МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

На правах рукопису

Улічев Олександр Сергійович

УДК 004.773.2+004.942

ДИСЕРТАЦІЯ

МОДЕЛЬ ТА МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Спеціальність 21.05.01 – Інформаційна безпека держави

Подається на здобуття наукового ступеня кандидата технічних наук

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

Улічев О.С.

Науковий керівник:

Мелешко Єлизавета Владиславівна

канд. техн. наук, доцент

Київ – 2021

АНОТАЦІЯ

Улічев О.С. Модель і методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 «Інформаційна безпека держави». – Національний авіаційний університет, Київ, 2021.

Дисертаційна робота присвячена розв'язанню актуальної науково-технічної задачі розроблення методів і засобів програмного моделювання та реалізації різних стратегій поширення інформаційних впливів у сегментах соціальних мереж.

У роботі проведено аналіз сучасних методів і моделей поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства, який показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла, таких як репутація, рівень інформаційного спротиву, активність вузла. Іншим недоліком розглянутих моделей є той факт, що вони не враховують поведінку окремого вузла – стратегію поширення інформації, яку обирає вузол в процесі інформаційного впливу. Фактично під стратегією варто розуміти спосіб вибору вузла для атаки серед наявних контактів суб'єкту інформаційного впливу.

Розроблено математичну модель поширення інформаційних впливів в сегменті соціальної мережі, яка враховує індивідуальні характеристики вузлів мережі, що дає можливість застосування різних поведінкових стратегій суб'єктами впливу на основі аналізу наявних даних про параметри вузлів та їх структурне положення.

Окремою задачею є безпосередня генерація структури мережі в моделі. В результаті дослідження ряду запропонованих методів генерації структрури мережі виявлено, що основними недоліками запропонованих методів є

неможливість генерації мережі з наперед заданою структурою, а, також, низький рівень кластеризації мереж, отриманих на основі запропонованих раніше методів. Враховуючи вище сказане, запропоновані методи не можуть бути застосовані для генерації сегменту мережі на основі наявної інформації про характеристики вузлів та топологічні собливості.

В роботі запропоновано удосконалений метод генерації структури сегменту соціальної мережі, що дозволяє обирати кількість і типи кластерів сегменту соціальної мережі. В якості кластерів запропоновано обрати групу, лідерську групу, кліку – як найбільш поширені типи структурних утворень в реальних соціальних мережах. Запропонований підхід дає можливість генерувати сегменти мереж з наперед заданою структурою зв'язків та наявними сталими підмножинами вузлів (групи, лідерські групи, кліки).

На базі запропонованої математичної моделі поширення інформаційних впливів розроблено алгоритми програмного імітаційного моделювання процесу поширення інформаційних впливів у сегментах соціальної мережі, а також алгоритми генерації структури сегментів соціальної мережі.

Розроблено базові поведінкові стратегії суб'єктів впливу у соціальній мережі під час інформаційних протиборств, що дозволяють ефективно моделювати різні підходи до вибору цільових вузлів суб'єктами впливу та процес поширення ІВ. Серед запропонованих моделей розглядаються моделі без аналізу вузлів-контактів – випадковий вибір вузла для атаки, та стратегії з аналізом окремої характеристики чи набору характеристик. Застосування стратегій, що базуються на аналізі особистісних характеристик вузлів та їх структурних особливостей, можуть сприяти підвищенню швидкості поширення інформаційних впливів. В якості параметрів для аналізу обрано наступні характеристики вузлів: репутація, рівень інформаційного спротиву. Структурні особливості визначаються кількісттю контактів вузла, що є потенційним претендентом для інформаційного впливу, та структурними особливостями вузлів, з якими він контактує. Вибір стратегії може базуватись і на наявній комплексній інформації про сегмент мережі, наприклад – якщо сегмент мережі

містить значну кількість вузлів з високим інформаційним спротивом до ідеї, що росповсюджується, то для накопичення критичної маси «однодумців» варто аналізувати саме показник інформаційного спротиву. Відповідно - стратегія поширення має будуватись на аналізі показника «рівень інформаційного спротиву».

В роботі проведено ряд експериментів на програмній моделі, метою яких було порівняння швидкості росповсюдження інформаційного впливу при різних початкових умовах та з застосуванням різних стратегій.

В експериментальній частині роботи представлено усереднені результати серій експериментів, що підтверджують гіпотезу про можливість підвищення швидкості поширення інформаційних впливів за рахунок застосування стратегій, що базуються на аналізі наявної про мережу інформації. Запропоновано підходи до вибору поведінкових стратегій суб'єкту впливу у соціальній мережі під час інформаційних протиборств, які дозволяють за меншу кількість часу поширити інформаційний вплив серед вузлів сегменту соціальної мережі.

Окрім стратегії поширення інформаційних впливів суттєвим, з точки зору швидкості розповсюдження, є вибір розміщення початкового генератора в сегменті мережі. Найбільш розповсюдженним підходом, що запропоновано рядом авторів, є залучення до процесу інформаційних впливів «лідерів думок» (вузол з великою кількістю контактів та високим рівнем інформаційного впливу, репутацією). Такий підхід обумовлено тим, що «лідер думок» за своєю природою має і особистісні, і структурні переваги в порівнянні з іншими вузлами сегменту мережі.

В роботі запропоновано використовувати для вибору початкового вузла-генератора адаптований метод аналізу ієрархій. Як показали проведені експерименти, «лідери думок» за методом аналізу ієрархій отримують високу оцінку, але більш глибокий аналіз структри мержі та особистісних параметрів дозволяє вибрати альтернативу, що показує кращі результати ніж «лідер думок», з точки зору швидкості поширення інформації.

Таким чином, набув подальшого розвитку метод оптимального вибору цільового вузла для атаки в ході поширення впливів суб’єктом мережі на основі методу аналізу ієрархій та застосування поведінкових стратегій на основі наявних даних про мережу під час інформаційних протиборств. Застосування поведінкових стратегій суб’єктів інформаційних впливів на основі аналізу даних про мережу дозволяє підвищити швидкість поширення інформації в середньому на 70% в порівнянні з випадковим вибором вузлів для атаки. Вибір оптимального цільового вузла дозволяє за меншу кількість часу поширити ІВ серед вузлів сегменту мережі. Швидкість поширення ІВ через вузли, обрані за запропонованим методом, в експериментах на моделі, в середньому на 16% вища, ніж швидкість через вузли, обрані випадковим чином серед виграшних структурних позицій СМ. В порівнянні з запропонованим іншими авторами методом поширення ІВ через «лідера думок» приріст швидкості поширення ІВ через вузол вибраний по методу MAI склав 6%.

Ключові слова: інформаційна безпека, інформаційне протиборство, соціальні мережі, інформаційні впливи, імітаційне моделювання, соціальна мережі, кластер мережі, поведінкова стратегія.

ABSTRACT

Ulichev O. Model and methods of dissemination of information influences in social networks in the conditions of information confrontation - Qualifying research paper made as manuscript.

The dissertation on competition of a scientific degree of the candidate of technical sciences on a specialty 21.05.01 "Information security of the state". - National Aviation University, Kyiv, 2021.

The dissertation is devoted to solving the current scientific and technical problem of developing methods and tools for software modeling and implementation of various strategies for the dissemination of information influences in segments of social networks during the information confrontation in order to spread the speed of information influences.

The analysis of modern methods and models of dissemination of information influences in social networks in the conditions of information confrontation is shown, which showed that the vast majority of models and methods do not take into account individual characteristics of node, such as reputation, level of information resistance, node activity. Another disadvantage of these models is the fact that they do not take into account the behavior of an individual node, the information dissemination strategy chosen by the node in the process of informational influence. In fact, the strategy should be understood as a way to choose a node to attack among the available contacts of the subject of information influence.

A mathematical model of information influences distribution in the social network segment has been developed, which takes into account the individual characteristics of network nodes, which allows the application of different behavioral strategies by influencers based on analysis of available data on node parameters and their structural position.

A separate task is the direct generation of the network structure in the model. As a result of studying a number of proposed methods of generating network structure, it was found that the main disadvantages of the proposed methods are the inability to generate a network with a predetermined structure, as well as low clustering of networks obtained on the basis of previously proposed methods. Given the above, the proposed methods cannot be applied to generate a network segment based on available information about node characteristics and topological features.

The paper proposes an improved method of generating the structure of the social network segment, which allows you to choose the number and types of clusters of the social network segment. As clusters it is offered to choose group, leader group, clique - as the most widespread types of structural formations in real social networks. The proposed approach makes it possible to generate network segments with a predefined connection structure and available fixed subsets of nodes (groups, leadership groups, clique).

On the basis of the offered mathematical model of distribution of information influences algorithms of program simulation modeling of process of distribution of information influences in segments of a social network, and also algorithms of generation of structure of segments of a social network are developed.

Basic behavioral strategies of subjects of influence in the social network during information confrontations are developed, which allow to effectively model different approaches to the choice of target nodes by subjects of influence and the process of informational influence (II) dissemination. Among the proposed models are considered models without analysis of nodes-contacts - random selection of the node for the attack, and strategies with the analysis of a single characteristic or set of characteristics. It is obvious that the application of strategies based on the analysis of personal characteristics of nodes and their structural features should increase the speed of dissemination of information influences. The following characteristics of nodes were chosen as parameters for analysis: reputation, level of

information resistance. Structural features are determined by the number of contacts of the node, which is a potential contender for informational impact, and structural features of the nodes with which it contacts. The choice of strategy can be based on the available comprehensive information about the network segment, for example - if the network segment contains a significant number of nodes with high information resistance to the spreading idea, then to accumulate a critical mass of "like-minded" should analyze the information resistance. Accordingly, the dissemination strategy should be based on the analysis of the indicator "level of information resistance".

A number of experiments on the software model were conducted in the work, the purpose of which was to compare the speed of information influence propagation under different initial conditions and with the application of different strategies.

The experimental part of the work presents the average results of a series of experiments that confirm the hypothesis of the possibility of increasing the rate of dissemination of information influences through the use of strategies based on the analysis of available information about the network. Approaches to the choice of behavioral strategies of the subject of influence in the social network during the information confrontation are proposed, which allow to spread the information influence among the nodes of the social network segment in less time.

In addition to the strategy of dissemination of information influences, the choice of the location of the initial generator in the network segment is significant from the point of view of the speed of propagation. The most common approach proposed by a number of authors is to involve "opinion leader" in the process of informational influences (a node with a large number of contacts and a high level of informational influence, reputation). This approach is due to the fact that the "opinion leader" by its nature has both personal and structural advantages over other nodes of the network segment.

The paper proposes to use an adapted method of hierarchy analysis to select the initial generator node. Experiments have shown that "opinion leader" are

highly rated by hierarchy analysis, but a deeper analysis of the network structure and personality parameters allows you to choose an alternative that shows better results than a "opinion leader" in terms of speed of information dissemination.

Thus, the method of optimal selection of the target node for the attack during the spread of influences by the network entity based on the method of analysis of hierarchies and the application of behavioral strategies based on available data about the network during information conflicts. Applying the behavioral strategies of the subjects of information influences based on the analysis of network data allows to increase the speed of information dissemination by an average of 70% compared to the random selection of nodes to attack. Selecting the optimal target node allows you to spread II among nodes of the network segment in less time. The rate of propagation of II through the nodes selected by the proposed method, in the experiments on the model, is on average 16% higher than the rate through the nodes randomly selected among the winning structural positions of the SN (social network). In comparison with the method of II propagation proposed by other authors through the "opinion leader", the increase in the rate of II propagation through the node selected by the MAI method was 6%.

Key words: information security, information confrontation, social networks, information influences, simulation, social networks, network cluster, behavioral strategy.

Список публікацій здобувача:

1. Ulichev O., Meleshko Ye., Sawicki D., Smailova S. Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors // Proc. SPIE 11176, Wilga, Poland (ISSN: 0277-786X). – 2019. – Number article: 111761T. **(SCOPUS)**.

2. Ulichev O., Meleshko Ye., Smirnov O., Khokh V., Goncharenko Iu. The method of choosing objects for informational influence in social networks during information campaign based on the analytic hierarchy process // CEUR-

WS, Vol. 2588, Lviv, Ukraine (ISSN: 1613-0073). – 2019. – P. 215-227 **(SCOPUS)**.

3. Улічев О.С. Дослідження моделей розповсюдження інформації та інформаційних впливів в соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 4(50). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2018. – С. 147-151.

4. Улічев О.С. Математична модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник наукових праць ЦНТУ. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кропивницький: ЦНТУ, 2018. – Вип. 31. – С. 165-174.

5. Ulichev O., Meleshko Y., Khokh V. The computer simulation method of a social network structure for the research of dissemination processes of informational influences // Scientific and Practical Cyber Security Journal (SPCSJ) 4(3). – Georgia, Tbilisi, 2019. – P. 34-47.

6. Улічев О.С., Мелешко Є.В. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах // Збірник наукових праць " Сучасні інформаційні системи". Випуск 2(2). – Харків: ХПІ. – 2018. – С. 35-39.

7. Улічев О.С., Мелешко Є.В. Моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі // Науковий журнал «Захист інформації». – Київ: НАУ, 2020. – Т. 22, № 3. – С. 166-176.

8. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження робастності рекомендаційних систем з колаборативною фільтрацією до інформаційних атак // Наукове видання Кібербезпека: освіта, наука, техніка.– Київ: КУБГ, 2019. Т.1 № 5. – С. 95-104.

9. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження відомих моделей атак на рекомендаційні системи з колаборативною фільтрацією //

Збірник наукових праць Системи управління, навігації та зв’язку. – Полтава: ПНТУ, 2019. – № 5 (57). – С. 67-71.

10. Мелешко Є.В., Константинова Л.В., Улічев О.С. Дослідження властивостей інформації та методів її поширення з точки зору інформаційної безпеки в соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв’язку". Випуск 3(35). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2015. – С. 98-106.

11. Улічев О.С. Генерування моделі соціальної мережі для дослідження впливу її структури на розповсюдження інформаційних впливів // Збірник тез II Міжнародної науково-практичної конференції «Інформаційна безпека та комп’ютерні технології». м. Кропивницький. 20-22 квітня 2017 р. – Кропивницький: ЦНТУ. – 2017. – С. 103-104.

12. Улічев О.С., Мелешко Є.В. Програмна модель соціальної мережі та стратегій поширення інформаційно-психологічних впливів // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп’ютерні технології». м. Кропивницький. 19-20 квітня 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 136-220.

13. Улічев О.С., Мелешко Є.В. Математична модель розповсюдження інформації в сегменті соціальної мережі // Матеріали Двадцятого Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 13-14 квітня 2018 р. – Кропивницький: КЛА НАУ. – 2018. – С. 68-72.

14. Улічев О.С., Мелешко Є.В. Програмна модель розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Матеріали VIII Міжнародної науково-технічної конференції «ITSEC», м. Київ, 16-18 травня 2018 р. – Київ: НАУ. – 2018. – С. 34-35.

15. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез Сьомої міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 17-19 травня 2018 р. – Львів: Національний

університет "Львівська політехніка". – 2018. – С. 29-30.

16. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Збірник тез X Всеукраїнської науково-практичної конференції «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем(SITS'2018)»,21-23 червня 2018 року. – Миколаїв-Коблево: НАУ та МІПРО. – 2018. – С. 77–79.

17. Мелешко Є.В., Шингалов Д.В., Улічев О.С. Дослідження Баєсових мереж довіри як засобів для моделювання динамічних процесів у складних мережах // Матеріали XVII Міжнародної науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем», 20-22 листопада 2019 р. – Дніпро: ДНУ. – 2019. – С. 284-285.

18. Мелешко Є.В., Хох В.Д., Улічев О.С. Методи тестування робастності рекомендаційних систем з колаборативною фільтрацією // Матеріали Всеукраїнської науково-практичної Інтернет-конференції «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» 13-14 листопада 2019 р. – м. Кропивницький: ЦНТУ. – 2019. С. 88-89.

19. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження методів підвищення робастності рекомендаційних систем до інформаційних атак // Матеріали VI Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», 19-22 лютого 2020 р. – м. Київ: Вид-во Європейського університету, 2020. – С. 65-70.

ЗМІСТ

ВСТУП

Актуальність. Соціальні мережі (СМ) в наш час стали одним з основних джерел інформації для користувачів мережі Інтернет [1-3]. Вони надають інструменти для міжособової та масової комунікації, пошуку даних, перегляду новин, тощо. У той же час СМ стали зручним середовищем для поширення інформаційно впливів (ІВ) та маніпулювання суспільною думкою, що викликає загрози як для окремих користувачів, так і для суспільства і держави в цілому [4-8]. У сучасному світі однією з головних загроз інформаційній безпеці держави є саме ІВ через засоби масової інформації, соціальні медіа, тощо. На відміну від інформаційно-кібернетичних (інформаційно-технічних) впливів, які направлені на інформаційні ресурси, ІВ направлені на свідомість та підсвідомість людей. Вони мають на меті формування певних ідей, поглядів, уявлень, переконань, спонукання до певних дій або бездіяльності; одночасно він викликає у людей позитивні або негативні емоції, почуття і навіть бурхливі масові реакції.

З точки зору стрімкої глобалізації інформаційних процесів, входження України до світового інформаційного простору та інформаційної експансії з боку інших держав важливим є розробка методологічних основ забезпечення інформаційної безпеки держави.

Одними з найважливіших завдань забезпечення інформаційної безпеки держави є запобігання негативним інформаційним впливам на індивідуальну, групову та суспільну свідомість, захист від ворожої або недружньої пропаганди, створення технологій дослідження, захисту та контрзахисту людини, суспільства й держави від негативних наслідків інформаційно-психологічного впливу.

Сучасні наукові роботи, спрямовані на дослідження ІВ в умовах інформаційного протиборства (роботи науковців В. Горбулін, А. Пую, О. Додонов, В. Хорошко, Г. Почепцов, С. Розторгуєв, Р. Грищук, К. Молодецька) розглядають два напрямки:

– методи нападу: формування, поширення та використання ІВ.

– методи протидії: виявлення, прогнозування наслідків та захист від ІВ.

Оскільки СМ є одним з каналів поширення ІВ, актуальною є задача дослідження процесу поширення таких впливів СМ для розробки методів прогнозування наслідків та методів захисту. СМ та процеси, що у них протікають, на даний час активно досліджуються різними науковцями, однак розвиток СМ значно випереджає темпи наукових досліджень. Дослідження інформаційних атак на СМ шляхом їх моделювання дозволить розробити і реалізувати превентивні та контрзаходи для запобігання негативним ПІВ на індивідуальну, групову та суспільну свідомість, захист від ворожої або недружньої пропаганди. Також, це дозволить розробити науково-методичні засади і технології захисту людини, суспільства й держави від негативних наслідків ІВ.

Роботи науковців, спрямовані на дослідження процесів поширення ІВ (не технічних) у СМ, можна поділити на такі основні групи:

1) застосовують збір та аналіз даних з відкритих частин веб-ресурсів СМ, парсинг і аналіз даних (Д. Ланде, Р. Гумінський, Т. Батура, Є. Князєва Є., Б. Хоган).

2) використовують математичне та програмне моделювання СМ та процесів у них, застосування теорії комплексних мереж в умовах інформаційного протиборства (А.Барабаши, Р. Альберт, Б. Боллобаш, О. Ріордан, П. Ердьош, А. Реньї, П. Баклі, Д. Остхус, Дж. Чаес, К. Боргс, М. Грановветер, Д. Губанов, А. Чхартишвили, Д. Горковенко, І. Гончаров, Б. Торопов, Д. Ланде).

3) досліджують інформаційні атаки та ІВ на СМ (В. Горбулін, А. Пую, О. Додонов, В. Хорошко, Г. Почепцов, С. Розторгуєв, Р. Грищук, К. Молодецька).

Сучасні СМ використовують різні методи протидії парсингу інформації з їх веб-ресурсів, зокрема, зростає об’єм закритої частини інформації, а на збір відкритої інформації створюють значні часові затримки, тому все

актуальнішою стає друга група методів. Імітаційні моделі СМ дозволяють проводити дослідження процесів, що у них протікають, без значних часових та фінансових затрат та без доступу до даних, які відкриті тільки власникам веб-ресурсів. Проведений аналіз показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла соціальної мережі (вузол – користувач СМ), а саме поведінку окремого вузла, стратегію розповсюдження інформації, яку обирає вузол в процесі ІВ тощо. З огляду на зазначене, розроблення методів і засобів моделювання та реалізації різних стратегій поширення ІВ у сегментах СМ є *актуальною науково-технічною задачею*, що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у межах пріоритетних наукових напрямів, які охоплюють актуальні проблеми, відповідно до рішення Ради президентів академій наук України від 30 січня 2019 року «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019-2023 роки», «Інформатика» за темою: «Розроблення обчислювальних алгоритмів і процедур з метою вирішення практичних задач міждисциплінарного характеру для застосувань, що належать до науково-технічної та соціально-економічної сфер діяльності людини», «Наукова інформація» за темою: «Соціальні мережі, формування в Україні інформаційного суспільства». Дисертаційну роботу виконано у межах зареєстрованих НДР Центральноукраїнського національного технічного університету: «Моделювання та аналіз складних мереж та інформаційних систем» (№ д.р. 0119U003587), «Методи використання інформаційних технологій та інтелектуальних систем для аналізу даних та забезпечення інформаційної безпеки суспільства» (№ д.р. 0116U008161) та «Методи підвищення оперативності передачі даних та захисту інформації у телекомунікаційній мережі» (№ д.р. 0112U006631).

Мета і задачі дослідження. Мета дисертаційної роботи – підвищення швидкості поширення інформаційних впливів у соціальних мережах за рахунок оптимального вибору об’єктів впливу.

Мета дисертаційної роботи визначає необхідність розв’язання таких **основних задач:**

1. Дослідити методи генерації мереж і моделі поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства.
2. Розробити математичну модель поширення інформаційних впливів в сегменті соціальної мережі з врахуванням особистісних характеристик вузлів мережі, що дає можливість, на основі аналізу запропонованих характеристик, застосувати різні поведінкові стратегії суб’єктами інформаційного впливу.
3. Удосконалити метод генерації сегменту соціальної мережі з можливістю моделювання різних варіантів структури сегменту мережі за рахунок обрання різної кількості та різних типів кластерів соціальної мережі.
4. Удосконалити метод оптимального вибору цільових вузлів соціальної мережі суб’єктами поширення інформаційного впливу під час інформаційного протиборства, а також метод вибору поведінкових стратегій суб’єктів впливу на основі наявної про мережу інформації.
5. Провести експериментальне дослідження програмної моделі, що підтверджує ефективність запропонованих методів, з точки зору швидкості поширення інформаційних впливів в сегменті соціальної мережі

Об’єктом дослідження є процес поширення інформаційних впливів у сегменті соціальної мережі.

Предметом дослідження є методи моделювання соціальних мереж та моделі поширення у них інформаційних впливів в умовах інформаційного протиборства.

Методи дослідження. Для вирішення завдань математичного моделювання структури соціальної мережі та процесів поширення

інформаційних впливів використано теорію графів, теорію складних мереж, теорію множин. Для створення програмної моделі на основі розробленої математичної моделі використано методи об'єктно-орієнтованого програмування, методи візуалізації графів та алгоритми роботи з графами. Для моделювання об'єктів та суб'єктів впливу в соціальних мережах, їх характеристик та стратегій поведінки використовувалися теорія множин, основи соціальної психології, теорія інформаційних протиборств.

Наукова новизна одержаних результатів полягає у такому:

– *вперше розроблено* математичну модель поширення інформаційних впливів у сегменті соціальної мережі, яка за рахунок параметризації особистісних характеристик вузлів мережі, а саме – введення параметрів вузла: активність, репутація, залученість до ідеї, інформаційний спротив, дає можливість застосування різних поведінкових стратегій суб'єктами інформаційного впливу на основі аналізу параметрів атакованих вузлів;

– *удосконалено* метод генерації структури сегменту соціальної мережі, який за рахунок комбінування структури мережі з набору параметризованих кластерів і вибору їх топологічних особливостей, дозволяє генерувати мережу з наперед заданою структурою;

– *набув подальшого розвитку* метод поширення інформаційних впливів у сегменті соціальної мережі під час інформаційного протиборства, який відрізняється від існуючих застосуванням методу аналізу ієрархій для здійснення оптимального вибору цільового вузла мережі, а також застосуванням та вибором різних поведінкових стратегій суб'єктом інформаційного впливу на основі наявної інформації про мережу, що дозволяє за меншу кількість часу поширити інформаційний вплив серед вузлів соціальної мережі за рахунок вибору оптимальних початкового цільового вузла та стратегії поширення інформації.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати дають змогу здійснити програмне імітаційне

моделювання процесу поширення інформаційних впливів у сегменті соціальної мережі та вибір поведінкових стратегій суб'єкту впливу під час інформаційного протиборства.

Практична цінність роботи полягає у такому:

– розроблено алгоритми генерації структури сегментів соціальної мережі, що дають можливість моделювати сегмент мережі з наперед заданою структурою зв'язків, розроблено програмну імітаційну модель поширення інформаційних впливів у сегменті соціальної мережі під час інформаційного протиборства та алгоритми моделювання і вибору різних поведінкових стратегій суб'єктів впливу, що дозволяє аналізувати та прогнозувати поширення інформаційних впливів у соціальних мережах з використанням різних поведінкових стратегій;

– застосування поведінкових стратегій суб'єктів інформаційних впливів на основі аналізу даних про мережу дозволяє підвищити швидкість поширення інформації в середньому на 70% в порівнянні з випадковим вибором вузлів для атаки. Швидкість поширення ІВ через вузли, обрані за запропонованим методом, в середньому на 16% вища, ніж швидкість поширення через інші вузли, що мають виграшні структурні позиції. В порівнянні з запропонованим іншими авторами методом поширення інформаційних впливів через «лідера думок» приріст швидкості поширення інформаційних впливів через вузол вибраний за адаптованим МАІ склав 6%.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження. Результати дисертації впроваджені і використовуються у діяльності таких організацій як ТОВ «Сайфер БІС», що розробляє програмні системи захисту інформації, а також використано у навчальному процесі Центральноукраїнського національного технічного університету для покращення викладання дисциплін «Інформаційна безпека держави», «Спеціальні розділи математики для інформаційної безпеки» та «Прогнозування та моделювання в соціальній сфері», що підтверджено відповідними актами.

Особистий внесок здобувача. У друкованих працях, опублікованих у співавторстві, здобувачеві належать: [9] – дослідження методів поширення інформації у соціальних мережах з точки зору інформаційної безпеки держави; [20] – математична модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі; [12-14, 19, 21-23] – програмна модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі з різними стратегіями поведінки суб'єктів впливу; [15, 25, 26] – дослідження впливу інформаційних атак на соціально-інформаційні системи; [16] – дослідження різних видів інформаційних атак на соціально-інформаційні системи; [17] – метод вибору цільового вузла суб'єктом інформаційних впливів соціальної мережі під час інформаційних протиборств; [24] – дослідження моделей складних мереж.

Апробація результатів дисертації. Основні результати наукових досліджень неодноразово доповідалися на міжнародних та всеукраїнських наукових конференціях та семінарах, зокрема:

II Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» (м. Кропивницький, 20-22 квітня 2017 р.);

III Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» (м. Кропивницький, 19-20 квітня 2018 р.);

XX Міжнародний науково-практичний семінар «Комбінаторні конфігурації та їх застосування» (м. Кропивницький, 13-14 квітня 2018 р.);

VIII Міжнародна науково-технічна конференція «ITSEC» (м. Київ, 16-18 травня 2018 р.);

VII Міжнародна наукова конференція "Інформація. Комунікація. Суспільство" (м. Львів, 17-19 травня 2018 р.);

X Всеукраїнська науково-практична конференція «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2018)» (Миколаїв-Коблево, 21-23 червня 2018 р.).

Міжнародна науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем» (Дніпро, 2019 р.).

Всеукраїнська науково-практична Інтернет-конференція «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» (Кропивницький, 2019 р.).

Результати дисертаційних досліджень регулярно доповідалися на наукових семінарах кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Публікації. Основні положення дисертації опубліковано в 19 наукових працях, у тому числі: 10 наукових статей (з яких 2 опубліковані у закордонних рецензованих виданнях та 2 входить до бази даних Scopus), 6 – у вітчизняних фахових наукових журналах), а також 9 матеріалів і тез доповідей на конференціях.

Структура та обсяг роботи. Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 143 сторінки основного тексту, 51 рисунків, 14 таблиць, 12 сторінок додатків. Список використаних джерел містить 115 найменувань і займає 13 сторінок. Загальний обсяг роботи 170 сторінок.

РОЗДІЛ 1
СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Інформація завжди була важливим фактором суспільного розвитку. З її допомогою людство концентрувало багатовіковий досвід життя попередніх поколінь. Подальший соціальний розвиток, безумовно, буде в першу чергу пов'язаний з інформатизацією. Володіння інформацією відкриває нові моделі управління, формує нові соціальні структури суспільства.

Останнім часом, за рахунок розвитку комунікацій та засобів зв'язку, до яких відносяться і соціальні мережі, територіальні та інші перешкоди в інформаційному обміні абсолютно знівельовані.

В дослідженні соціальні мережі розглядаються як засіб інформаційних атак і, за участю різних технологій, засіб навіювання і нав'язування певних ідей та інформаційних посилів. Так як соціальна мережа є об'єктом моделювання з метою дослідження, то, первинно, варто визначити саме поняття - «соціальна мережа», охарактеризувати її структуру, особливості інформаційних зв'язків і функціонування.

Соціальні мережі – один із популярних Інтернет сервісів для створення віртуальних спільнот, якими користується 90 % користувачів українського Інтернет середовища.

