta": 0.00055, "Br": 0.1},
        "vary": {"Pf": [2, 5, 10], "beta": [0.0003, 0.00055, 0.001]}
    },
```

```
    {
        "title": "Тролі",
        "label": "Тролі (q)",
        "func": lambda p: influence_troll(**p)[0],
        "params": {"Af": 250, "t": 600, "k": 0.001, "delta": 0.000114, "Loi": 0.0059},
        "vary": {"delta": [0.00005, 0.000114, 0.0002], "k": [0.0005, 0.001, 0.002]}
    },
    {
        "title": "Звичайні користувачі",
        "label": "Звичайні користувачі (b)",
        "func": lambda p: influence_person(**p),
        "params": {"Nlr": 17, "Al": 6, "eta": 0.0013, "Fs": 5, "lambd": 0.009},
        "vary": {"eta": [0.0005, 0.0013, 0.003], "lambd": [0.005, 0.009, 0.015]}
    },
]

# === Побудова графіків ===
for scenario in scenarios:
    v1, v2 = list(scenario["vary"].keys())
    values = []
    labels = []

    for val1, val2 in product(scenario["vary"][v1], scenario["vary"][v2]):
        params = scenario["params"].copy()
        params[v1] = val1
        params[v2] = val2
        val = scenario["func"](params)
        values.append(val)
        labels.append(f"{v1}={val1}, {v2}={val2}")

    # Побудова графіку
    plt.figure(figsize=(12, 6))
    bars = plt.bar(labels, values, color='orange')
    plt.yscale("log")
    plt.xticks(rotation=45, ha='right')
    plt.ylabel("Коефіцієнт впливу (лог шкала)")
    plt.title(f"Коефіцієнт впливу для: {scenario['label']}")
    for bar, val in zip(bars, values):
        plt.text(bar.get_x() + bar.get_width() / 2, val, f"{val:.6f}", ha='center', va='bottom',
fontsize=8)
    plt.tight_layout()
    plt.savefig(f"scenario_{scenario['label'].replace(' ', '_').replace('(', '').replace(')', '')}.png")
    plt.close()
```

Програмний код моделі симуляції з одним типом агентів

```
turtles-own
[
  infected?
  resistant?
  virus-check-timer
]

to setup
  clear-all
  setup-nodes
  setup-spatially-clustered-network
  ask n-of initial-outbreak-size turtles
    [ become-infected ]
  ask links [ set color white ]
  reset-ticks
end

to setup-nodes
  set-default-shape turtles "circle"
  create-turtles number-of-nodes
  [
    ; for visual reasons, we don't put any nodes *too* close to the edges
    setxy (random-xcor * 0.95) (random-ycor * 0.95)
    become-susceptible
    set virus-check-timer random virus-check-frequency
  ]
```

```
end

to setup-spatially-clustered-network
  let num-links (average-node-degree * number-of-nodes) / 2
  while [count links < num-links ]
  [
    ask one-of turtles
    [
      let choice (min-one-of (other turtles with [not link-neighbor? myself])
                   [distance myself])
      if choice != nobody [ create-link-with choice ]
    ]
  ]
  ; make the network look a little prettier
  repeat 10
  [
    layout-spring turtles links 0.3 (world-width / (sqrt number-of-nodes)) 1
  ]
end

to go
  if all? turtles [not infected?]
    [ stop ]
  ask turtles
  [
     set virus-check-timer virus-check-timer + 1
     if virus-check-timer >= virus-check-frequency
       [ set virus-check-timer 0 ]
  ]
```

```
  spread-virus
  do-virus-checks
  tick
end

to become-infected
  set infected? true
  set resistant? false
  set color red
end

to become-susceptible
  set infected? false
  set resistant? false
  set color blue
end

to become-resistant
  set infected? false
  set resistant? true
  set color gray
  ask my-links [ set color gray - 2 ]
end

to spread-virus
  ask turtles with [infected?]
    [ ask link-neighbors with [not resistant?]
        [ if random-float 100 < virus-spread-chance
            [ become-infected ] ] ]
```