1.1. Соціальні мережі як засіб інформаційного обміну, методи аналізу соціальних мереж та інформаційних процесів у них

Соціальна мережа (Social service networks) являє собою Інтернет сервіс, сайт (частіше Інтернет-портал), який дає змогу зареєстрованим на ньому користувачам розміщувати інформацію про себе, спілкуватися між собою, налагоджуючи соціальні зв'язки, обмінюватись контентом. На основі

технологій web 2.0 контент на цьому сервісі створюють безпосередньо самі користувачі [1].

Соціальна мережа – соціальна структура, що складається з групи вузлів, якими виступають суб'єкти (люди чи організації, спільноти людей) і інформаційні зв'язки між ними [55].

Сучасний рівень розвитку та популярності соціальних мереж (як сервісу) у користувачів завдячує наступним можливостям, що надаються користувачеві подібними сервісами [2, 3]:

– можливість спілкування з різними учасниками мережі в режимі реального часу. При цьому користувач обирає найбільш зручний для себе спосіб: текстові повідомлення, голосовий чи відео-зв'язок;

– інформаційний обмін, отримання інформації від інших учасників мережі;

– можливість пошуку та фільтрації, зручна навігація по контенту, що представлений іншими учасниками мережі;

– можливість створення внутрішніх спільнот (групи) об'єднаних спільними інтересами чи ідеями, підтвердження своїх ідей в таких спільнотах їх просування в маси та розповсюдження.

Наявність такого набору можливостей в сервісах зумовили їх напрямки використання [4, 5, 6, 7] та певні переваги СМ. На ряду з основною функцією – спілкування окремих людей, СМ почали широко використовуватись для:

– використання соціальних мереж як засобів масових комунікацій: вузького спрямування – в межах певної групи чи організації, широкого спрямування – електронні засоби масової інформації (електронні газети, журнали, новинні сайти);

– використання СМ як засобів політичної боротьби та агітації;

– використання сторінок соціальних мереж для об'єднання користувачів соціальних мереж та їх комунікації;

– поєднання і інтеграція традиційних ЗМІ в віртуальний простір: забезпечення двостороннього зв’язку з аудиторією, розширення кола користувачів (читачів, глядачів ЗМІ);

– зростання рівня довіри до соціальних медіа з боку аудиторії (який в середньому в декілька разів перевищує довіру до традиційних ЗМІ);

– перенесення медіа війн та інформаційного протистояння в середовище СМ, використання соціальних мереж для пропаганди та просування певних ідей.

Перевага в соціальних мережах направлено на адаптацію перевіреного і широко доступного програмного забезпечення і систем, які здаються зручними для користувачів. Прості правила і робочі процедури є відмінною рисою широкого впровадження інструментів соціальних мереж. Чим більше інтуїтивним є інструмент, тим більша ймовірність того, що він буде схвалений. І там має бути щось для користувачів. Користувачі звертаються до соціальних мереж тому, що вони вважають, що участь принесе їм ту перевагу, яку вони хочуть отримати.

Все вищезазначене приводить до того, що кількість користувачів соціальних мереж зростає з кожним роком. Аудиторія соціальної мережі «Facebook» перевищує мільярда користувачів, «Twitter», «Vk.com» та «Google+» – більше ніж 200 мільйонів, «LinkedIn» та «Odnoklassniki.ru» – понад 100 мільйонів [27].

Методи дослідження, безпосередньо, соціальних мереж здебільшого наслідувані від методів дослідження мережі в широкому розумінні цього поняття. Соціальні мережі мають структуру та характеристики взаємодії між вузлами в загальному подібні до мережі в широкому розумінні цього терміну. Загалом соціальна мережа визначається як граф:

$$G\,(V, E), \tag{1.1}$$

де V – множина вузлів (користувачів СМ), а E – множина ребер (контакти між користувачами СМ).

У випадку соціальної мережі граф утворюють взаємодіючі користувачі (виступають вузлами в графі), а ребрами виступають інформаційні зв'язки між користувачами. Соціальна мережа може трактуватись і як соціальна структура і як реалізація такої структури з використанням інформаційних технологій та засобів мережі Інтернет. Технічні особливості реалізації дозволяють підвищити динаміку зв’язків, розширити доступ (збільшити множину можливих контрагентів для встановлення зв’язків), але, в той же час, не мають вирішального впливу на структуру мережі.

Вперше поняття графа-мережі ввів математик Л. Ейлер, запропонувавши задачу про обхід контрольних точок міста з обмеженою кількістю мостів. Пізніше дане математичне представлення широко використовували для моделювання різноманітних задач та структур.

Слід зазначити, що області застосування мережевого аналізу найрізноманітніші:

– в економіці та управлінні це: організаційний консалтинг; внутрішні та зовнішні взаємодії організацій; аналіз ринків; мережі соціальної та економічної підтримки індивідів і домогосподарств; тіньова економіка; реклама; дослідження вподобань та вплив на вибір користувачів послуг чи товарів;

– в соціології - когнітивний аналіз; історіографічний аналіз; наукові мережі; професійні групи і т.д.

– в медицині та біології - мережі поширення інфекційних захворювань; мережі підтримки у душевнохворих;

– в криміналістиці - мережі розповсюдження наркотиків; терористичні мережі; злочинні угруповання.

Конкретно соціальні мережі досліджуються різними науками, до переліку варто віднести: соціологію, психологію, економіку, математику та аналіз.

У 1930-х рр. Дж. Морено опублікував серію робіт по соціометрії, присвячену міжособистісних і міжгрупових відносин [74]. Основний

інновацією наукових робіт Морено прийнято вважати соціограму, як схематичне зображення структури міжособистісних відносин в малій соціальній групі. Своїми експериментами Дж. Морено фактично поклав початок аналітичного дослідження соціальних мереж [75]. А. Бейвлас і Х. Левітт [68] розглядали мережу як сукупність позицій, а не індивідів в якості вузлів. В роботах А. Бейвласа вперше з'являється згадка про централі, а також запропонована ідея розглядати зв'язки як потоки ресурсів.

У другій половині XX в. істотно розширився системний аналіз соціальних мереж в роботах таких дослідників, як Р. Соломонофф, С. Берковіц, С. Боргетті, Р. Берт, К. Карлі, К. Фост, Д. Нок, П. Марсден, Н. Маллинс, А. Рапопорт, С. Уоссермен, Б. Веллмен, Д. Вайт, В. Харрісон і багатьох інших. У 1950-ті рр. англійські антропологи Дж. Барнес і Е. Ботте звернули увагу на соціальний феномен – утворення соціальних угрупувань (соціальних мереж), зокрема, термін «соціальна мережа» було введено в 1954 р. соціологом Джеймсом Барнсом [76]. В 1959-1968 рр. угорські математики Пол Ердос і Альфред Реньї опублікували ряд статей, що описують принципи формування соціальних мереж. Вчені вперше застосували математичну теорію для ілюстрації принципу побудови соціальних мереж. Запропонована теорія випадкових графів дозволила описувати складні мережі, які не мають очевидних принципів побудови [77].

Ще більшої зацікавленості та конкретизації тематика досліджень набула в кінці XX на початку XXI століть. Варто згадати роботи авторів Вебера К., Сазанова В., Батури Т., Губанова Д., Градосельской Г., Чхартішвілі Г., Б. Хогана , П. Лайнбарджера та багатьох інших.

Така зацікавленість даним об'єктом (соціальними мережами) пояснюється тим фактом, що сьогодні СМ це альтернативний засіб спілкування та інформаційного обміну між людьми, що включає мільйони, а у випадку найбільших мереж вже мільярди користувачів. За масштабністю та активністю інформаційного обміну з соціальними мережами не може зрівнятись жоден інший засіб інформаційного обміну (за виключенням

Інтернету в цілому). Від так соціальні мережі стають інструментом масового впливу, розповсюдження цільової інформації, реклами, пропаганди, тощо. Природно виникають протилежні задачі: оптимізувати та підвищити ефективність розповсюдження інформації і, як наслідок, посилити інформаційний вплив та вироблення методик і засобів протидії інформаційним впливам. І перша і друга задачі вимагають всебічного аналізу мережі.

Мережу взаємодії можна проаналізувати різними методами теорії графів, теорії інформації та математичної статистики. Класифікацію методів мережевого аналізу пов'язують як з напрямками досліджень, так і з конкретними завданнями (етапами) мережевого аналізу. В даний час в аналізі соціальних мереж виділяють чотири основні напрями досліджень: структурний, ресурсний, нормативний та динамічний. Ці напрямки сформулював М. Доверн [73], в подальшому ця класифікація підтримана багатьма дослідниками соціальних мереж, наприклад - [70-72].

У структурному підході всі учасники мережі розглядаються як вершини графа, які впливають на конфігурацію ребер і інших учасників мережі. Основна увага приділяється геометричній формі мережі і інтенсивності взаємодій (вазі ребер), тому досліджуються такі характеристики, як взаємне розташування вершин, центральність, транзитивність взаємодій. Основною задачею структурного підходу є пошук підмножин з характерними конфігураціями, встановлення найбільш вагомих вузлів з точки зору зв’язку між окремими підмножинами мережі. При структурному аналізі та аналізі поведінки зв'язків використовуються методи статистичного аналізу, методи визначення спільнот, алгоритми та класифікації мереж за різними критеріями.

Ресурсний підхід розглядає можливості учасників на предмет залучення індивідуальних і мережевих ресурсів для досягнення певних цілей і диференціює учасників, що перебувають в ідентичних структурних позиціях соціальної мережі, по їх ресурсам. Під мережевими ресурсами

розуміються вплив, статус, інформація, капітал. Основним ресурсом є інформація, особливістю цього ресурсу є невичерпність – при передачі ресурсу від одного вузла до іншого кількість інформації у першого не зменшується. Кількість знань та інформації окремого вузла і запас знань мережі в цілому постійно зростає та накопичується.

Нормативний напрямок вивчає рівень довіри між учасниками, а також норми, правила і санкції, які впливають на поведінку учасників в соціальній мережі і процеси їх взаємодій. В цьому випадку аналізуються соціальні ролі, які пов'язані з окремим ребром мережі або вибраною підмножиною. Основним визначальним чинником в даному підході розглядається набір формальних правил, технічних можливостей та обмежень, що впливають на формування поведінкових моделей вузлів та визначення стратегій.

Динамічний підхід розглядає різного роду зміни (в першу чергу структурні) мережі з плином часу. Методами, що застосовуються в рамках динамічного підходу, є математичне моделювання та засоби візуалізації. Важливим є створення алгоритмів які поєднують методи аналізу і візуалізації для унаочнення та спрощення розуміння структури і динаміки інформаційних процесів в мережі. До основних задач, в рамках динамічного підходу, варто віднести прогнозування структурних змін, планування стратегій та перевірку ефективності поведінкових моделей. Окремим напрямком є дослідження залежності динаміки від початкової структури та впливи зовнішніх чинників на структурні зміни в часі, утворення відносно стаціонарних підструктур та кластерів.

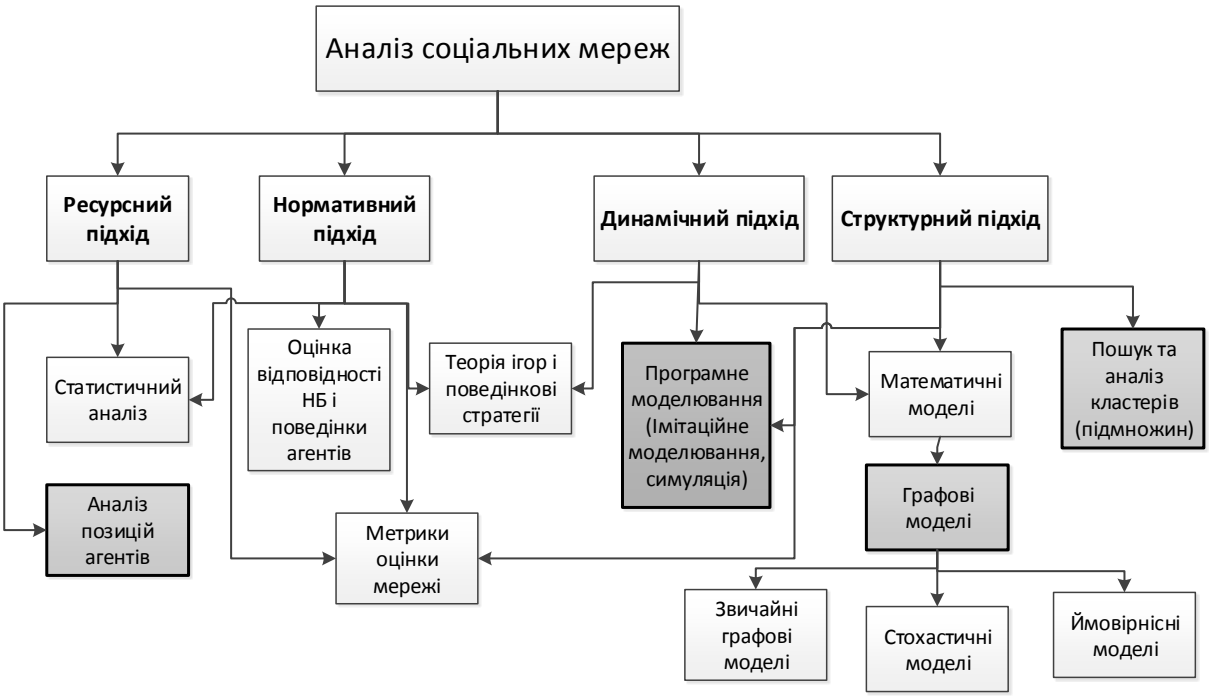


Рисунок 1.1 – Підходи і методи аналізу соціальних мереж

Розвиток соціальних мереж сприяє задоволенню потреб користувачів, вони пропонують низьку сервісів для їх комунікації:

Публічні сторінки – переважно їх організовують різні організації або окремі особистості, як відкриті джерела для всіх, кого хоч трохи цікавить тема сторінки. Наповнювати контент може тільки адміністрація, учасники соціальної мережі мають змогу лише підписуватися на сторінку і стежити за подіями та коментувати записи.

Групи, в яких люди можуть спілкуватися, ділитися інформацією та взаємодіяти, але тільки в межах заданої теми або ідеї, тобто група має ознаки тематичних дискусій. Можливе гнучке налаштування дій, які будуть доступні користувачам.

Групи поділяють на закриті та відкриті. У відкритій групі доступ до інформаційного наповнення сторінки мають всі зареєстровані користувачі соціальної мережі. В закритій групі доступ до інформаційного наповнення сторінки мають тільки зареєстровані в групі користувачі. Реєстрацію користувача в групі здійснюється тільки адміністратори групи. Отже, для інформаційного впливу на користувачів соціальної мережі доцільно

розглядати відкриті групи, в яких доступ до інформаційного наповнення необмежений.

Зазвичай з однієї тематики створюються велика кількість груп, що крім тематики інформаційного наповнення, можуть відрізнятися:

– віковими ознаками;
– регіональною або територіальною ознакою;
– мовою спілкування;
– прихильністю до політичних партій тощо.

Заходи – призначені для анонсування подій.

В соціальних мережах формуються віртуальні спільноти, основна діяльність яких полягає в інформаційному обміні, що являють собою сукупність дискусій, об'єднаних відповідно до їх інформаційного наповнення та тематичної спрямованості повідомлень і дописів, контенту яким обмінюються учасники дискусії.

Фактично соціальна мережа являє собою комплексну віртуальну конструкцію, що включає три основні складові: користувачі, сервіси, контент.

Користувачі – зареєстровані користувачі соціальної мережі, які беруть участь у спільнотах, зареєструвавшись, та взаємодіють, створюючи інформаційне наповнення на сторінці дискусії.

Інформаційне наповнення (контент) – це текстовий, візуальний чи звуковий контент, який створюють учасники спільноти. Може містити: текст, зображення, звук, відео та анімацію, а також посилання на інші ресурси інтернет.

Спостерігаються ознаки децентралізованої ієрархії учасників віртуальної спільноти (принцип полікерівництва), які розподіляються відповідно до їхньої ролі під час існування спільноти [28, 29]:

– незареєстровані учасники (гості) – можуть лише переглядати (не завжди в повному обсязі) інформаційне наповнення спільноти;

– зареєстровані учасники – можуть переглядати повідомлення, брати участь у дискусіях і опитуваннях та створювати їх, коригувати свої повідомлення;

– модератори – крім можливостей, які мають зареєстровані учасники, модератори виконують функції управління контентом: коригування інформаційного наповнення – видалення некоректних, беззмістовних повідомлень та таких, що не відповідають чи суперечать ідеології спільноти, залучення нових учасників;

– адміністратори – в ієрархії спільноти мають найвищий статус: окрім функцій модератора, виконують функції реєстрації учасників, блокування порушників, призначення модераторів; основне їх завдання – управління спільнотою та технічна підтримка.

Модераторів спільноти вибирають з-поміж зареєстрованих учасників спільноти, які повністю підтримують її ідеологію та беруть активну участь у її функціонуванні. Адміністратори спільноти можуть не підтримувати ідеологію, а виконують функції щодо створення спільноти замовниками. В ролі замовника можуть виступати як окремі особи або організації, які зацікавлені в пропагуванні ідеології для досягнення визначеної мети.

Процес спілкування та функціонування особистих сторінок користувачів мають ряд особливостей:

– сторінки мають низький ранг в алгоритмах ранжування сторінок, що ускладнює пошук цих сторінок;

– велику кількість сторінок спільнот не ранжують глобальні пошукові системи;

– отримати доступ до інформації в дискусіях соціальних мереж може лише зареєстрований користувач соціальних мереж, а в закритих дискусіях – тільки учасник дискусії;

– значна частина відвідувачів потрапляє на сайт за безпосередньою рекомендацією інших користувачів;

– взаємопов’язаність сторінок дискусій;

– збереження дискусій неактуальної тематичної спрямованості;

– анонімність або спотворення даних про себе самими користувачами соціальних мереж.

Вище вказані особливості інформаційного обміну та функціонування окремих спільнот в СМ дають смогу використовувати СМ в якості інструменту інформаційного впливу. Соціальні мережі створюють нові загрози, оскільки держава вже не здатна контролювати їх в повному обсязі [31].

1.2. Методи розповсюдження інформаційних впливів у соціальних мережах під час інформаційного протиборства

У соціальних мережах, як і в Інтернет мережі в цілому, користувачі можуть зустрічатися з наступними видами інформаційних загроз:

1) загрози порушення конфіденційності, доступності та цілісності інформації;

2) загрози наявності інформаційно-психологічних впливів, порушення достовірності, повноти, об’єктивності, адекватності, корисності.

У даній роботі зосередимося на дослідженні другої групи загроз, оскільки соціальні мережі на сьогоднішній день все частіше стають для зловмисників інструментом для здійснення інформаційних впливів як на окремих користувачів для реалізації різних методів соціальної інженерії, так і на цілі соціуми та держави під час інформаційних протиборств та воєн.

Вплив – процес і результат зміни індивідом (суб'єктом впливу) поведінки іншого суб'єкта (індивідуального або колективного об'єкта впливу), його установок, намірів, уявлень і оцінок (а також дій, ґрунтуються на них) в ході взаємодії з ним [60].

В розрізі тематики дослідження необхідно конкретизувати дане означення: під впливом будемо розуміти інформаційний (інформаційно-

психологічний) вплив, а зміна поведінки – зміна думки відносно певної інформаційної ідеї (посилу).

Інформаційний вплив – вплив словом, інформацією; його метою є формування певних ідеологічних (соціальних) ідей, поглядів, уявлень, переконань; одночасно він викликає у людей позитивні або негативні емоції, почуття і навіть бурхливі масові реакції [62].

На відміну від традиційної реальності, віртуальна є більш терпимою відносно різних суспільних проблем. Цифрові мережеві зв'язки є основою сучасного мережевого суспільства, можна говорити про те, що віртуальні соціальні мережі мають претензію на статус глобальних.

СМ це середовище, де практично відсутня соціальна ізоляція і соціальні ізгої. Однак, наряду з відчутними плюсами, беззаперечним є послаблення соціального контролю в середовищі, в якій співіснує і взаємодіє величезна кількість людей, зокрема така соціальна група, як молодь. Дана категорія, в силу відсутності чітко сформованої життєвої позиції та вікових особливостей, є найбільш вразливою до інформаційних впливів та маніпуляцій.

В частково формалізованих моделях та представленнях мереж дослідники в області соціології та психології розділяють користувачів мережі на **агентів (акторів)** – активні (інколи інформаційно-агресивні) учасники мережі і **звичайні вузли** – учасники мережі на яких направлено інформаційний вплив.

Набір соціальних цінностей, які поділяє і пропагує агент, впливає на формування психологічних установок, думок і ставлення до соціальної ситуації у навколишніх вузлів. Агенти спільноти, маючи більш високий соціальний статус, ніж вузли, вони стають «front man» спільноти. Сам факт спілкування з агентом може сприйматися як доказ належності до віртуальної еліти даного соціального утворення (певної групи в мережі). Агенти (актори) – це люди, а точніше їх соціальні ролі, що впливають на вузли своєї гілки соціальної мережі значно більше, ніж інші суб'єкти [67]. Агенти формують

звичаї і традицій, поведінкові моделі в своїй соціальній групі, встановлюють цілі, які переслідує дане співтовариство, виконують функції інтеграції (виконання цільових заходів по залученню нових членів до спільноти), соціалізації (прийняття норм і координація), ідентифікації (розробка спеціальних механізмів виду «свій – чужий»), консервативна функція (розробка методик утримання популяції співтовариства) Крім усього іншого, агент регулює комунікативні процеси в мережі, якщо володіє достатнім для цього багажем знань безпосередньо в сфері, яка є профільною для даного співтовариства. Виконуючи весь спектр функцій, агент впливає та формує емоційний стан інших учасників спільноти, а постійна турбота про збереження власного авторитету й репутації спільноти, профілактика дезінтеграції вузлів, підсилює позиції спільноти серед подібних і тим самим закріплює й підсилює позицію агента в конкретній спільноті. Ідея встановлення зв'язку звичайних вузлів і агентів методом інформаційної активності висувається комунікаційними експериментами, які проводили Е. Бейвлес і Г. Лівітт [68]. Досліджуючи впливи в віртуальних мережах, дослідники соціальної реальності Інтернету [43] висувають гіпотезу, що вся інтернет-реальність являє собою складну багатогранну соціальну мережу, топологія якої являє собою сукупність топологій форм, іменованих «зірка» (рис. 1.2).

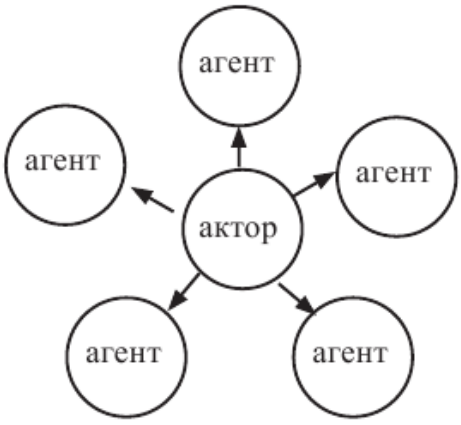


Рисунок 1.2 – Підмножина типу «Лідерська група»

Фактично запропонована автором базова топологія являє собою

підмножину розглянуту в п. 1.3 – «лідерська група».

Найважливішим індикатором положення людини в групі вважається рівень його активності, тобто кількість дій чи комунікацій. З цієї точки зору, агента можна визначити як центр або вузол комунікативної мережі, який замикає інформацію на себе. Статусна величина в соціальній мережі визначається кількістю, характером і особливостями взаємодії агента з іншими вузлами даної соціальної підгрупи. Чим більше переваг і «виборів» отримує агент в процесі внутрішньо мережевого спілкування, тим стійкіша його позиція і вища оцінка його статусу як серед учасників групи, так і в зовнішньому середовищі (звідки агент вербує потенційних членів своєї групи). Зростає і рівень стійкості самої особистості (психологічний стан агента як реальної людини) агента в своїх поглядах, агент менше піддається груповому тиску.

Спостереження психологів [69] показали, що в соціальній мережі звичайні вузли не мають достатньої кількості інформації для прийняття об'єктивного власного рішення, тому їх думки можуть ґрунтуватися на спостережуваних ними рішеннях інших вузлів. Це обумовлено таким явищем, як соціальний вплив або «ефект натовпу». Соціальний вплив реалізується в двох процесах: комунікації (в ході обміну досвідом та інформацією, обговорення тих чи інших питань з авторитетними для вузла іншими звичайними вузлами або агентами; так вузол формує певні уявлення, думки та ідеї, що, оманливо, можуть здаватися для вузла власними) і порівняння (очікувані від вузла дії, прийняті агентом для отримання зворотного зв'язку й соціального схвалення). Людина оцінює, як повів би себе референт даної групи, і, порівнюючи себе з ним, визначає адекватність свого рішення, згодом приміряючи на себе відповідну роль. Необхідно відзначити, що при комунікативному процесі соціального впливу вузли можуть прийти до подібних висновків, проте поведінка може бути абсолютно різною. При порівняльному процесі вузол не опосередковано копіює поведінку лідера своєї групи або вузла з вищим рівнем авторитету.

Донесення потрібної інформації до об’єкту впливу може відбуватися за допомогою **соціально-інформаційних вірусів** – мемів. Мемом може стати будь-яка інформація: ідея, образ, символ. Передаватися у соціальних мережах мем може у вигляді тексту, зображення, відео тощо.

Інформація стає вірусною та починає розповсюджуватися без особливих зусиль з боку суб’єкта впливу, якщо виконуються наступні принципи [64]:

– *Дана інформація є соціальною валютою* (розповсюдження певного мему дозволяє агенту соціальної мережі показати себе в очах інших експертом, цікавим співрозмовником, VIP-персоною тощо).

– *Дана інформація містить тригери* – стимули, що викликають асоціації, спонукають замислитися про мем при згадках про схожі популярні речі.

– *Дана інформація викликає емоції* (благоговіння, натхнення, втіху, гнів, занепокоєння). В [65] автор виділяє набір емоцій, які використовуються при поширенні пропаганди: страх, гнів, радість, – при маніпулюванні ними поширювана інформація перестає сприйматися критично.

– *Дана інформація має соціальний доказ* – об’єкт впливу повинен бути переконаний, що певну думку розділяє багато людей з його оточення.

– *Дана інформація має практичну цінність* для оточуючих об’єкта впливу.

– *Дана інформація міститься в цікавій історії,* переповідання якої пожвавлює спілкування.

Меми в соціальних мережах можуть поширювати з різними цілями: маркетинговими, політтехнологічними, соціальними, розважальними тощо.

Окремим видом впливу варто виділити пропаганду.

Пропаганда – планомірне використання будь-яких форм суспільних або масових комунікацій для того, щоб здійснювати вплив на розум та почуття певної групи населення з чітко визначеною суспільною, економічною, воєнною або політичною метою [66]. В [66] наводяться

наступні типи пропаганди:

1. За часом дії:

– Стратегічна пропаганда – призначена для досягнення мети через декілька тижнів, місяців або років.

– Тактична пропаганда – здійснюється для підтримки поточних дій.

2. За спрямованістю на захист або придушення ідеї:

– Оборонна пропаганда – призначена для підтримки соціальної, або якої-небудь іншої акції суспільства.

– Наступальна пропаганда – призначена для припинення тої чи іншої соціальної дії, яка здається пропагандисту шкідливою, і сприяння тій дії, яка здається йому бажаною за допомогою революційних, дипломатичних або військових засобів.

3. За цілями:

– Конверсійна пропаганда – спрямована на те, щоб примусити людей змінити свої ціннісні орієнтації, своє емоційне та практичне відношення до одної групи людей та почати підтримувати іншу.

– Розподіляюча пропаганда – призначена для того, щоб внести розкол в групу, що підтримує ворога і, порушивши єдність її рядів, послабити цього ворога.

– Консолідуюча пропаганда – спрямована на мирне населення захоплених територій. Її мета – примусити населення підкорятися розпорядженням командування окупантів і політиці, яку вони проводять.

Спочатку варто виділити дві категорії користувачів соціальних мереж з погляду поширення інформаційних впливів: *суб'єкти впливу (агенти)* та *об'єкти впливу (звичайні вузли)*.

Суб'єкти впливу – активні користувачі метою, яких є поширення (впровадження) певної ідеї або інформації. Їхньою метою може бути широка аудиторія за принципом «чим більше – тим краще» або ж певна обрана група користувачів (targetgroup). Критерій вибору цільової групи залежить від конкретних завдань і кінцевих цілей, це може бути вікова група, статева

ознака, соціальний стан, національна приналежність та інші. Суб'єкти характеризуються будь-якими активними інформаційними впливами спрямованими на об'єкти.

Об'єкти впливу – користувачі, на яких спрямований інформаційний потік з метою переконати їх у чомусь, або схилити до певної ідеї.

Множини суб'єктів і об'єктів в розрізі інформаційної атаки перетинаються (рис. 1.3). Користувачі, які спочатку розглядаються як об'єкти, в процесі можуть ставати суб'єктами або ж одночасно перебувати в обох множинах: ще перебуваючи під цільовим інформаційним впливом, вже самостійно починають просувати в мережі нав’язану їм інформацію, відчувати свою зацікавленість (реальну, або уявну) в її поширенні.

У широкому значенні метою суб'єктів є поглинання множини вибраних або досяжних об'єктів і перетворення їх в активні ланки подальшого просування інформації в мережі.

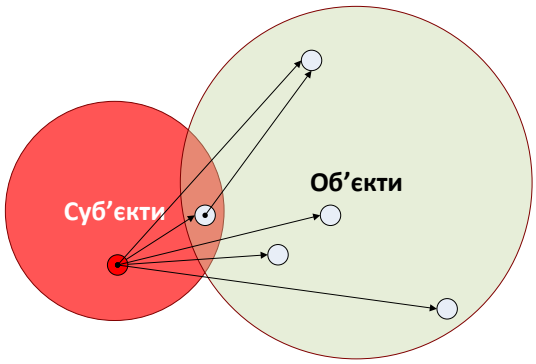


Рисунок 1.3 - Множини суб’єктів та об’єктів інформаційного впливу у соціальних мережах

Пропонується виділити наступні ролі користувачів соціальних мереж з погляду поширення та сприйняття ними вірусної інформації, що може бути корисним для подальшого імітаційного моделювання інформаційних впливів та поширення інформації у соціальних мережах.