```
end

to do-virus-checks
  ask turtles with [infected? and virus-check-timer = 0]
  [
    if random 100 < recovery-chance
    [
      ifelse random 100 < gain-resistance-chance
        [ become-resistant ]
        [ become-susceptible ]
    ]
  ]
end
```

Програмний код моделі симуляції з чотирма типами агентів

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
***********************************************
                AnyLogic Project File
***********************************************
-->
<AnyLogicWorkspace WorkspaceVersion="1.9" AnyLogicVersion="8.9.1.202408021040" AlpVersion="8.9.1">
<Model>
	<Id>1727960821468</Id>
	<Name><![CDATA[X_dessemination]]></Name>
	<EngineVersion>6</EngineVersion>
	<JavaPackageName><![CDATA[твитер]]></JavaPackageName>
	<ModelTimeUnit><![CDATA[Minute]]></ModelTimeUnit>

	<Folders>

	</Folders>
	<ActiveObjectClasses>
		<!--  =========  Active Object Class  ========  -->
		<ActiveObjectClass>
			<Id>1727960821471</Id>
			<Name><![CDATA[Main]]></Name>
			<AdditionalClassCode><![CDATA[Random random = new Random();

int currentTrollCount = 0; // Поточна кількість агентів у стані troll
```

```
int currentPersonCount = 0; // Поточна кількість агентів у стані user
int currentLomCount = 0; // Поточна кількість агентів у стані lom
int currentBotCount = 0; // Поточна кількість агентів у стані bot
int All = 0;

void releaseAgentsToLom(int agentsToRelease) {
    Set<Integer> selectedAgents = new HashSet<>();
    int freeAgents = (int) users.stream().filter(agent -> !agent.hasChangedStatus).count();

    if (freeAgents == 0) {
        //System.out.println("Немає вільних агентів для зміни стану на lom.");
        return;
    }

    for (int i = 0; i < agentsToRelease; i++) {
        // Перевірка, чи не досягнуто обмеження lomLimit
        if (currentLomCount >= lom_people) {
          break;

        }

        int randomIndex;
        do {
            randomIndex = random.nextInt(users.size());
        } while (selectedAgents.contains(randomIndex));

        selectedAgents.add(randomIndex);
        User agent = users.get(randomIndex);
```

```
            // Перевіряємо, чи агент вже змінював статус
            if (!agent.hasChangedStatus) {
                // Змінюємо стан на lom
                agent.shapeBody.setFillColor(Color.BLUE);
                agent.hasChangedStatus = true;
                currentLomCount++; // Збільшуємо лічильник агентів у стані lom
                All++;
            } else {
                i--; // Якщо агент вже змінював статус, зменшуємо лічильник, щоб не втрачати ітерацію
            }
        }
        // traceln("Перехід у стан lom. Відпущено агентів: " + agentsToRelease);
}

void releaseAgentsToPerson(int agentsToRelease) {
    Set<Integer> selectedAgents = new HashSet<>();
    int freeAgents = (int) users.stream().filter(agent -> !agent.hasChangedStatus).count();

    // Якщо немає вільних агентів, виходимо з методу
    if (freeAgents == 0) {
        //System.out.println("Немає вільних агентів для зміни стану на lom.");
        return;
    }
    for (int i = 0; i < agentsToRelease; i++) {
        // Перевірка, чи не досягнуто обмеження userLimit
        if (currentPersonCount >= max_person) {
                break;
```

```
            }

            int randomIndex;
            do {
                randomIndex = random.nextInt(users.size());
            } while (selectedAgents.contains(randomIndex));

            selectedAgents.add(randomIndex);
            User agent = users.get(randomIndex);

            // Перевіряємо, чи агент вже змінював статус
            if (!agent.hasChangedStatus) {
                // Змінюємо стан на user
                agent.shapeBody.setFillColor(Color.GREEN);
                agent.hasChangedStatus = true;
                currentPersonCount++; // Збільшуємо лічильник агентів у стані user
                All++;
            } else {
                i--; // Якщо агент вже змінював статус, зменшуємо лічильник, щоб не
втрачати ітерацію
            }
        }
       // traceln("Перехід у стан person. Відпущено агентів: " + agentsToRelease);
}



void releaseAgentsToBot(int agentsToRelease) {
    Set<Integer> selectedAgents = new HashSet<>();
```

```
int freeAgents = (int) users.stream().filter(agent -> !agent.hasChangedStatus).count();

// Якщо немає вільних агентів, виходимо з методу
if (freeAgents == 0) {
    //System.out.println("Немає вільних агентів для зміни стану на lom.");
    return;
}
for (int i = 0; i < agentsToRelease; i++) {
    // Перевірка, чи не досягнуто обмеження botLimit
    if (currentBotCount >= max_bot) {
        break;

    }

    int randomIndex;
    do {
        randomIndex = random.nextInt(users.size());
    } while (selectedAgents.contains(randomIndex));

    selectedAgents.add(randomIndex);
    User agent = users.get(randomIndex); // Використовуємо User замість MyUser

    // Перевіряємо, чи агент вже змінював статус
    if (!agent.hasChangedStatus) {
        // Змінюємо стан на bot
        agent.shapeBody.setFillColor(new Color(139, 69, 19));
        agent.hasChangedStatus = true; // Вказуємо, що агент змінив статус
        currentBotCount++; // Збільшуємо лічильник агентів у стані bot
        All++;
```

```
            } else {
                i--; // Якщо агент вже змінював статус, зменшуємо лічильник, щоб не втрачати ітерацію
            }
        }
        // traceln("Перехід у стан bot. Відпущено агентів: " + agentsToRelease);
}

void releaseAgentsToTroll(int agentsToRelease) {
    Set<Integer> selectedAgents = new HashSet<>();
    int freeAgents = (int) users.stream().filter(agent -> !agent.hasChangedStatus).count();

    // Якщо немає вільних агентів, виходимо з методу
    if (freeAgents == 0) {
        //System.out.println("Немає вільних агентів для зміни стану на lom.");
        return;
    }
    for (int i = 0; i < agentsToRelease; i++) {
        // Перевірка, чи не досягнуто обмеження trollLimit
        if (currentTrollCount >= max_troll) {
            break;
        }

        int randomIndex;
        do {
            randomIndex = random.nextInt(users.size());
        } while (selectedAgents.contains(randomIndex));

        selectedAgents.add(randomIndex);
```

```
        User agent = users.get(randomIndex); // Використовуємо User замість MyUser


        // Перевіряємо, чи агент вже змінював статус
        if (!agent.hasChangedStatus) {
            // Змінюємо стан на troll
            agent.shapeBody.setFillColor(Color.MAGENTA);
            agent.hasChangedStatus = true; // Вказуємо, що агент змінив статус
            currentTrollCount++; // Збільшуємо лічильник агентів у стані troll
            All++;
        } else {
            i--; // Якщо агент вже змінював статус, зменшуємо лічильник, щоб не втрачати ітерацію
        }
    }
    // traceln("Перехід у стан troll. Відпущено агентів: " + agentsToRelease);
}



]]></AdditionalClassCode>
                        <Generic>false</Generic>
                        <GenericParameter>
                                <Id>1727960821477</Id>
                                <Name><![CDATA[1727960821477]]></Name>
                                <GenericParameterValue Class="CodeValue">
                                        <Code><![CDATA[T extends Agent]]></Code>
                                </GenericParameterValue>
                                <GenericParameterLabel><![CDATA[Параметр настройки:]]></GenericParameterLabel>
                        </GenericParameter>
                        <FlowChartsUsage>ENTITY</FlowChartsUsage>
```

<SamplesToKeep>100</SamplesToKeep>

<LimitNumberOfArrayElements>false</LimitNumberOfArrayElements>

<ElementsLimitValue>100</ElementsLimitValue>

<MakeDefaultViewArea>true</MakeDefaultViewArea>

<SceneGridColor/>

<SceneBackgroundColor/>

<SceneSkybox>null</SceneSkybox>

<AgentProperties>

<EnvironmentDefinesInitialLocation>true</EnvironmentDefinesInitialLocation>

<RotateAnimationTowardsMovement>true</RotateAnimationTowardsMovement>

<RotateAnimationVertically>false</RotateAnimationVertically>

<VelocityCode Class="CodeUnitValue">

<Code><![CDATA[10]]></Code>

<Unit Class="SpeedUnits"><![CDATA[MPS]]></Unit>

</VelocityCode>

<PhysicalLength Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="LengthUnits"><![CDATA[METER]]></Unit>

</PhysicalLength>

<PhysicalWidth Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="LengthUnits"><![CDATA[METER]]></Unit>

</PhysicalWidth>

<PhysicalHeight Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit
Class="LengthUnits"><![CDATA[METER]]></Unit>

</PhysicalHeight>

</AgentProperties>

<EnvironmentProperties>

<EnableSteps>false</EnableSteps>

<StepDurationCode Class="CodeUnitValue">

<Code><![CDATA[1.0]]></Code>

<Unit
Class="TimeUnits"><![CDATA[SECOND]]></Unit>

</StepDurationCode>

<SpaceType>CONTINUOUS</SpaceType>

<WidthCode><![CDATA[500]]></WidthCode>

<HeightCode><![CDATA[500]]></HeightCode>

<ZHeightCode><![CDATA[0]]></ZHeightCode>

<ColumnsCountCode><![CDATA[100]]></ColumnsCountCode>

<RowsCountCode><![CDATA[100]]></RowsCountCode>

<NeigborhoodType>MOORE</NeigborhoodType>

<LayoutType>RANDOM</LayoutType>

<LayoutTypeApplyOnStartup>true</LayoutTypeApplyOnStartup>

<NetworkType>USER_DEF</NetworkType>

<NetworkTypeApplyOnStartup>true</NetworkTypeApplyOnStartup>

<ConnectionsPerAgentCode><![CDATA[2]]></ConnectionsPerAgentCode>

<ConnectionsRangeCode><![CDATA[50]]></ConnectionsRangeCode>

<NeighborLinkFractionCode><![CDATA[0.95]]></NeighborLinkFractionCode>

```
                    <MCode><![CDATA[10]]></MCode>
                </EnvironmentProperties>
                <DatasetsCreationProperties>
                    <AutoCreate>true</AutoCreate>
                    <OccurrenceAtTime>true</OccurrenceAtTime>
                    <OccurrenceDate>1728028800000</OccurrenceDate>
                    <OccurrenceTime Class="CodeUnitValue">
                        <Code><![CDATA[0]]></Code>
                        <Unit
Class="TimeUnits"><![CDATA[MINUTE]]></Unit>
                    </OccurrenceTime>
                    <RecurrenceCode Class="CodeUnitValue">
                        <Code><![CDATA[1]]></Code>
                        <Unit
Class="TimeUnits"><![CDATA[MINUTE]]></Unit>
                    </RecurrenceCode>
                </DatasetsCreationProperties>
                <ScaleRuler>
                    <Id>1727960821474</Id>
                    <Name><![CDATA[scale]]></Name>
                    <X>0</X><Y>-150</Y>
                    <PublicFlag>false</PublicFlag>
                    <PresentationFlag>false</PresentationFlag>
                    <ShowLabel>false</ShowLabel>
                    <DrawMode>SHAPE_DRAW_2D3D</DrawMode>
                    <Length>100</Length>
                    <Rotation>0</Rotation>
                    <ScaleType>BASED_ON_LENGTH</ScaleType>
                    <ModelLength>10</ModelLength>
                    <LengthUnits>METER</LengthUnits>
```