Генератор ідеї – суб’єкт впливу, що створив певну ідею та намагається поширити її серед якомога більшої кількості користувачів. Генератор ідеї

виконує стратегічну функцію, розкидаючи «інформаційне насіння» в різних сегментах мережі і постійно підживлюючи породжені гілки прихильників новою інформацією в рамках впроваджуваної ідеї.

Користувач – об'єкти впливу, який може мати різний рівень довірливості. Під час впливу, в залежності від власних характеристик, може заразитися ідеєю, стати контргенератором та проводити поширення контр ідеї, або стати генератором ідеї другого рівня.

Отже, генераторів ідеї варто розподіляти на рівні. Суб'єкт, що породжує інформаційну хвилю – генератор ідеї першого рівня. В процесі інформаційного впливу на інших користувачів мережі можуть виникати послідовники ідеї, що активно включаються в процес розповсюдження інформації. Таких користувачів варто віднести до генераторів 2-го, 3-го та наступних рівнів.

Пасивними впливом можна вважати використання особистої інформації учасників мережі для досягнення певних власних інтересів.

В першу чергу це стосується маркетингових технологій та реклами.

Можна з упевненістю сказати, що профіль користувача (їм же добровільно надана інформація про себе) і його поведінка в соціальній мережі (недобровільно надана інформація) є безцінним джерелом інформації для маркетологів і дуже перспективним джерелом для прибутку.

Окремо варто згадати рекламні технології. Вже зараз більшість соціальних мереж надають можливість поведінкової реклами, і дані технології стрімко розвиваються. Починаючи від простого розподілу на групи (наприклад за критерієм статі чи вікової групи) і закінчуючи складними системами стеження і аналізу дій користувача, на основі яких йому і буде пропонуватись відповідна реклама.

СМ можна взагалі розглядати як ідеальний інструмент маркетолога:

- користувачі самі реєструються в мережі й вносять особисту інформацію (вказують вік, стать, контактну інформацію);

- аналізуючи мережу і публікації можна виділяти групи за інтересами

та вподобаннями, виявляти «target group» для конкретних цілей;

- відслідковувати реакції потенціальних покупців та вносити кореляції в стратегії.

Прикладами використання мереж для маркетингових і рекламних впливів можна навести впровадження в FaceBook рекламного сервісу Beacon, який фактично шпигував за користувачами цієї соціальної мережі, загальна кількість яких на той момент перевищувала 50 мільйонів чоловік. Facebook Beacon розсилав друзям користувачів інформацію про покупки користувачів. В результаті понад 70 тисяч осіб виступили проти таких нововведень, і незабаром сервіс був відправлений на доопрацювання.

Іншим напрямком є відбір особистої інформації, що може бути використана як засіб шантажу чи тиску поза мережею. Такі випадки досить часто зустрічаються в середовищах публічних осіб, в політичній боротьбі, як засоби під час бізнесових війн. Окремим варіантом є доступ до особистої інформації (особливо інформація про родину та найближче оточення) солдатів – учасників збройних конфліктів. Ще в лютому 2008 року Міністерство оборони Канади поширило меморандум, який говорить, що військовим не слід залишати особисті відомості про себе в соціальних мережах Інтернету, так як за такими сайтами пильно спостерігають бойовики «Аль-Каїди». Відомі і випадки шантажу військових через інформацію отриману з СМ в збройному конфлікті України та Росії.

Окрім особистісно-орієнтованих впливів використовуються і масовані інформаційні атаки. Ціллю таких атак є окремі соціальні групи або громадяни цілих держав. Наприклад основними напрямами та способами маніпулятивних психо-інформаційних технологій РФ відносно України були (та і залишаються надалі):

– поступове пониження міжнародного іміджу України з метою послаблення її геополітичного значення;

– відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики “керованого хаосу”;

– формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу;

– домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури [58].

В таких впливах спрацьовує в більшості ефект масовості та повторюваності. Неважливими є ні зміст інформації ні її правдивість. Це можна порівняти з піснею що прокручується в радіоефірі багаторазово протягом дня – людина чує пісню з свого приймача, в громадських місцях, в міському транспорті, деінде, і, не залежно від її якості (з музичної точки зору), жанрових вподобань людини і інших факторів, через деякий час людина вже наспівує мелодію пісні і вона здається їй гарною.

Учені з американського Політехнічного інституту Ренсселера (Rensselaer Polytechnic Institute) виявили, що коли всього 10% населення володіє непохитною впевненістю в чому-небудь, то вона завжди буде прийнята більшістю суспільства. «Якщо завербувати (чи взяти на роботу) 10% від кількості певної соціальної групи – то ми отримаємо механізм управління думкою цієї групи. Швидкість отримання результатів залежить лише від вдалих методів маніпулювання та інформаційного впливу» - зауважують дослідники.

«Коли кількість повністю одержимих певною ідеєю знаходиться на рівні нижче 10%, то ніякого видимого прогресу в поширенні ідей немає. По суті, для того, щоб в такому випадку думка стала переважаючою (домінуючою) в суспільстві, необхідно час, що прівнюється з віком Всесвіту. Однак як тільки кількість залучених людей переходить кількість 10%, ідея поширюється блискавично», - говорить керівник дослідження Болеслав Шиманьскі (Boleslaw Szymanski).

Як приклад наводяться недавні події в Тунісі і Єгипті. Шиманьскі пояснює свою думку наступним прикладом - в цих країнах (Туніс, Єгипет) диктатори, що перебували при владі десятиліттями, були несподівано повалені протягом декількох тижнів.

Були промодельовані три різних типи соціальних мереж. 10 відсотків завжди ставали критичною масою для того, щоб думка заволоділа розумом більшості учасників. За результатами їх досліджень (Rensselaer Polytechnic Institute) - відсоток ідейно одержимих людей, який необхідний для того, щоб похитнути думку більшості, не змінюється значною мірою незалежно від типу мережі, в якій вони працюють.

1.3. Методи протидії інформаційним впливам у соціальних мережах під час інформаційного протиборства

Досвід інформаційного впливу за допомогою віртуального спілкування, зокрема використовуючи соціальні мережі як інструмент, безперечно свідчить про необхідність моніторингу і контролю з боку держави до діяльності та розвитку «соціальних мереж». Водночас така увага не повинна порушувати права людини, зафіксовані у законодавстві [33, 34].

Сучасні різносторонні (в різних галузях науки) дослідження відзначають недостатній рівень актуалізації питання інформаційної безпеки в цілому й соціальних мереж, як ефективного інструменту інформаційних впливів. Зокрема Гаркуша в своєму дослідженні [50] вказує на суттєвий вплив і активне використання соціальних мереж в російсько-українському конфлікті.

З одного боку СМ являють собою небезпечний інструмент інформаційного впливу й маніпуляцій масовою свідомістю, що становлять загрозу стабільності та національній безпеці, з іншого – не можна забувати про свободу слова, як одну з основних рис громадянського суспільства. Сьогодні ми можемо спостерігати беззаперечні негативні для України

результати, що не в останню чергу були досягнені завдяки використанню соціальних мереж.

За рахунок наявного в СМ ресурсу соціальної довіри, а також при умові певної підготовки та наявності спеціально підготовлених груп в середені соціальної мережі, СМ може успішно використовуватись для просування в маси конкретної інформації, дестабілізації суспільства, відверто деструктивної, шкідливої для свідомості громадян інформації. Соціальні мережі вдало можуть бути застосованя як інструмент для організації, моніторингу та керування соціальними заворушення в інших країнах віддалено. Для цього мужуть бути застосовані:

- розпалювання протестних настроїв серед населення з використанням різних сервісів: блоги, форуми, розсилка повідомлень користувачам СМ;

- визначення часу початку акцій, синхронізація учасників, динамічне оперативне керування акціями, моніторинг учасників та звітність про їх участь (наприклад фото звіти проведених акцій)

Провідні країни світу (США, Великобританія, Китай, Росія) використовують мережі для просування власних впливів в суспільствах інших країн, вербування та підготовки агентури, формування та закріплення стратегічних ідеологій [51].

Соціальні мережі можуть використовуватись як майданчики попередньої підготовки державних переворотів та революцій. Прикладом можуть слугувати низка подій в країнах Північної Африки та Близького Сходу 2010 року, що отримали назву «арабська весна». Під впливом цих подій було повалено ряд режимів, що отримували владу протягом десятиліть, а спільною рисою всіх цих подій стало активне використання інтернет - технологій та соціальних мереж [52].

Ще одним яскравим прикладом агресивного використання соціальних мереж стала підготовка до анексії Криму, дестабілізація обстановки почалася з повномасштабної інформаційної атаки в соціальних мережах: критика української влади, роздмухування етнічних конфліктів,

специфічний ракурс огляду економічної ситуації, обіцянки «кращого майбутнього». Цей інцидент являється прикладом особливої форми ведення інформаційної війни з використанням попередньо підготовленого дезінформаційного контенту, спеціальних активних груп в соціальних мережах, застосування методик психологічного впливу на населення (користувачів інтернет-сервісів та соціальних мереж). На передодні подій 2014 року Росія вела активну пропогандиську кампанію з залученням всіх доступних засобів масової інформації: ЗМІ (НТВ, Росія-24, РТР), новинні портали (Итар-ТАСС, Риа Новости), он-лайнові додатки для мобільних пристроїв («Становление Империи», «Мировое господство»), соціальні мережі («ВКонтакте», «Одноклассники», FaceBook, Twitter) [53].

Враховуючи вище сказане – необхідність державного контролю, вироблення механізмів та методик інформаційного протистояння не викликає жодних сумнівів.

В своєму дослідженні Гумінський [56] виділяє наступні напрямки протидії інформаційному впливу:

– силові методи – закриття серверів, обмеження трафіку;

– юридично-правові методи – притягнення до кримінальної відповідальності організаторів та учасників віртуальних спільнот;

– інтернет цензура;

– моніторинг віртуальних спільнот та контент аналіз.

Якщо розглядати короткострокову перспективу, то ефективними представляються перші два методи, хоча вони й мають ряд недоліків пов’язаних з характерними властивостями, що притаманні віртуальним спільнотам – суб’єктам інформаційної безпеки.

Зокрема варто виділити наступні характерні властивості:

– відсутні географічні кордони, не існує обмежень для швидкого (в деяких випадках миттєвого) поширення, збору, обробки та інтерпретації інформації, висока динаміка (виникнення та зникнення інформаційних

ресурсів). Дана особливість унеможливлює виключне правове регулювання й контроль комунікацій з боку держави;

– можливість анонімності в інформаційних процесах. Даний факт також унеможливлює застосування традиційних юридичних підходів та притягнення до відповідальності за скоєне правопорушення або злочин в інформаційній сфері. Це забезпечує високий рівень латентності та низький рівень розкриття правопорушень в сфері інформаційної безпеки;

– легкодоступна змінюваність інформації в електронній формі: на відміну від стабільної, документально оформленої інформації, електронна інформація не має форми, сталої у часі та просторі.

Основна особливість і головна небезпека деструктивних віртуальних спільнот пов'язані з тим, що визнати за законом їхню діяльність деструктивною в умовах дії норм свободи слова, друку, віросповідання можливо тільки після реалізації в реальному світі їх учасниками якихось заходів, здійснених під дією інформаційно-психологічного впливу. Тільки тоді дії та події можна співвідносити з нормами чинного законодавства та відповідно кваліфікувати.

Ще одним із проблемних питань щодо неефективності використання силових методів є те, що українські соціальні мережі дуже сильно інтегровані в російський або світовий Інтернет (з десяти сайтів в Україні, що мають найвищий рейтинг відвідуваності – лише два українських).

В Україні, згідно з чинним законодавством [35], цензурі в інтернет просторі підлягає інформація, яка містить елементи дитячої порнографії, законодавчої бази щодо цензури в інших питаннях (інформаційної безпеки держави, суспільства) немає.

Методи моніторингу та контент аналізу віртуальних спільнот є більш ефективним в довгостроковій, але потребує залучення фахівців різних галузей науки. Виходячи з характерних рис віртуальних спільнот (здатності реорганізації) основною задачею моніторингу та контент аналізу віртуальних спільнот є не їх знищення, які представляють загрозу для

інформаційної безпеки Держави, а управління та контроль діяльністю віртуальних спільнот методами інформаційного впливу.

1.4. Методи імітаційного моделювання інформаційних впливів для динамічного аналізу інформаційної безпеки соціальних мереж

З огляду теми дослідження доцільно розглянути різні класи та окремі представники моделей, запропонованих для моделювання інформаційних впливів у соціальних мережах. Моделі дозволяють проводити певні дослідження та спостереження, що викликають зацікавлення в багатьох прикладних напрямках. В аналізі тенденцій та динаміки розповсюдження інформації в СМ зацікавлені маркетологи з точки зору просування товарів на ринки, з тих же міркувань даним напрямком цікавляться і бізнес-аналітики. Іншим проявом явища розповсюдження інформації в СМ є інформаційний вплив та переконання людей в певній ідеї, з цієї точки зору процес цікавить політиків, PR-менеджерів, політтехнологів та пропагандистів.

Інструменти аналізу дозволяють оцінити індивідуальні та групові переваги клієнтів, виявити тренди інтересів і надалі вирішувати важливі стратегічні завдання.

Одним з основних завдань і засобів інформаційного обміну соціальних мереж є поширення інформації: статті, огляди, аудіо, відео, короткі повідомлення («Твіти») та інші види інформації в сукупності утворюють інформаційний контент соціальних мереж.

Велика кількість запропонованих підходів дослідження призвела до необхідності їх класифікації, науковці виділяють кілька напрямків дослідження СМ, зокрема автори [78] класифікують дослідження по чотирьом основним напрямкам: структурний, ресурсний, нормативний та динамічний. В подальшому в статті будуть розглядатись моделі, що в більшості відносяться до структурного підходу, але можуть мати і ознаки динамічного підходу.

У структурному підході всі учасники мережі розглядаються як вершини графа, які впливають на конфігурацію ребер і інших учасників мережі. Основна увага приділяється геометричній формі мережі і інтенсивності взаємодій (вазі ребер), тому досліджуються такі характеристики, як взаємне розташування вершин, центральність, транзитивність взаємодій. Динамічний підхід аналізує зміни в структурі мережі: появу нових учасників, утворення стійких підструктур, динаміку зміни зв'язків.