<Scale>10</Scale>

<InheritedFromParentAgentType>true</InheritedFromParentAgentType>

</ScaleRuler>

<CurrentLevel>1727960821478</CurrentLevel>

<ConnectionsId>1727960821472</ConnectionsId>

<Variables>

<Variable Class="PlainVariable">

<Id>1727961220197</Id>

<Name><![CDATA[lom_count]]></Name>

<X>20</X><Y>300</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1727961295594</Id>

<Name><![CDATA[bot_count]]></Name>

<X>20</X><Y>350</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1727961309013</Id>

<Name><![CDATA[troll_count]]></Name>

<X>20</X><Y>400</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1727961322793</Id>

<Name><![CDATA[person_count]]></Name>

<X>20</X><Y>450</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1727961334888</Id>

<Name><![CDATA[total_count]]></Name>

<X>20</X><Y>500</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1727961503276</Id>

<Name><![CDATA[a]]></Name>

```
                    <X>200</X><Y>300</Y>
                    <Label><X>10</X><Y>0</Y></Label>
                    <PublicFlag>false</PublicFlag>
                    <PresentationFlag>true</PresentationFlag>
                    <ShowLabel>true</ShowLabel>
                    <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                        <Type><![CDATA[double]]></Type>
                        <InitialValue Class="CodeValue">
                            <Code><![CDATA[0.011]]></Code>
                        </InitialValue>
                    </Properties>
                </Variable>
                <Variable Class="PlainVariable">
                    <Id>1727961526009</Id>
                    <Name><![CDATA[b]]></Name>
                    <X>200</X><Y>400</Y>
                    <Label><X>10</X><Y>0</Y></Label>
                    <PublicFlag>false</PublicFlag>
                    <PresentationFlag>true</PresentationFlag>
                    <ShowLabel>true</ShowLabel>
                    <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                        <Type><![CDATA[double]]></Type>
                        <InitialValue Class="CodeValue">
                            <Code><![CDATA[0.0006]]></Code>
                        </InitialValue>
                    </Properties>
                </Variable>
                <Variable Class="PlainVariable">
```

<Id>1727961544920</Id>

<Name><![CDATA[tal_count_at_60]]></Name>

<X>150</X><Y>50</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[lom_people * Math.log10(0.1 * 60 + 1);

]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1728029035908</Id>

<Name><![CDATA[tal_count]]></Name>

<X>20</X><Y>550</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

```
                    </InitialValue>
                </Properties>
            </Variable>
            <Variable Class="PlainVariable">
                <Id>1728046591116</Id>
                <Name><![CDATA[tal_count_at_600]]></Name>
                <X>150</X><Y>100</Y>
                <Label><X>10</X><Y>0</Y></Label>
                <PublicFlag>false</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>true</ShowLabel>
                <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                    <Type><![CDATA[double]]></Type>
                    <InitialValue Class="CodeValue">
                        <Code><![CDATA[k1 * log10 (0.01 *
(600-60) + 1) + tal_count_at_60


]]></Code>
                    </InitialValue>
                </Properties>
            </Variable>
            <Variable Class="PlainVariable">
                <Id>1728047717430</Id>
                <Name><![CDATA[k1]]></Name>
                <X>200</X><Y>550</Y>
                <Label><X>10</X><Y>0</Y></Label>
                <PublicFlag>false</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>true</ShowLabel>
```

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">
<Type><![CDATA[double]]></Type>
<InitialValue Class="CodeValue">
<Code><![CDATA[4.857142857 * lom_people
]]></Code>
</InitialValue>
</Properties>
</Variable>
<Variable Class="PlainVariable">
<Id>1728047787454</Id>
<Name><![CDATA[k2]]></Name>
<X>200</X><Y>500</Y>
<Label><X>10</X><Y>0</Y></Label>
<PublicFlag>false</PublicFlag>
<PresentationFlag>true</PresentationFlag>
<ShowLabel>true</ShowLabel>
<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">
<Type><![CDATA[double]]></Type>
<InitialValue Class="CodeValue">
<Code><![CDATA[0.457142857 * lom_people]]></Code>
</InitialValue>
</Properties>
</Variable>
<Variable Class="PlainVariable">
<Id>1728049478625</Id>
<Name><![CDATA[k_bot]]></Name>

```
                    <X>120</X><Y>250</Y>
                    <Label><X>10</X><Y>0</Y></Label>
                    <PublicFlag>false</PublicFlag>
                    <PresentationFlag>true</PresentationFlag>
                    <ShowLabel>true</ShowLabel>
                    <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                        <Type><![CDATA[double]]></Type>
                        <InitialValue Class="CodeValue">
                            <Code><![CDATA[0.3]]></Code>
                        </InitialValue>
                    </Properties>
                </Variable>
                <Variable Class="PlainVariable">
                    <Id>1728049490829</Id>
                    <Name><![CDATA[k_troll]]></Name>
                    <X>200</X><Y>250</Y>
                    <Label><X>10</X><Y>0</Y></Label>
                    <PublicFlag>false</PublicFlag>
                    <PresentationFlag>true</PresentationFlag>
                    <ShowLabel>true</ShowLabel>
                    <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                        <Type><![CDATA[double]]></Type>
                        <InitialValue Class="CodeValue">
                            <Code><![CDATA[0.2]]></Code>
                        </InitialValue>
                    </Properties>
                </Variable>
                <Variable Class="PlainVariable">
```

<Id>1728049500107</Id>

<Name><![CDATA[k_person]]></Name>

<X>20</X><Y>250</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0.5]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1729586066181</Id>

<Name><![CDATA[lom_count_prev]]></Name>

<X>200</X><Y>710</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0]]></Code>

</InitialValue>

</Properties>

```
                </Variable>
                <Variable Class="PlainVariable">
                        <Id>1729586085966</Id>
                        <Name><![CDATA[bot_count_prev]]></Name>
                        <X>200</X><Y>690</Y>
                        <Label><X>10</X><Y>0</Y></Label>
                        <PublicFlag>false</PublicFlag>
                        <PresentationFlag>true</PresentationFlag>
                        <ShowLabel>true</ShowLabel>
                        <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                                <Type><![CDATA[double]]></Type>
                                <InitialValue Class="CodeValue">
                                        <Code><![CDATA[0]]></Code>
                                </InitialValue>
                        </Properties>
                </Variable>
                <Variable Class="PlainVariable">
                        <Id>1729586123136</Id>
                        <Name><![CDATA[troll_count_prev]]></Name>
                        <X>200</X><Y>670</Y>
                        <Label><X>10</X><Y>0</Y></Label>
                        <PublicFlag>false</PublicFlag>
                        <PresentationFlag>true</PresentationFlag>
                        <ShowLabel>true</ShowLabel>
                        <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                                <Type><![CDATA[double]]></Type>
                                <InitialValue Class="CodeValue">
                                        <Code><![CDATA[0]]></Code>
```

```
                    </InitialValue>
                </Properties>
            </Variable>
            <Variable Class="PlainVariable">
                <Id>1729586146524</Id>
                <Name><![CDATA[person_count_prev]]></Name>
                <X>200</X><Y>650</Y>
                <Label><X>10</X><Y>0</Y></Label>
                <PublicFlag>false</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>true</ShowLabel>
                <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                    <Type><![CDATA[double]]></Type>
                    <InitialValue Class="CodeValue">
                        <Code><![CDATA[0]]></Code>
                    </InitialValue>
                </Properties>
            </Variable>
            <Variable Class="PlainVariable">
                <Id>1729864008328</Id>
                <Name><![CDATA[tal_count_at_1440]]></Name>
                <X>150</X><Y>150</Y>
                <Label><X>10</X><Y>0</Y></Label>
                <PublicFlag>false</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>true</ShowLabel>
                <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                    <Type><![CDATA[int]]></Type>
```

<InitialValue Class="CodeValue">

<Code><![CDATA[(int) Math.round(k2 * Math.log10(0.01 * (1440 - 600) + 1) + tal_count_at_600);]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1730106500367</Id>

<Name><![CDATA[lom_people_0]]></Name>

<X>400</X><Y>650</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[(int) Math.round(tal_count_at_1440 / (0.357142857 * Math.log10(0.01 * (1440 - 600) + 1) + 4.857142857 * Math.log10(0.01 * (600 - 60) + 1) + Math.log10(0.1 * 60 + 1)));

]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1730125943241</Id>

<Name><![CDATA[q]]></Name>

<X>200</X><Y>350</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0.017]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1730289207071</Id>

<Name><![CDATA[v]]></Name>

<X>200</X><Y>450</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[double]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[0.0001]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1730293468667</Id>

<Name><![CDATA[max_person]]></Name>

<X>40</X><Y>740</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[int]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[(int) Math.round(((lom_people * k_person * b * (600 - 60)) * Math.pow(1 + b, 1440 - 600)))

]]></Code>

</InitialValue>

</Properties>

</Variable>

<Variable Class="PlainVariable">

<Id>1730385866168</Id>

<Name><![CDATA[max_bot]]></Name>

<X>40</X><Y>660</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Properties SaveInSnapshot="true" Constant="false" AccessType="public" StaticVariable="false">

<Type><![CDATA[int]]></Type>

<InitialValue Class="CodeValue">

<Code><![CDATA[(int) Math.round(((lom_people * k_bot * a * (600 - 60)) * Math.pow(1 + v, 1440 - 600)))]]></Code>

</InitialValue>

```
                </Properties>
            </Variable>
            <Variable Class="PlainVariable">
                <Id>1730385871823</Id>
                <Name><![CDATA[max_troll]]></Name>
                <X>40</X><Y>700</Y>
                <Label><X>10</X><Y>0</Y></Label>
                <PublicFlag>false</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>true</ShowLabel>
                <Properties SaveInSnapshot="true" Constant="false"
AccessType="public" StaticVariable="false">
                    <Type><![CDATA[int]]></Type>
                    <InitialValue Class="CodeValue">
                        <Code><![CDATA[      (int)
Math.round(((lom_people * k_troll * q * (600 - 60)) * Math.pow(1 + v, 1440 -
600)))]]></Code>
                    </InitialValue>
                </Properties>
            </Variable>
            <Variable Class="Parameter">
                <Id>1728031167794</Id>
                <Name><![CDATA[lom_people]]></Name>
                <X>20</X><Y>50</Y>
                <Label><X>10</X><Y>0</Y></Label>
                <PublicFlag>false</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>true</ShowLabel>
                <Properties SaveInSnapshot="true"
ModificatorType="STATIC">
```

<Type><![CDATA[int]]></Type>
<UnitType><![CDATA[NONE]]></UnitType>
<SdArray>false</SdArray>
<DefaultValue Class="CodeValue">
<Code><![CDATA[700]]></Code>
</DefaultValue>
<ParameterEditor>
<Id>1728031167792</Id>

<EditorContolType>TEXT_BOX</EditorContolType>

<MinSliderValue><![CDATA[0]]></MinSliderValue>

<MaxSliderValue><![CDATA[100]]></MaxSliderValue>

<DelimeterType>NO_DELIMETER</DelimeterType>
</ParameterEditor>
</Properties>
</Variable>
</Variables>
<Events>
<Event>
<Id>1727961776017</Id>
<Name><![CDATA[dynamicGrowth]]></Name>
<X>10</X><Y>150</Y>
<Label><X>10</X><Y>0</Y></Label>
<PublicFlag>false</PublicFlag>
<PresentationFlag>true</PresentationFlag>
<ShowLabel>true</ShowLabel>
<Properties TriggerType="timeout" Mode="cyclic">

<Timeout Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

</Timeout>

<Rate Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="RateUnits"><![CDATA[PER_MINUTE]]></Unit>

</Rate>

<OccurrenceAtTime>true</OccurrenceAtTime>

<OccurrenceDate>1728028800000</OccurrenceDate>

<OccurrenceTime Class="CodeUnitValue">

<Code><![CDATA[0]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

</OccurrenceTime>

<RecurrenceCode Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

</RecurrenceCode>

<Condition><![CDATA[false]]></Condition>

</Properties>

<Action><![CDATA[if (time() <= 60) {

// Фаза 1: Зростання Lom до 7000

lom_count = lom_people * time() / 60;

total_count = lom_count + bot_count + troll_count + person_count;

tal_count = lom_people * Math.log10(0.1 * time() + 1);