Модель епідемії та похідні моделі

Перші моделі для дослідження СМ запропоновані достатньо давно, зокрема варто розглянути модель епідемії, або SIR (Susceptibles - Infectives - Removed). Дана модель запропонована вперше авторами Кермаком та МакКендріком в роботі [79]. Початково модель запропонована для прогнозування розповсюдження епідемій, модель пропонує поділити населення на три групи S- сприятливі до захворювання, I – інфіковані, R – одужали та мають імунітет. Автори моделі запропонували систему диференційних рівнянь що описує процес розповсюдження хвороби:

$$\begin{cases} \frac{dS}{dt} = -\frac{\beta IS}{N} \\ \frac{dI}{dt} = \frac{\beta IS}{N} - \gamma I, \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (1.2)$$

де β – середня частота зараження, γ – стала середня швидкість одужання, N – загальна кількість особин популяції (кількість населення).

Розповсюдження хвороби багато в чому подібне до розповсюдження інформації в мережі, але дослідження показують що результати моделювання на SIR досить сильно розбігаються з результатами експерименту проведеного на реальній моделі [80]. Основним недоліком даної моделі є те, що вона не враховує динаміки зміни кількості вузлів мережі в часі: окремі користувачі можуть приєднуватись до мережі або, навпаки, покидати мережу вибуваючи

з ланцюга розповсюдження інформації. Тому для моделювання соціальної мережі було запропоновано розширену модель SIR. Розширена модель доповнена параметрами μ – середня частота залучення нового агента в мережу, δ – середня частота покидання мережі окремим агентом. Розширення набору параметрів дозволило більш точно наблизити модель до реальних показників. Взявши за основу модель SIR в 1965 році була запропонована модель Далея-Кендалла (DK - модель), дана модель відома ще як «модель розповсюдження чуток». В своїй моделі автори дещо змінили критерії розбиття населення на групи порівняно з моделлю SIR і виділили такі групи:

U – група, що починає розповсюдження чутки (новини);

V – група, що сприймає чутку і продовжує її розповсюдження;

W – група, що не сприймає інформації і не розповсюджує її далі.

Як бачимо, в моделі «розповсюдження чуток» виділено все ті ж три групи але їх інтерпретація адаптована саме до процесу інформаційного обміну. В DK-моделі чутка розповсюджується з ймовірністю β/N, а ступінь сприйняття визначається параметром μ. Розповсюдження припиняється якщо, розповсюджуючи, агент натикається на представника групи W, ймовірність даного факту визначається співвідношенням:

$$\frac{\gamma V(V+W)}{N}. \tag{1.3}$$

Моделі на основі клітинних автоматів

Окремим напрямком в моделюванні мереж є моделі на основі клітинних автоматів. В основі таких моделей лежить дискретна динамічна система, що складається з однорідних клітин. Кожна клітина може мати певний набір станів та правила переходу від одного стану до іншого. На перехід клітини до іншого стану впливають інші клітини, що оточують її. Моделі відрізняться наборами станів та правилами переходу. Дані моделі враховують до певної міри динаміку та структуру мережі: окіл кожної окремо взятої клітини та стан оточуючих клітин. Дані моделі в деяких

джерелах називають моделями дифузії інновацій. Формально клітинний автомат може бути описаний співвідношенням:

$$y_j(t+1) = F(y_j(t), O(j), T), \quad (1.4)$$

де t – крок ітерації, F – формально представлене правило переходу до іншого стану, $y_j(t)$ – стан на попередній ітерації, $O(j)$ – множина сусідніх клітин (окіл кінцевого клітинного автомату).

В найпростішому випадку для клітинного автомату можна визначити стани аналогічні критерію розподілу на підмножини DK-моделі (сприймає новину, сприймає і розповсюджує, не сприймає). Більш адекватно модель відображає процес, якщо розширити набір станів та ускладнити правила переходів. Наприклад деякі автори пропонують враховувати параметр старіння новини та використовувати систему порогів.

Розглянуті вище моделі являються класичними моделями для оцінки інформаційного «зараження», але цікавим є також і дослідження розподілу думок і впливів.

Моделі з порогами та моделі незалежних каскадів

На системі порогів побудовані так звані порогові моделі. Їх суть полягає в тому, що агенти поділяються на активних (ті що розповсюджують інформацію) та неактивних. Моделюється ітераційний процес, вході інформаційного обміну в кожного окремого агента накопичується рівень інформаційного впливу та існує певний поріг. При переході даного порогу агент стає активним, при цьому перехід розглядається як незворотній. Якщо функція накопичення є лінійною такі моделі відокремлюють в окремий клас – «Моделі з лінійним порогом».

Подібною по суті є і модель незалежних каскадів, але суттєвою відмінністю від попередньої є те, що вузол v_i може лише однократно (з певною ймовірністю) впливати на вузол v_j Такі моделі відносять до класу систем взаємодії незалежник частинок. В роботі [81] описана узагальнююча

модель, для якої порогові моделі та моделі незалежних каскадів є частковими випадками.

Моделі з використанням ланцюгів Маркова

Запропоновано моделі, що враховують події властиві виключно соціальним мережам. Прикладом такої моделі можна навести мультиагентну модель розповсюдження інформації в мережі запропоновану Ланде Д.В. та співавторами в статті [82], дану модель варто віднести до моделі, що базується на ланцюгах Маркова. В якості базового параметра моделі автори пропонують розглядати деяку величину E (енергія агента) в процесі моделювання ітераційного процесу розповсюдження інформації, з певною ймовірністю можуть відбуватись події, що змінюють рівень енергії агента:

Лайк = E+1

Дизлайк = E-1

Репост = E+2

Лінк = E+1

Окрім зовнішніх впливів агент за умовами моделі втрачає по 1 енергії на кожній ітерації моделі. Ймовірність виникнення подій залежить від ряду факторів: актуальність повідомлення, рівень зацікавленості в інформації, інші характеристичні зовнішні оцінки інформаційного повідомлення. Ймовірності того, що в наслідок повідомлення з енергією агента відбувається певна зміна автори визначили наступним чином:

$$\begin{aligned} P_{like}^{(E)} &= P_{l_0}\varphi(E); \\ P_{dislike}^{(E)} &= P_{d_0}\varphi(E); \\ P_{repost}^{(E)} &= P_{r_0}\varphi(E); \end{aligned} \tag{1.5}$$

де $P_{l_0}, P_{d_0}, P_{r_0}$ – параметри моделі, а $\varphi(E)$ – деяка монотонно неспадаюча функція з значенням в діапазоні [0, 1].

При падінні значення енергії агента до 0 - він «помирає» і більше в моделі не розглядається. Життєвий цикл моделі пропонується починати з одного агента, його можна представити наступним графом:

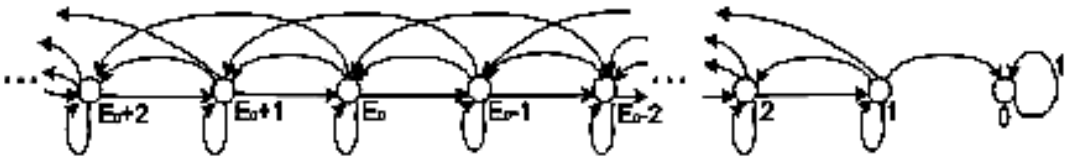


Рисунок 1.4 - Представлення моделі графом

Досліджуючи ймовірнісний розподіл послідовності через ймовірність переходів при фіксованих початкових параметрах, дослідники приходять до висновку - розподіл ймовірності отримання агентом n лайків відповідає розподілу Вейбулла. Дуже схожі данні були отримані і в ході експерименту проведеному авторами з даними отриманими з реальної мережі.

Ігрові моделі

Окремий вид моделей - так звані «теоретико-ігрові» моделі. Вклад в розвиток цієї гілки та ґрунтовні дослідження проведені в роботах Губанова Д.А., Новікова Д.А., Чхартішвілі А.Г. [84-86]. В моделях даного типу акцент робиться на інформованість і взаємозв'язок між гравцями (агентами). Загалом автори пропонують триступеневу ієрархічну задачу.

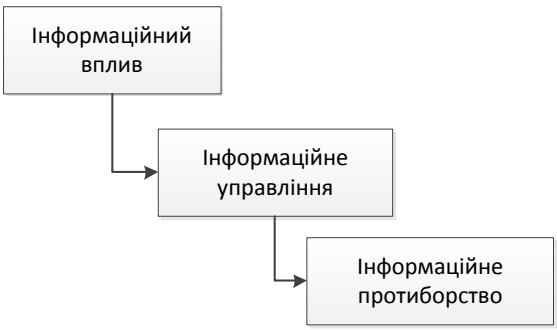


Рисунок 1.5 - Ієрархічна структура задач дослідження інформаційних процесів

Ігрова модель розглядає початкові умови гри, кінцеву мету гравця та дії опонентів (інших учасників гри). Агент вибудовує свою гру таким чином, щоб максимізувати свою вигоду з урахуванням поточних умов. Теоретико-ігрові моделі розглядаються в залежності від кінцевої мети, серед них виділяють наступні класи:

1. моделі взаємної інформованості;
2. моделі узгоджених колективних дій (і суспільних благ);
3. моделі комунікацій і завдання пошуку мінімально достатньою мережі;
4. моделі стабільності мережі;
5. моделі інформаційного впливу та управління;
6. моделі інформаційного протиборства.

В залежності від типу моделі визначаються правила гри і можлива поведінка гравця для досягнення кінцевої мети.

Порівняння імітаційних моделей інформаційних впливів у соціальних мережах

Порівняння моделей ускладняються і вибором критеріїв для порівняння і різною внутрішньою структурою та математичною природою моделей. Зрозумілим є той факт, що кожна з моделей має своє спрямування та базується на певних відокремлених з реального процесу компонентах: окремо взяті характеристики і властивості.

Запропонована нижче порівняльна таблиця не розподіляє моделі на «кращі» та «гірші», а лише визначає характеристики та прояви, що враховуються моделлю.

Таблиця 1.1

Порівняння існуючих імітаційних моделей інформаційних впливів у соціальних мережах

Моделі	Зміна думки під впливом оточуючих агентів	Вплив структурних особливостей околу агента, та структури мережі в цілому	Різний ступінь схильності агентів до ІВ	Наявність ймовірнісних параметрів	**Врахування активності агента**	Оптимізація ІВ	**Поведінкові стратегії агентів**	Оцінка ймовірності певного результату та розподіл агентів в визначений момент часу	**Параметризація особистісних якостей агента**
Модель Грановветера[110]	+	+	+	-	-	+	-	-	-
Модель Торопова[112]	+	+/-	-	+	-	+	-	-	-
Модель Гончарова-Сироти[115]	+	+	+	-	-	+	-	+/-	-
Модель Ланде[82]	+	-	-	+	-	-	-	+	+/-
Модель Губанова[84, 86, 94]	+	+	+/-	+/-	-/+	+	**-/+**	-	-/+

В моделі на основі ланцюгів Маркова, запропонованій автором Ланде Д.В.[82], в якості параметра вузла, що моделює користувача мережі, розглядається єдиний параметр Е (енергія користувача). Даний параметр є певним узагальненням параметрів (характеристик) користувача, всі можливі реакції інших вузлів на інформаційний посил від вузла (лайк, дізлайк, репост) впливають на даний параметр. Тобто даний параметр є не індивідуальною характеристикою вузла (користувача мережі), а відображенням реакції на даний вузол, сприйняття його інформаційних посилів іншими учасниками мережі.

Автори, що пропонують теоретико-ігрові моделі [94, 95], в якості параметра вузла розглядають або довіру до інших вузлів, представлену матрицею коефіцієнтів, або репутацію вузла. Зокрема автори статті [94] зазначають, що в обох випадках отримується якісно однаковий результат, це

логічно з огляду на прямо пропорційний зв’язок даних параметрів – чим вище репутація вузла, тим більший ступінь довіри йому з боку інших учасників мережі.

З таблиці 1.1 видно, що серед розглянутих моделей жодна не дає комплексного представлення процесу і лише частково враховує окремі характеристики, що притаманні конкретним вузлам (суб’єктам процесу інформаційного обміну) й впливають на реальний процес розповсюдження інформації в СМ. З урахуванням оцінок в таблиці 1.1, найкращий результат на наборі критеріїв показують теоретико-ігрові моделі, але тут необхідно враховувати й той факт, що теоретико-ігрові моделі представляють собою цілий набір класів. Кожна окрема модель враховує, в тій чи іншій мірі, окремі характеристики. Мінімізація кількості параметрів обумовлена суттєвим збільшенням складності математичної моделі при збільшені кількості параметрів.

З таблиці 1.1 видно, що більшість моделей не враховують активності агента, його поведінкових стратегій в життєвому циклі процесу. Більшість класичних моделей взагалі не розглядають параметрів агента, всі агенти в цих моделях ідентичні. Ці недоліки суттєво знижують адекватність моделей, бо в реальній ситуації соціальна мережа складається з особистостей з індивідуальними якостями та характеристиками. Поведінка окремого агента звичайно має суттєвий локальний вплив, але, в той же час, це може вплинути і на кінцевий результат чи стан мережі відносно досліджуваного інформаційного впливу. Будь-який інформаційний вплив, розповсюдження новини чи лобіювання певної ідеї в мережі починається з одного (або невеликої обмеженої групи) агентів, і на початковому етапі суттєве значення має саме стратегія і особливі якості агента-генератора. В найгіршому для нього випадку інформація взагалі може не набути розповсюдження, або канали й способи розповсюдження будуть обрані невірно й інформаційна хвиля швидко згасне.

1.5. Висновки до першого розділу

Аналіз методів і моделей поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства дозволив виявити як комбіновані комплексні моделі, що мають підвищити адекватність і відповідність моделювання реальним процесам, так і моделі, орієнтовані на дослідження конкретних характеристик. Аналіз показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла, а саме поведінку окремого вузла, стратегію розповсюдження інформації, яку обирає вузол в процесі інформаційного впливу тощо.

Сьогодні соціальні мережі в різних їх проявах та реалізаціях стали потужним інструментом інформаційного впливу. При цьому впливи можуть носити як конструктивний так і деструктивний характер. Але не залежно від характеру впливу він має бути прогнозованим та контрольованим. Цей факт визначає актуальність та необхідність досліджень соціальних мереж як потужного інструменту для інформаційного впливу. Інформаційні впливи завжди були дієвим інструментом для маніпуляцій людьми та навіювання певних ідей. Перші методики інформаційних впливів розроблені досить давно. В останній час підходи набули особливого значення і отримали суттєвий приріст ефективності, це пов’язано з розвитком мережі Інтернет та щільним повсякденним використанням користувачами різноманітних соціальних мережевих сервісів. Реєструючись в соціальних мережах користувач потенційно стає об’єктом інформаційних атак різноманітної направленості. Мета інформаційних атак може бути абсолютно різною: від маркетингових і рекламних кампаній до політичної боротьби та інформаційної війни, як засобу створення відповідного ідейного підґрунтя для реальних бойових дій або військових переворотів. Відтак зростає інтерес до використання існуючих СМ для інформаційних впливів. Факт використання сервісів для деструктивних інформаційних впливів вимагає

вироблення методів та засобів протистояння таким впливам. Ефективний спротив повинен передбачати: дослідження проблеми та аналіз мети впливу, виявлення зон впливу, прогнозування наслідків, вироблення методів пасивного та активного інформаційного захисту. Аналіз інформації та інформаційних тенденцій в СМ дозволяє робити певні висновки про процеси, що протікають в суспільстві, прогнозувати поведінку його учасників, моделювати соціальну взаємодію.