bot_count = 0;

```
    troll_count = 0;
    person_count = 0;

}

else if (time() > 60 && time() <= 600) {
        // Фаза 2: Підключення Bot, Troll, User
    bot_count = (lom_people * k_bot) * a * (time() - 60);
    troll_count = (lom_people * k_troll) * q * (time() - 60);
    person_count = (lom_people * k_person) * b * (time() - 60);
    total_count = lom_count + bot_count + troll_count + person_count;
    tal_count = k1 * Math.log10(0.01 * (time() - 60) + 1) + tal_count_at_60;
    }

else {
    // Фаза 3: Після 600 хвилин зростає тільки User
    bot_count = bot_count + (bot_count * v);
    troll_count = troll_count + (troll_count * v);
    person_count = person_count + (person_count * b);
    total_count = lom_count + bot_count + troll_count + person_count;
    tal_count = k2 * Math.log10(0.01 * (time() - 600) + 1) + tal_count_at_600;

}



if (time() > 1440) {
        pauseSimulation();
}
```

```
]]></Action>
                                    </Event>
                                    <Event>
                                        <Id>1729586165342</Id>
                                        <Name><![CDATA[Counter_Agent]]></Name>
                                        <X>200</X><Y>740</Y>
                                        <Label><X>10</X><Y>0</Y></Label>
                                        <PublicFlag>false</PublicFlag>
                                        <PresentationFlag>true</PresentationFlag>
                                        <ShowLabel>true</ShowLabel>
                                        <Properties TriggerType="timeout" Mode="cyclic">
                                            <Timeout Class="CodeUnitValue">
                                                <Code><![CDATA[1]]></Code>
                                                <Unit
Class="TimeUnits"><![CDATA[MINUTE]]></Unit>
                                            </Timeout>
                                            <Rate Class="CodeUnitValue">
                                                <Code><![CDATA[1]]></Code>
                                                <Unit
Class="RateUnits"><![CDATA[PER_MINUTE]]></Unit>
                                            </Rate>
                                            <OccurrenceAtTime>true</OccurrenceAtTime>

        <OccurrenceDate>1729670400000</OccurrenceDate>
                                            <OccurrenceTime Class="CodeUnitValue">
                                                <Code><![CDATA[0]]></Code>
                                                <Unit
Class="TimeUnits"><![CDATA[MINUTE]]></Unit>
```

```
                                        </OccurrenceTime>
                                        <RecurrenceCode Class="CodeUnitValue">
                                            <Code><![CDATA[1]]></Code>
                                            <Unit
Class="TimeUnits"><![CDATA[MINUTE]]></Unit>
                                        </RecurrenceCode>
                                        <Condition><![CDATA[false]]></Condition>
                                    </Properties>
                                    <Action><![CDATA[// Таймер або подія, що
перевіряє змінні
if (lom_count != lom_count_prev) {
    int agentsToRelease = (int) Math.ceil(lom_count - lom_count_prev);
    if (agentsToRelease > 0) {
        releaseAgentsToLom(agentsToRelease);
    }
    lom_count_prev = lom_count;   // Оновлюємо значення після перевірки
}

if (bot_count != bot_count_prev) {
    int agentsToRelease = (int) Math.ceil(bot_count - bot_count_prev);
    if (agentsToRelease > 0) {
        releaseAgentsToBot(agentsToRelease);
    }
    bot_count_prev = bot_count;   // Оновлюємо значення після перевірки
}

if (troll_count != troll_count_prev) {
    int agentsToRelease = (int) Math.ceil(troll_count - troll_count_prev);
    if (agentsToRelease > 0) {
        releaseAgentsToTroll(agentsToRelease);
```

```
    }
    troll_count_prev = troll_count;   // Оновлюємо значення після перевірки
}

if (person_count != person_count_prev) {
    int agentsToRelease = (int) Math.ceil(person_count - person_count_prev);
    if (agentsToRelease > 0) {
        releaseAgentsToPerson(agentsToRelease);
    }

    // Оновлюємо значення тільки якщо agentsToRelease не є від'ємним
    person_count_prev = person_count;
}
]]></Action>
                                </Event>
                        </Events>
                        <AgentLinks>
                                <AgentLink>
                                        <Id>1727960821472</Id>
                                        <Name><![CDATA[connections]]></Name>
                                        <X>50</X><Y>-50</Y>
                                        <Label><X>15</X><Y>0</Y></Label>
                                        <PublicFlag>false</PublicFlag>
                                        <PresentationFlag>true</PresentationFlag>
                                        <ShowLabel>true</ShowLabel>

            <HandleReceiveInConnections>false</HandleReceiveInConnections>

            <AgentLinkType>COLLECTION_OF_LINKS</AgentLinkType>
```

<AgentLinkBidirectional>true</AgentLinkBidirectional>

<MessageType><![CDATA[Object]]></MessageType>

<LineStyle>SOLID</LineStyle>

<LineWidth>1</LineWidth>

<LineColor>-16777216</LineColor>

<LineZOrder>UNDER_AGENTS</LineZOrder>

<LineArrow>NONE</LineArrow>

<LineArrowPosition>END</LineArrowPosition>

</AgentLink>

</AgentLinks>

<EmbeddedObjects>

<EmbeddedObject>

<Id>1727960930528</Id>

<Name><![CDATA[users]]></Name>

<X>20</X><Y>100</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<PresentationId>1727960930530</PresentationId>

<ActiveObjectClass>

<PackageName><![CDATA[твитер]]></PackageName>

<ClassName><![CDATA[User]]></ClassName>

</ActiveObjectClass>

<GenericParameterSubstitute>

<GenericParameterSubstituteReference>

```
        <PackageName><![CDATA[твитер]]></PackageName>

        <ClassName><![CDATA[User]]></ClassName>

        <ItemName><![CDATA[1727960885000]]></ItemName>
                                        </GenericParameterSubstituteReference>
                                    </GenericParameterSubstitute>
                                    <Parameters>
                                    </Parameters>
                                    <ReplicationFlag>true</ReplicationFlag>
                                    <Replication Class="CodeValue">
                                        <Code><![CDATA[(int)
Math.round((lom_people * 60 / 60)
    + ((lom_people * k_bot * a * (600 - 60)) * Math.pow(1 + v, 1440 - 600))
    + ((lom_people * k_troll * q * (600 - 60)) * Math.pow(1 + v, 1440 - 600))
    + ((lom_people * k_person * b * (600 - 60)) * Math.pow(1 + b, 1440 - 600)));
    ]]></Code>
                                    </Replication>

        <CollectionType>ARRAY_LIST_BASED</CollectionType>
                                    <InEnvironment>true</InEnvironment>

        <InitialLocationType>AT_ANIMATION_POSITION</InitialLocationType>
                                    <XCode Class="CodeValue">
                                        <Code><![CDATA[0]]></Code>
                                    </XCode>
                                    <YCode Class="CodeValue">
                                        <Code><![CDATA[0]]></Code>
                                    </YCode>
                                    <ZCode Class="CodeValue">
```

<Code><![CDATA[0]]></Code>
</ZCode>
<ColumnCode Class="CodeValue">
<Code><![CDATA[0]]></Code>
</ColumnCode>
<RowCode Class="CodeValue">
<Code><![CDATA[0]]></Code>
</RowCode>
<LatitudeCode Class="CodeValue">
<Code><![CDATA[0]]></Code>
</LatitudeCode>
<LongitudeCode Class="CodeValue">
<Code><![CDATA[0]]></Code>
</LongitudeCode>
<LocationNameCode Class="CodeValue">
<Code><![CDATA[""]]></Code>
</LocationNameCode>

<InitializationType>SPECIFIED_NUMBER</InitializationType>
<InitializationDatabaseTableQuery>
<TableReference>
</TableReference>
</InitializationDatabaseTableQuery>

<InitializationDatabaseType>ONE_AGENT_PER_DATABASE_RECORD</InitializationDatabaseType>
<QuantityColumn>
</QuantityColumn>
</EmbeddedObject>
</EmbeddedObjects>

<Presentation>

<Level>

<Id>1727960821478</Id>

<Name><![CDATA[level]]></Name>

<X>0</X><Y>0</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>true</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>false</ShowLabel>

<DrawMode>SHAPE_DRAW_2D3D</DrawMode>

<Z>0</Z>

<LevelVisibility>DIM_NON_CURRENT</LevelVisibility>

<Presentation>

<TimePlot>

<Id>1727962097942</Id>

<Name><![CDATA[plot]]></Name>

<X>250</X><Y>0</Y>

<Label><X>0</X><Y>-10</Y></Label>

<PublicFlag>true</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>false</ShowLabel>

<DrawMode>SHAPE_DRAW_2D3D</DrawMode>

<AutoUpdate>true</AutoUpdate>

<OccurrenceAtTime>true</OccurrenceAtTime>

<OccurrenceDate>1728028800000</OccurrenceDate>

<OccurrenceTime Class="CodeUnitValue">

<Code><![CDATA[0]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

</OccurrenceTime>

<RecurrenceCode Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

</RecurrenceCode>

<EmbeddedIcon>false</EmbeddedIcon>

<Width>660</Width>

<Height>530</Height>

<BackgroundColor/>

<BorderColor/>

<ChartArea>

<XOffset>50</XOffset>

<YOffset>30</YOffset>

<Width>580</Width>

<Height>440</Height>

<BackgroundColor>-1</BackgroundColor>

<BorderColor>-16777216</BorderColor>

<GridColor>-12566464</GridColor>

</ChartArea>

<Legend>

<Place>SOUTH</Place>

<TextColor>-16777216</TextColor>

<Size>30</Size>

</Legend>

<Labels>

<HorLabelsPosition>DEFAULT</HorLabelsPosition>

<VerLabelsPosition>DEFAULT</VerLabelsPosition>

<TextColor>-12566464</TextColor>

</Labels>

<ShowLegend>true</ShowLegend>

<TimeWindowsMovementType>MOVEMENT_WITH_DATA</TimeWindowsMovementType>

<TimeWindowUnits>MINUTE</TimeWindowUnits>

<VerScaleFromExpression><![CDATA[0]]></VerScaleFromExpression>

<VerScaleToExpression><![CDATA[5000]]></VerScaleToExpression>

<VerScaleType>AUTO</VerScaleType>

<DrawLine>true</DrawLine>

<Interpolation>LINEAR</Interpolation>

<DatasetExpression>

<Title><![CDATA[bot_count]]></Title>

<Id>1727962099904</Id>

<Expression><![CDATA[0]]></Expression>

<Color>-7650029</Color>

<Expression2><![CDATA[bot_count]]></Expression2>

<Expression2Flag>true</Expression2Flag>

<PointStyle>NONE</PointStyle>

<LineWidth>2.0</LineWidth>

</DatasetExpression>

<DatasetExpression>

<Title><![CDATA[troll_count]]></Title>

<Id>1727962117837</Id>

<Expression><![CDATA[0]]></Expression>
<Color>-60269</Color>

<Expression2><![CDATA[troll_count]]></Expression2>
<Expression2Flag>true</Expression2Flag>
<PointStyle>NONE</PointStyle>
<LineWidth>2.0</LineWidth>
</DatasetExpression>
<DatasetExpression>
<Title><![CDATA[person_count]]></Title>
<Id>1727962124763</Id>
<Expression><![CDATA[0]]></Expression>
<Color>-16711936</Color>

<Expression2><![CDATA[person_count]]></Expression2>
<Expression2Flag>true</Expression2Flag>
<PointStyle>NONE</PointStyle>
<LineWidth>2.0</LineWidth>
</DatasetExpression>
<DatasetExpression>
<Title><![CDATA[lom_count]]></Title>
<Id>1727963848985</Id>
<Expression><![CDATA[0]]></Expression>
<Color>-16776961</Color>
<Expression2><![CDATA[lom_count]]></Expression2>
<Expression2Flag>true</Expression2Flag>
<PointStyle>NONE</PointStyle>
<LineWidth>1.0</LineWidth>
</DatasetExpression>
<DatasetExpression>

<Title><![CDATA[tal_count]]></Title>
<Id>1728029009432</Id>
<Expression><![CDATA[my_dataset]]></Expression>
<Color>-9728477</Color>
<Expression2><![CDATA[tal_count]]></Expression2>
<Expression2Flag>true</Expression2Flag>
<PointStyle>NONE</PointStyle>
<LineWidth>4.0</LineWidth>
</DatasetExpression>
<DatasetExpression>
<Title><![CDATA[total_count]]></Title>
<Id>1730121796057</Id>
<Expression><![CDATA[my_dataset1]]></Expression>
<Color>-29696</Color>

<Expression2><![CDATA[total_count]]></Expression2>
<Expression2Flag>true</Expression2Flag>
<PointStyle>NONE</PointStyle>
<LineWidth>2.0</LineWidth>
</DatasetExpression>
<SamplesToKeep>1450</SamplesToKeep>

<TimeWindowExpression><![CDATA[1450]]></TimeWindowExpression>
<FillAreaUnderLine>false</FillAreaUnderLine>

<LabelFormat>MODEL_TIME_UNITS</LabelFormat>
</TimePlot>
</Presentation>

</Level>

<EmbeddedObjectPresentation>

<Id>1727960930530</Id>

<Name><![CDATA[users_presentation]]></Name>

<X>880</X><Y>40</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>true</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>false</ShowLabel>

<DrawMode>SHAPE_DRAW_2D</DrawMode>

<EmbeddedIcon>false</EmbeddedIcon>

<Z>0</Z>

<Rotation>0.0</Rotation>

<DrawingMode>POSITION_WITH_OFFSET</DrawingMode>

<ScaleType>AUTOMATICALLY_CALCULATED</ScaleType>

<GISScaleForRealEmbeddedObjectPresentationSize>1000</GISScaleForRealEmbeddedObjectPresentationSize>

<GISScaleForFixedEmbeddedObjectPresentationSize>1000000000</GISScaleForFixedEmbeddedObjectPresentationSize>

<Latitude>0.0</Latitude>

<Longitude>0.0</Longitude>

</EmbeddedObjectPresentation>

</Presentation>

</ActiveObjectClass>

<!-- ========= Active Object Class ======== -->

<ActiveObjectClass>

<Id>1727960884994</Id>

<Name><![CDATA[User]]></Name>

<AdditionalClassCode><![CDATA[boolean hasChangedStatus = false; // Поле для перевірки, чи змінював агент статус

]]></AdditionalClassCode>

<Generic>false</Generic>

<GenericParameter>

<Id>1727960885000</Id>

<Name><![CDATA[1727960885000]]></Name>

<GenericParameterValue Class="CodeValue">

<Code><![CDATA[T extends Agent]]></Code>

</GenericParameterValue>

<GenericParameterLabel><![CDATA[Параметр настройки:]]></GenericParameterLabel>

</GenericParameter>

<FlowChartsUsage>ENTITY</FlowChartsUsage>

<SamplesToKeep>100</SamplesToKeep>

<LimitNumberOfArrayElements>false</LimitNumberOfArrayElements>

<ElementsLimitValue>100</ElementsLimitValue>

<MakeDefaultViewArea>true</MakeDefaultViewArea>

<SceneGridColor/>

<SceneBackgroundColor/>

<SceneSkybox>null</SceneSkybox>

<AgentProperties>

<EnvironmentDefinesInitialLocation>true</EnvironmentDefinesInitialLocation>

<RotateAnimationTowardsMovement>true</RotateAnimationTowardsMovement>

<RotateAnimationVertically>false</RotateAnimationVertically>

<VelocityCode Class="CodeUnitValue">

<Code><![CDATA[10]]></Code>

<Unit Class="SpeedUnits"><![CDATA[MPS]]></Unit>

</VelocityCode>

<PhysicalLength Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="LengthUnits"><![CDATA[METER]]></Unit>

</PhysicalLength>

<PhysicalWidth Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="LengthUnits"><![CDATA[METER]]></Unit>

</PhysicalWidth>

<PhysicalHeight Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="LengthUnits"><![CDATA[METER]]></Unit>