Одним з підходів для дослідження мереж є моделі. Створення нових та інтеграція вже створених методів і моделей аналізу комп'ютерних соціальних мереж становить інтерес для дослідження. Існування різних підходів до аналізу комп'ютерних соціальних мереж призводить до проблеми об'єднання результатів, отриманих в ході досліджень. У дослідженні атрибутів учасників мережі, зв'язків між ними, виявленні закономірностей побудови мереж між учасниками можуть бути корисні нові методи статистичного аналізу, комбінації їх з алгоритмами з теорії графів та програмними ітераційними моделями. Іноді відносини між учасниками мережі зручно розглядати як імовірнісні (стохастичні) характеристики для опису процесу еволюції мереж, в інших випадках можуть бути використані моделі з детермінованими наборами правил. Наявність великої кількості запропонованих моделей потребує комплексного підходу до порівняння та оцінки моделей. Необхідно також враховувати зміни, що відбуваються в суспільстві, в тому числі в соціальних мережах, як одному з проявів суспільного життя.

Огляд джерел та публікацій виявив суттєвий інтерес до питання дослідження та моделювання соціальних мереж серед науковців сучасності. Дослідники пропонують як комбіновані комплексні моделі, що мають підвищити адекватність і відповідність моделювання реальним процесам, так і моделі орієнтовані на дослідження конкретного питання чи характеристики. Перші стикаються з проблемами математичного характеру, суттєвого ускладнення структури моделі внаслідок нашарування параметрів і породженням різного роду колізій. Другі стикаються з ризиками отримання

великих похибок в результаті відкидання певних характеристик та параметрів.

Порівняння вибраних моделей виявляє, що більшість моделей не враховують індивідуальних характеристик вузла. Класичні моделі орієнтовані на дослідження певних підгруп вузлів мережі та динаміку зміни даних підгруп, при цьому всі вузли мають однакові характеристики. Практика дослідження ситуацій в реальних умовах показує суттєвість значення та впливу на процес особистих характеристик учасників процесу інформаційного обміну. В тому числі існуючі моделі не враховують і поведінки чи стратегій, що обираються окремими вузлами в ході реалізації процесів інформаційного впливу. Впливи ботів та автоматизованого підходу до процесу розповсюдження інформації втрачають свою актуальність за рахунок наявності розроблених методів для розпізнавання та нейтралізації таких впливів. В ході «живого спілкування» та інформаційних процесів між людьми - вузлами мережі вирішальне значення мають характеристики окремо взятого вузла та обрана ним поведінкова стратегія для досягнення поставленої мети. Як показує проведене дослідження - більшість моделей дані аспекти не враховує.

РОЗДІЛ 2.
МАТЕМАТИЧНА МОДЕЛЬ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНІЙ МЕРЕЖІ ТА МЕТОД ГЕНЕРАЦІЇ СТРУКТУРИ СЕГМЕНТУ СОЦІАЛЬНОЇ МЕРЕЖІ ДЛЯ ЇЇ ПРОГРАМНОГО ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Об’єктом моделювання є не лише соціальні мережі в їх електронному варіанті реалізації як веб-сервісів мережі, поняття розглядається в широкому змісті. Соціальна мережа - це структура, що складається з масиву вузлів, які представлені соціальними об'єктами (людьми, групами або організаціями) та взаємозв'язками між ними. В якості зв’язків розглядаються будь-які засоби комунікацій та інформаційного обміну.

Реалізуючи модель необхідно розв’язати декілька базових складових задач та визначитись з обмеженнями моделі. До основних задач при моделюванні соціальної мережі варто віднести:

- вибір методу генерування структури мережі;
- формальний опис вузла та визначення набору характеристичних параметрів вузла;
- формалізація процесу інформаційної взаємодії.

Обґрунтування підходу до генерування структури мережі та його реалізація буде розглянута в наступному пункті

2.1. Моделювання структурних властивостей соціальних мереж для їх динамічного аналізу та обґрунтування підходу до автоматичної генерації структури сегменту соціальної мережі

Структура соціальної мережі, з точки зору інформаційних зв’язків та інформаційного обміну, може бути представлена у вигляді графу. В якості вузлів графа виступають суб’єкти інформаційного обміну, а ребрами є наявні інформаційні зв’язки (рис. 2.1).

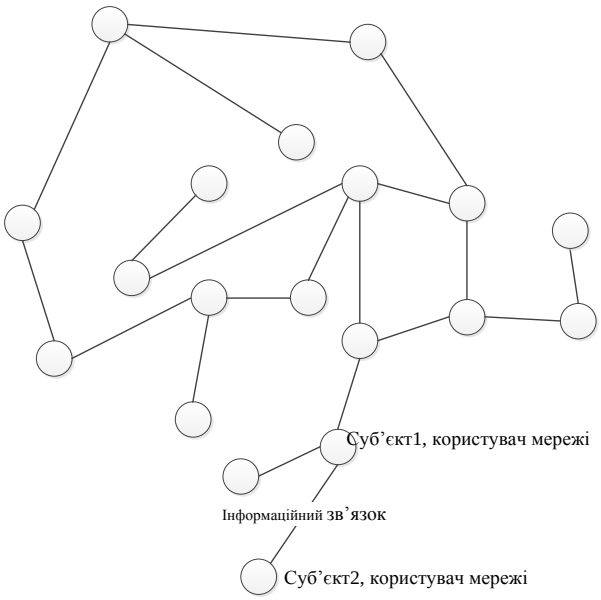


Рисунок 2.1 – Представлення соціальної мережі у вигляді графа

В основі аналізу соціальних мереж лежить математична теорія графів (вона представлена в роботах таких авторів, як Ердос, Харари і Раппапорт) [37, 39], а також емпіричні дослідження в області соціальної психології та антропології (Хайдер і Морено) [40, 41] . У той час як перша група вчених відкривала різні закони побудови абстрактних вузлів і ліній, останні виявили, що вузлами і лініями найзручніше позначати відносини між людьми.

Більшість класифікацій СМ проводяться за типами послуг, що надаються (особисте спілкування, ділове спілкування, геолокації, блогінг і т.д.), по доступності (відкриті, закриті, змішані), по регіону (світ, країна, організація). Даний підхід до класифікації констатує поточний стан, дозволяє згрупувати соціальні мережі тільки за певними зовнішніми ознаками, але не враховує впливу структури на процеси, що відбуваються в СМ.

Досліджувати структуру мережі і теоретично моделювати різні типи мереж почали задовго до того як з’явилися соціальні мережі в сучасному розумінні даного терміну – реалізовані на основі сучасних Інтернет технологій та сервісів. Початковою мережа розглядалась як система взаємозв’язків та спілкування між людьми (частіше досліджувались

конкретизовані групи: співробітники установи, гравці біржі, юристи, покупці, люди в межах певної соціальної групи).

Загалом мережа не має яскраво вираженої структури – розташування її вузлів та щільність зв'язків, особливо на початковому етапі функціонування мережі, мають хаотичний характер. Але в ході свого життєвого циклу, в процесі спілкування суб'єктів в мережі, виникають досить сталі за структурою підмножини.

Формування вище згаданих підмножин їх конфігурація і кількісні показники досить суттєво впливають на інформаційні процеси в СМ. Фактично множина таких відносно сталих структур і визначає як локальну структуру фрагмента мережі так і структуру мережі в цілому.

Різними дослідниками виділено ряд сталих підмножин с характерними конфігураціями. Серед них варто виділити зокрема наступні: група, лідерська група, кліка.

Пропонується розглядати СМ як набір певних підмножин, типів кластерів (кластерами далі будемо називати певну частину мережі, що має характерну структуру) і розглядати СМ с точки зору мережевого підходу [43-45] з урахуванням певних обмежень.

Дамо означення деяким вибраним типам підмножин (кластерів).

Група (**Г**) - граф з таким набором зв'язків, що дозволяє встановити зв'язок між будь-якими двома вузлами графу напряму або використовуючи проміжні вузли. В літературі таку підмножину часто називають – «цілісна мережа» [47]. Схематично підмножина типу «Група» представлена на рис. 2.2.

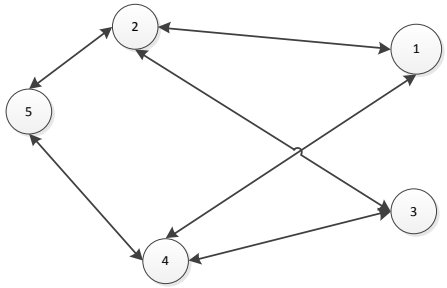


Рисунок 2.2 – Підмножина типу «Група»

Кліка (**К**) – граф в якому кожен вузол зв’язаний з кожним, або, іншими словами – всі вершини графа суміжні (рис. 2.3).

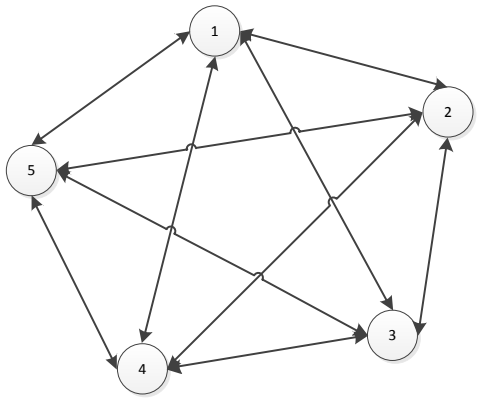


Рисунок 2.3 – Підмножина типу «Кліка»

Такі кластери в мережах представляють цікавість с точки зору аналізу мережі. Зокрема в дослідженні [61] вказується, що підмножини типу «кліка» є найбільш стійкими і активними, з точки зору інформаційного обміну та впливу на навколишні вузли (інші суб’єкти мережі). Теоретично в межах кліки можуть формуватися протилежні ідеї, але на практиці, в більшості випадків, «кліка» об’єднує однодумців з спільними інтересами та ідеями. Учасники кліки, зазвичай спілкуються і поза межами мережі, їх зв’язки досить стійкі та сталі. Рівень інформаційного впливу на порядки вищий на відміну від підмножин де основним носієм ідеї є окремий суб’єкт, тому що у випадку «кліки» носієм і активним розповсюджувачем ідеї виступає цілий кластер, що відображається і на кількості зв’язків з зовнішніми (по відношенню до кліки) вузлами і на щільності інформаційних повідомлень. В дослідженні [61] вказується і на можливість оцінки віку (зрілості) мережі (як давно вона сформувалась). Наявність клік з великою кількістю включених вузлів говорить про достатньо великий час формування мережі. Пошук клік і їх аналіз є однією з основних задач структурного аналізу мереж.

У випадку коли в межах кліки виникають дві протилежних ідеї і носіями цих ідей є лідери з високим ступенем впливу і довіри – кліка може трансформуватись в лідерську групу. Лідерська група може також

сформуватись за наявності одного яскраво вираженого лідера і наявної множини навколишніх розрізнених вузлів.

Лідерська група (**ЛГ**) – підвид групи з одним або кількома вираженими вузлами, що мають зв’язки з усіма іншими вузлами групи (рис. 2.4).

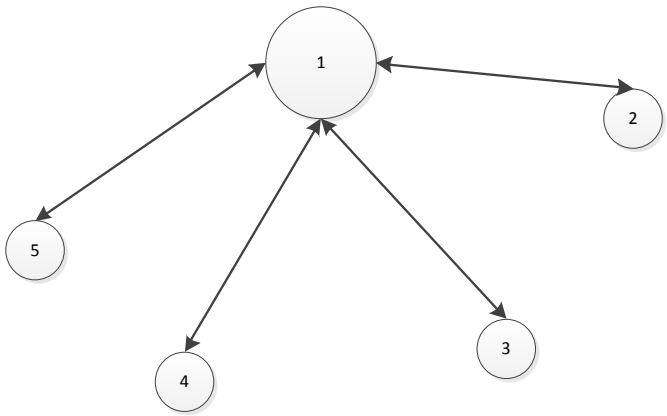


Рисунок 2.4 – Підмножина типу «Лідерська група»

«**ЛГ**» – фактично є підвидом «**Г**» з точки зору теорії графів, але суттєво відрізняється з точки зору структури побудови комунікацій і розвитку. Такі підгрупи утворюються за умови наявності в кластері явного лідера. В класифікаціях можна зустріти тип «его-мережа», підмережа з яскраво вираженим домінуючим лідером, що тяжіє до закритості (мінімум зв’язків з вузлами поза межами даної групи). Варто розглядати також багатополюсні **ЛГ** – коли в групі не один, а декілька вузлів – лідерів.

Варіативність структури СМ досягається за рахунок домішування (або у випадку «К» - вилучення) певної міри випадкових зв’язків. «Пом’якшений» варіант кліки називають К-плекс (поняття введено авторами [45]) – в такій підмножині не всі, але переважна більшість вузлів зв’язані між собою. Такий варіант є ближчим до реальності.

Підмножина типу **Г** в реальності, зазвичай, має певну кількість надлишкових зв’язків відносно означення.

Під структурою мережі можна розуміти не лише топологічні особливості розміщення вузлів в графі та наявні зв’язки. В дослідженнях можна зустріти і інші структурні класифікації та виділення типів мереж. Так

в [63] наводиться класифікація Ч. Хефліна, де мережі структуруються на основі поведінкових моделей агента (суб'єкта мережі) та можливостей, що надає йому та чи інша мережа:

1. A-мережа. Дозволяє агенту позначити і вибудувати своє перебування в соціальній мережі як певній цілком реальній соціальній одиниці з можливістю побудови стійкої соціальної групи.

2. B-мережа. Дозволяє агенту позначити і вибудувати своє перебування в соціальній мережі як певній цілком реальній соціальній одиниці без можливості побудови стійкої соціальної групи.

3. C-мережа. Дозволяє агенту сформувати нові відносини всередині A і B мереж.

4. D-мережа. Допоміжна мережу, що надає інструментарій для побудови та розширення функціональних можливостей відносин між агентами в мережі Інтернет.

При цьому автор класифікації зазначає не лише особливості окремого типу мережі, а й вирішальну роль позиції суб'єкта в мережі (користувач, модератор, адміністратор і т.д.), що відображається і впливає в подальшому на всі інформаційні процеси.

Зустрічаються класифікації на основі критеріїв домінантності (вага лідера і кількість домінуючих лідерів) і комунікативності (щільність зв'язків та інформаційного обміну). Зрозуміло, що всі ці класифікації корелюються між собою. Мережа що відноситься до певної групи за критеріями домінантності і комунікативності буде мати і характерні набори кластерів з їх внутрішньою структурою.

На ряду з іншими критеріями структура носить визначальний характер для соціальної мережі і має вплив на всі процеси, що відбуваються в ході її функціонування та інформаційного обміну в середині. Структурний аналіз мереж є актуальною задачею. Дана задача дуже багатогранна, для досліджень можуть використовуватись різноманітні підходи, методи та засоби. На сьогоднішній день в різноманітних дослідженнях задача структурного налізу

знайшла величезну кількість конкретизацій та породила ряд нових задач і проблем.