</PhysicalHeight>

</AgentProperties>

<EnvironmentProperties>

<EnableSteps>false</EnableSteps>

<StepDurationCode Class="CodeUnitValue">

<Code><![CDATA[1.0]]></Code>

<Unit Class="TimeUnits"><![CDATA[SECOND]]></Unit>

</StepDurationCode>

<SpaceType>CONTINUOUS</SpaceType>

<WidthCode><![CDATA[500]]></WidthCode>

<HeightCode><![CDATA[500]]></HeightCode>

<ZHeightCode><![CDATA[0]]></ZHeightCode>

<ColumnsCountCode><![CDATA[100]]></ColumnsCountCode>

<RowsCountCode><![CDATA[100]]></RowsCountCode>

<NeigborhoodType>MOORE</NeigborhoodType>

<LayoutType>USER_DEF</LayoutType>

<LayoutTypeApplyOnStartup>true</LayoutTypeApplyOnStartup>

<NetworkType>USER_DEF</NetworkType>

<NetworkTypeApplyOnStartup>true</NetworkTypeApplyOnStartup>

<ConnectionsPerAgentCode><![CDATA[2]]></ConnectionsPerAgentCode>

<ConnectionsRangeCode><![CDATA[50]]></ConnectionsRangeCode>

<NeighborLinkFractionCode><![CDATA[0.95]]></NeighborLinkFractionCode>

<MCode><![CDATA[10]]></MCode>

</EnvironmentProperties>

<DatasetsCreationProperties>

<AutoCreate>true</AutoCreate>

<OccurrenceAtTime>true</OccurrenceAtTime>

<OccurrenceDate>1728028800000</OccurrenceDate>

<OccurrenceTime Class="CodeUnitValue">

<Code><![CDATA[0]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

</OccurrenceTime>

<RecurrenceCode Class="CodeUnitValue">

<Code><![CDATA[1]]></Code>

<Unit Class="TimeUnits"><![CDATA[MINUTE]]></Unit>

```
                    </RecurrenceCode>
                </DatasetsCreationProperties>
                <ScaleRuler>
                    <Id>1727960884997</Id>
                    <Name><![CDATA[scale]]></Name>
                    <X>0</X><Y>-150</Y>
                    <PublicFlag>false</PublicFlag>
                    <PresentationFlag>false</PresentationFlag>
                    <ShowLabel>false</ShowLabel>
                    <DrawMode>SHAPE_DRAW_2D3D</DrawMode>
                    <Length>100</Length>
                    <Rotation>0</Rotation>
                    <ScaleType>BASED_ON_LENGTH</ScaleType>
                    <ModelLength>10</ModelLength>
                    <LengthUnits>METER</LengthUnits>
                    <Scale>10</Scale>

        <InheritedFromParentAgentType>true</InheritedFromParentAgentType>
                </ScaleRuler>
                <CurrentLevel>1727960885001</CurrentLevel>
                <ConnectionsId>1727960884995</ConnectionsId>
                <StatechartElements>
                    <StatechartElement Class="State"
ParentState="ROOT_NODE">
                        <Id>1729501128676</Id>
                        <Name><![CDATA[full]]></Name>
                        <X>350</X><Y>60</Y>
                        <Label><X>10</X><Y>10</Y></Label>
                        <PublicFlag>false</PublicFlag>
                        <PresentationFlag>true</PresentationFlag>
```

<ShowLabel>true</ShowLabel>

<Properties Width="100" Height="30">

<EntryAction><![CDATA[shapeBody.setFillColor(silver);

]]></EntryAction>

<ExitAction><![CDATA[

]]></ExitAction>

<FillColor>-4144960</FillColor>

</Properties>

</StatechartElement>

<StatechartElement Class="EntryPoint" ParentState="ROOT_NODE">

<Id>1729501566797</Id>

<Name><![CDATA[statechart]]></Name>

<X>400</X><Y>20</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<Points>

<Point><X>0</X><Y>0</Y></Point>

<Point><X>0</X><Y>40</Y></Point>

</Points>

<Properties Target="1729501128676">

</Properties>

</StatechartElement>

</StatechartElements>

<AgentLinks>

<AgentLink>

<Id>1727960884995</Id>

<Name><![CDATA[connections]]></Name>

<X>50</X><Y>-50</Y>

<Label><X>15</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<HandleReceiveInConnections>false</HandleReceiveInConnections>

<AgentLinkType>COLLECTION_OF_LINKS</AgentLinkType>

<AgentLinkBidirectional>true</AgentLinkBidirectional>

<MessageType><![CDATA[Object]]></MessageType>

<StatechartReference>

<PackageName><![CDATA[твитер]]></PackageName>

<ClassName><![CDATA[User]]></ClassName>

<ItemName><![CDATA[statechart]]></ItemName>

</StatechartReference>

<LineStyle>SOLID</LineStyle>

<LineWidth>1</LineWidth>

<LineColor>-16777216</LineColor>

<LineZOrder>UNDER_AGENTS</LineZOrder>

<LineArrow>NONE</LineArrow>

<LineArrowPosition>END</LineArrowPosition>

</AgentLink>

</AgentLinks>

<ContainerLinks>

<ContainerLink>

<Id>1727960930535</Id>

<Name><![CDATA[main]]></Name>

<X>50</X><Y>-100</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>false</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>true</ShowLabel>

<ActiveObjectClass>

<PackageName><![CDATA[твитер]]></PackageName>

<ClassName><![CDATA[Main]]></ClassName>

</ActiveObjectClass>

</ContainerLink>

</ContainerLinks>

<Presentation>

<Level>

<Id>1727960885001</Id>

<Name><![CDATA[level]]></Name>

<X>0</X><Y>0</Y>

<Label><X>10</X><Y>0</Y></Label>

<PublicFlag>true</PublicFlag>

<PresentationFlag>true</PresentationFlag>

<ShowLabel>false</ShowLabel>

<DrawMode>SHAPE_DRAW_2D3D</DrawMode>

<Z>0</Z>

<LevelVisibility>DIM_NON_CURRENT</LevelVisibility>

```
<Presentation>
        <Group>
                <Id>1727960885004</Id>
                <Name><![CDATA[person]]></Name>
                <X>0</X><Y>0</Y>
                <Label><X>-20</X><Y>20</Y></Label>
                <PublicFlag>true</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>false</ShowLabel>
                <DrawMode>SHAPE_DRAW_2D</DrawMode>
                <EmbeddedIcon>false</EmbeddedIcon>
                <Z>0</Z>
                <Rotation>0.0</Rotation>

<Presentation>
        <Curve ControlPoints="true">
                <Id>1727960885006</Id>
                <Name><![CDATA[shapeBody]]></Name>
                <X>-2</X><Y>-7</Y>
                <Label><X>-20</X><Y>28</Y></Label>
                <PublicFlag>true</PublicFlag>
                <PresentationFlag>true</PresentationFlag>
                <ShowLabel>false</ShowLabel>
                <DrawMode>SHAPE_DRAW_2D</DrawMode>
                <EmbeddedIcon>false</EmbeddedIcon>
                <Z>0</Z>
                <ZHeight>10</ZHeight>
                <LineWidth>1</LineWidth>
                <LineColor/>
```

<LineMaterial>null</LineMaterial>

<LineStyle>SOLID</LineStyle>

<BeginArrowSize>1</BeginArrowSize>

<BeginArrowStyle>0</BeginArrowStyle>

<EndArrowSize>1</EndArrowSize>

<EndArrowStyle>0</EndArrowStyle>

<FillColor>-16777216</FillColor>

<FillMaterial>null</FillMaterial>

<Points>

<Point><X>0</X><Y>0</Y><Z>0</Z></Point>

<Point><X>0</X><Y>4</Y><Z>0</Z></Point>

<Point><X>3</X><Y>2</Y><Z>0</Z></Point>

<Point><X>-1</X><Y>3</Y><Z>0</Z></Point>

<Point><X>-2</X><Y>3</Y><Z>0</Z></Point>

<Point><X>-2</X><Y>10</Y><Z>0</Z></Point>

<Point><X>-2</X><Y>11</Y><Z>0</Z></Point>

<Point><X>0</X><Y>11</Y><Z>0</Z></Point>

<Point><X>-1</X><Y>9</Y><Z>0</Z></Point>

<Point><X>0</X><Y>17</Y><Z>0</Z></Point>

<Point><X>1</X><Y>17</Y><Z>0</Z></Point>

<Point><X>3</X><Y>17</Y><Z>0</Z></Point>

<Point><X>4</X><Y>17</Y><Z>0</Z></Point>

<Point><X>5</X><Y>9</Y><Z>0</Z></Point>

<Point><X>4</X><Y>11</Y><Z>0</Z></Point>

<Point><X>6</X><Y>11</Y><Z>0</Z></Point>

<Point><X>6</X><Y>10</Y><Z>0</Z></Point>

<Point><X>6</X><Y>3</Y><Z>0</Z></Point>

<Point><X>5</X><Y>3</Y><Z>0</Z></Point>

<Point><X>1</X><Y>2</Y><Z>0</Z></Point>

<Point><X>4</X><Y>4</Y><Z>0</Z></Point>
<Point><X>4</X><Y>0</Y><Z>0</Z></Point>
<Point><X>4</X><Y>-3</Y><Z>0</Z></Point>
<Point><X>0</X><Y>-3</Y><Z>0</Z></Point>
</Points>
<Closed>true</Closed>
</Curve>
</Presentation>

</Group>
</Presentation>

</Level>
</Presentation>

</ActiveObjectClass>
</ActiveObjectClasses>
<DifferentialEquationsMethod>EULER</DifferentialEquationsMethod>
<MixedEquationsMethod>RK45_NEWTON</MixedEquationsMethod>
<AlgebraicEquationsMethod>MODIFIED_NEWTON</AlgebraicEquationsMethod>
<AbsoluteAccuracy>1.0E-5</AbsoluteAccuracy>
<FixedTimeStep>0.001</FixedTimeStep>
<RelativeAccuracy>1.0E-5</RelativeAccuracy>
<TimeAccuracy>1.0E-5</TimeAccuracy>
<Frame>
<Width>1400</Width>
<Height>600</Height>
</Frame>
<Database>

```
        <Logging>false</Logging>
        <AutoExport>false</AutoExport>
        <ShutdownCompact>false</ShutdownCompact>
        <ImportSettings>
        </ImportSettings>
        <ExportSettings>
        </ExportSettings>
</Database>

<RunConfiguration ActiveObjectClassId="1727960821471">
        <Id>1727960821483</Id>
        <Name><![CDATA[RunConfiguration]]></Name>
        <MaximumMemory>512</MaximumMemory>
        <ModelTimeProperties>
                <StopOption><![CDATA[Stop at specified time]]></StopOption>
                <InitialDate><![CDATA[1727913600000]]></InitialDate>
                <InitialTime><![CDATA[0.0]]></InitialTime>
                <FinalDate><![CDATA[1730592000000]]></FinalDate>
                <FinalTime><![CDATA[100.0]]></FinalTime>
        </ModelTimeProperties>
        <AnimationProperties>
                <StopNever>true</StopNever>
                <ExecutionMode>realTimeScaled</ExecutionMode>
                <RealTimeScale>1.0</RealTimeScale>
                <EnableZoomAndPanning>true</EnableZoomAndPanning>
                <EnableDeveloperPanel>false</EnableDeveloperPanel>
                <ShowDeveloperPanelOnStart>false</ShowDeveloperPanelOnStart>
        </AnimationProperties>
        <Inputs>
```

```
            </Inputs>
            <Outputs>
            </Outputs>
        </RunConfiguration>
        <Experiments>
            <!--  =========  Simulation Experiment  ========  -->
            <SimulationExperiment ActiveObjectClassId="1727960821471">
                <Id>1727960821480</Id>
                <Name><![CDATA[Simulation]]></Name>

        <CommandLineArguments><![CDATA[]]></CommandLineArguments>
                <MaximumMemory>512</MaximumMemory>

        <RandomNumberGenerationType>fixedSeed</RandomNumberGenerationType>
                <CustomGeneratorCode>new Random()</CustomGeneratorCode>
                <SeedValue>1</SeedValue>

        <SelectionModeForSimultaneousEvents>LIFO</SelectionModeForSimultaneousEven
ts>
                <VmArgs><![CDATA[]]></VmArgs>
                <LoadRootFromSnapshot>false</LoadRootFromSnapshot>

                <Presentation>
                    <Text>
                        <Id>1727960821482</Id>
                        <Name><![CDATA[text]]></Name>
                        <X>50</X><Y>30</Y>
                        <Label><X>10</X><Y>0</Y></Label>
                        <PublicFlag>true</PublicFlag>
                        <PresentationFlag>true</PresentationFlag>
```

<ShowLabel>false</ShowLabel>
<DrawMode>SHAPE_DRAW_2D3D</DrawMode>
<EmbeddedIcon>false</EmbeddedIcon>
<Z>0</Z>
<Rotation>0.0</Rotation>
<Color>-12490271</Color>
<Text><![CDATA[Твитер]]></Text>
<Font>
<Name>SansSerif</Name>
<Size>24</Size>
<Style>0</Style>
</Font>
<Alignment>LEFT</Alignment>
</Text>
</Presentation>

<Parameters>
<Parameter>

<ParameterName><![CDATA[lom_people]]></ParameterName>
</Parameter>
</Parameters>
<PresentationProperties>
<EnableZoomAndPanning>true</EnableZoomAndPanning>

<ExecutionMode><![CDATA[realTimeScaled]]></ExecutionMode>
<Title><![CDATA[Твитер : Simulation]]></Title>
<EnableDeveloperPanel>true</EnableDeveloperPanel>

<ShowDeveloperPanelOnStart>false</ShowDeveloperPanelOnStart>

<RealTimeScale>1.0</RealTimeScale>
</PresentationProperties>
<ModelTimeProperties>
<StopOption><![CDATA[Never]]></StopOption>
<InitialDate><![CDATA[1727913600000]]></InitialDate>
<InitialTime><![CDATA[0.0]]></InitialTime>
<FinalDate><![CDATA[1730592000000]]></FinalDate>
<FinalTime><![CDATA[100.0]]></FinalTime>
</ModelTimeProperties>
<BypassInitialScreen>true</BypassInitialScreen>
</SimulationExperiment>
</Experiments>
<RequiredLibraryReference>
<LibraryName><![CDATA[com.anylogic.libraries.modules.markup_descriptors]]></LibraryName>
<VersionMajor>1</VersionMajor>
<VersionMinor>0</VersionMinor>
<VersionBuild>0</VersionBuild>
</RequiredLibraryReference>
</Model>
</AnyLogicWorkspace>