Підхід до генерування структури мережі також визначається завданням моделі. У випадку даного конкретного дослідження метою є розробка моделі, що враховувала б індивідуальні характеристики вузла та його поведінкові стратегії, а також дослідження вище згаданих стратегій.

З огляду на мету дослідження можна моделювати певний сегмент мережі з обмеженою кількістю вузлів. Іншим обмеженням щодо структури є статичність зв'язків, тобто зв'язки не змінюються в процесі життєвого циклу моделі, але підхід в той же час повинен передбачати можливість генерування сегментів мережі з різною топологією, тобто фрагмент мережі з урахуванням структурних особливостей на певний фіксований момент часу.

Враховуючи дослідження інших авторів та результати огляду джерел по аналізу мережевих структур, для генерування структури фрагменту мережі пропонується використовувати набір базових кластерів, а конкретні приклади фрагментів реалізувати як комбінацію з базових кластерів. Для моделювання конкретних структур фрагменту мережі обрано наступні типи кластерів: група, кліка, лідерська група. Окрім цього варто зауважити, що в моделі розглядаються сталі, двосторонні зв'язки. Тобто – якщо вузол $V_i \rightarrow V_j$, то і $V_j \rightarrow V_i$. На даному етапі дослідження вузол розглядається як абстрактний об'єкт, без конкретизації його опису та представлення в моделі, єдиною умовою на даному етапі є наявність у вузла зв'язків з іншими вузлами мережі. Саме наявність чи відсутність даних зв'язків і визначають структурні особливості та приналежність фрагменту СМ до певного типу кластерів.

Відомо багато різноманітних способів представлення графу мережі (чи підмножин графу), одним з способів є представлення у вигляді матриць суміжності. Такий спосіб є досить зручним для програмної реалізації, а також для подальшої обробки та аналізу.

Запропонуємо формальний опис кластерів, що використовуються при генерації структури соціальної мережі.

«Група» (Г)

Формальний опис такого кластеру може виглядати так:

$$G_{grupa} = (V_n | \forall\, V_i, V_j : i, j, k_i \leq n \;\exists\; \{E_{ik1}, E_{k1,k2}, E_{k2,k3} .. E_{kn,j}\}), \qquad (2.1)$$

Фактично група є зв'язним графом, матриця суміжності може мати різний вигляд (залежить від щільності зв'язків), а обов'язковою є умова зв'язності – існування шляху між будь-якими двома вершинами кластеру.

Кліка (К) – граф в якому кожен вузол зв'язаний з кожним, або, іншими словами – всі вершини графа суміжні.

Формальний опис кліки:

$$G_{clika} = (V_n | \forall\, V_i, V_j : i, j \leq n \;\exists\; E_{ij}), \qquad (2.2)$$

Матриця суміжності для кліки буде мати вигляд:

i\j	**1**	**2**	**3**	**…**	**n**
1	0	1	1	1	1
2	1	0	1	1	1
3	1	1	0	1	1
…	1	1	1	0	1
n	1	1	1	1	0

Лідерська група (**ЛГ**) – підвид групи з одним або кількома вираженими вузлами, що мають зв'язки з усіма іншими вузлами групи.

Формальний опис лідерської групи:

$$G_{lid\_grup} = (V_n | \exists\, i \leq n, \forall j \leq n \;\exists\; E_{ij}), \qquad (2.3)$$

Матриця суміжності для лідерської групи буде характеризуватись наявністю стовпчика та рядка повністю заповнених 1 (окрім діагонального елементу), матриця матиме вигляд:

i\j	1	**2**	3	…	n
1	0	1	***x***	***x***	***x***
2	1	0	1	1	1
3	***x***	1	0	***x***	***x***
…	***x***	1	***x***	0	***x***
n	***x***	1	***x***	***x***	0

Тут вузол з індексом 2 є лідером, елементи ***x*** в матриці суміжності означає, що інші вузли можуть мати і інші зв'язки, але вони не є обов'язковими для ідентифікації фрагменту мережі як кластера типу «лідерська група»

Задавання структури матрицею суміжності є досить ефективним способом, але для експериментів та візуального сприйняття структури доречним є реалізація в програмній моделі візуального конструктора, що базується на використанні набору базових кластерів з можливістю їх параметризації. Доречною функцією програмної моделі є також можливість внесення «ручних» коректив в структуру: додавання та вилучення вузлів/зв'язків.

Запропонований підхід до генерування структури мережі дозволяє генерувати сегменти мереж з досить різноманітною топологією, а можливість внесення коректив в ручному режимі забезпечує можливість локально змінити структуру та наблизити мережу в моделі до реальної структури мережі, що є об'єктом дослідження.

Запропонований підхід має свої переваги та недоліки.

Переваги

1. Можливість частково автоматизованого генерування структур з різною топологією:

- мережі внутрішньо корпоративних зв'язків
- мережі міжкорпоративних зв'язків
- замкнені мережі організацій

- ситуативні утворення (об’єднання людей спільною ідеєю, подією)

- сегменти соціальних Інтернет мереж

2. Наявність можливості редагування зв’язків дозволяє суттєво підвищити варіативність

3. Можливість детального моделювання структури в СМ в околі досліджуваного вузла.

Недоліки

1. Структура зв’язків і особливості внутрішньої будови кластерів носить випадковий характер

2. Необхідність ручного регулювання за умови більш точного відтворення наявної структури

Наявність випадковості в структурі СМ є відносним недоліком, в деяких випадках моделювання певний ступінь стохастичності є обов’язковою умовою. З іншого боку недолік може бути частково компенсований введенням параметрів при генеруванні базових кластерів.

2.2. Розробка математичної моделі поширення інформаційних впливів у сегменті соціальної мережі з врахуванням особистісних характеристик вузлів соціальної мережі та можливістю обрання різних поведінкових стратегій суб’єктами впливу

Підхід до генерування структури описано в попередньому пункті, наступними етапами в побудові моделі є визначення набору характеристичних параметрів вузла та спосіб формального опису процесу інформаційної взаємодії.

Формальне представлення вузла соціальної мережі в розроблюваній математичній моделі

Вузол мережі характеризується певним набором параметрів, що визначають його поведінку і поточній стан. При виборі параметрів – характеристик вузла необхідно намагатись мінімізувати їх кількість при

цьому не втративши адекватності моделі, модель має давати наближені до реальності результати.

В моделі вузол (користувач соціальної мережі) описується наступними характеристиками:

$$V_i =< Act_{v_i},\ R_{v_i},\ Op\alpha_{v_i},\ I_{v_i}, \{Vj_i\} >, \tag{2.4}$$

де (Act) **Active** – активність користувача, кількість активних діалогів (звернень до інших користувачів) за одну ітерацію моделі; (R) **Reputation** – репутація користувача, вплив інформаційного посилу, сила переконання; (Op) **Opposite** – інформаційний спротив, критичність по відношенню до ідеї, що розповсюджується; (I) **Involvement** – ступінь залученості до ідеї, рівень довіри; $\{Vj_i\}$ - множина контактів, вузлів з якими існує інформаційний обмін, вузла V_i.

Серед вузлів мережі виділимо окремі вузли – генератори ідеї. Дані вузли є активними вузлами і саме вони являються осередками розповсюдження інформаційного посилу. Модель розглядає розповсюдження ідеї конкретного змісту чи спрямування, далі будемо позначати її α-ідея. Модель може передбачати наявність генераторів контрідеї, позначимо її (-α), тобто ідея протилежна до α.

Вузол-генератор α-ідеї формально описується так:

$$Gen_{\alpha i} =< V_i, | Act_{v_i} \sim 1,\ I_{v_i} = Ig >. \tag{2.5}$$

Тобто, генератори – вузли з високою активністю, ступінь залученості до α-ідеї максимальний (залученість рівня генератора). Всі генератори сегменту мережі утворюють множину генераторів - Gen

Основна ідея моделі полягає в формалізації поведінкових стратегій активних вузлів сегменту мережі. Вузол починає активну діяльність за умови його залученості до ідеї $I_{v_i} > 0{,}5Ig$. Тут Ig – це залученість до ідеї рівня

генератора. Величина даного параметра визначається особливостями, метою та контекстом інформаційного впливу. Наприклад, існують дослідження (проводились на замовлення радіостанцій), що визначають необхідну кількість прослуховувань пісні аби вона відклалась в пам'яті слухача і стала популярною. Дослідження встановили, що після 8 прослуховувань пісні на протязі короткого періоду пересічний слухач запам'ятовує мелодію і починає підсвідомо підспівувати при перших акордах мелодії. Тобто в даному випадку, підспівуючи пісню, слухач фактично починає поширювати інформацію, а $Ig = 8$.

Кількість інформаційних посилів вузлам з множини доступних вузлів (контакти V_i) за одну ітерацію моделі пропорційна активності вузла - $|\alpha_i| \sim Act_{v_i}$.

Враховуючи останнє, можна сказати, що запропонована модель має ознаки порогових моделей та моделей на основі клітинних автоматів.

Імітаційне моделювання процесу інформаційного обміну у розроблюваній математичній моделі

Процес інформаційного обміну в моделі можна представляти ітераційним процесом, де кожна окремо взята ітерація відповідає певному часовому дискрету (наприклад: 1 ітерація = 1 уявний день)

Розповсюдження інформаційної ідеї в сегменті соціальної мережі можна оцінювати за інтегральним критерієм, що визначається як:

$$I_{\text{ССМ}}(G) = \sum_{i=1}^{n} I_{v_i}. \quad (2.6)$$

Залученість до α-ідеї окремого вузла визначається за адитивним принцом. Показник залученості рівний сумі накопичених α-посилів на поточну ітерацію:

$$I_{v_j} = \sum_{m=1}^{x} \sum_{i=1}^{n} k_{ij} * \alpha_{im}, \quad (2.7)$$

де I_{v_j} – рівень залученості j-го вузла до α-ідеї, x – поточна ітерація моделювання, n – кількість контактів j-го вузла, α_{im} – повідомлення від i-го вузла на ітерації m, фіксує наявність повідомлення значення параметра визначається як:

$$\alpha_{im} = \begin{cases} 1, & \alpha - \text{посил від } V_i \text{ був } (\text{на ітерації } m) \\ 0, & \alpha - \text{посилу від } V_i \text{ не було } (\text{на ітерації } m) \end{cases}, \quad (2.8)$$

де k_{ij} – коефіцієнт інформаційного впливу, що визначається співвідношенням (2.9):

$$k_{ij} = \frac{R_{v_i}}{Op\alpha_{v_i}}. \quad (2.9)$$

Поведінка і залученість до ідеї визначається параметром I_{v_j}, при перевищенні певного порогового значення вузол вважається залученим до ідеї. Тобто в цьому компоненті моделі прослідковується зв'язок з пороговими моделями. Класичні порогові моделі розглядають лінійну функцію накопичення впливу. Але реальні впливи та залученість до певної ідеї в більшості випадків далека від лінійної залежності. При спробах побудови моделей з нелінійними порогами виникає проблема обґрунтування вибору функції для визначення накопичення. Ступінь залученості до ідеї (рівень довіри) в реальності являє собою складну функцію, що гіпотетично повинна мати вигляд представлений на рис. 2.5.

Рисунок 2.5 – Функція залученості вузла до певної ідеї в результаті інформаційного впливу

Таке припущення можна частково аргументувати, наприклад, рейтингами довіри до політичних сил (особливо на великому проміжку часу, чим більший проміжок – тим ближче вигляд графіка до рис. 2.5) (рис. 2.6).

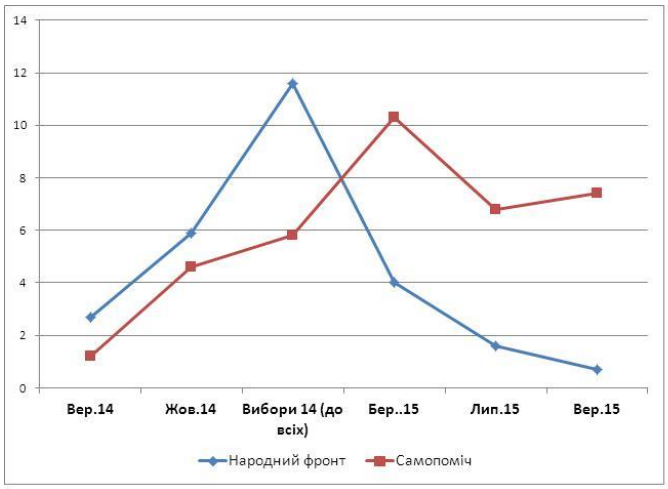


Рисунок 2.6 – Рейтинги політичних партій [87]

Можна провести аналогію і з графіком насичення ринку (рис. 2.7). В даному випадку товар можна розглядати як певну ідею, що пропонується виробником споживачеві. Ситуація представляється досить близькою, з тієї точки зору, що товар рекламується і займає певну позицію на ринку, формується попит. А реклама це теж інформаційний посил, але в даному випадку направлений не на конкретного споживача , а на ринок в цілому.

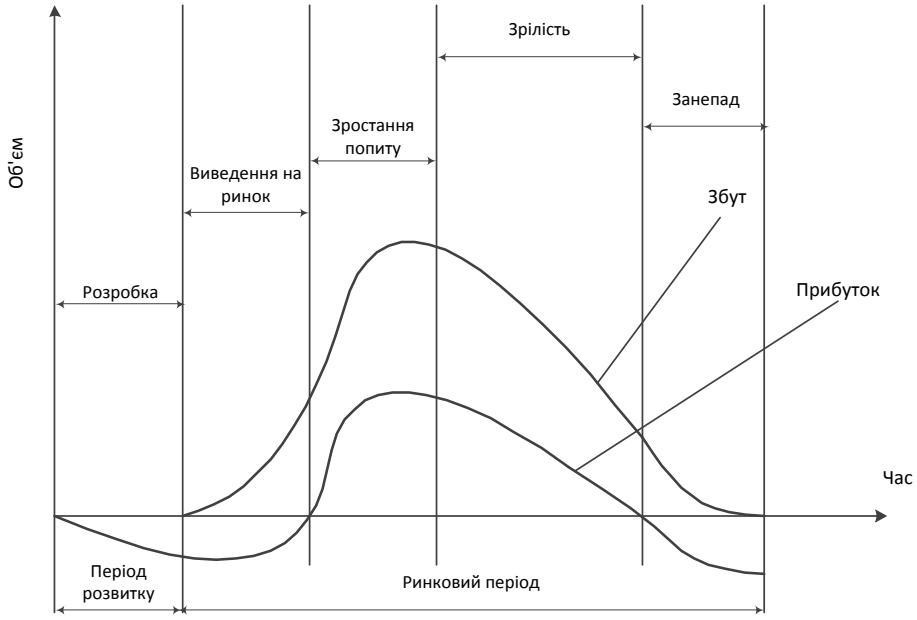


Рисунок 2.7 – Динаміка збуту товару на ринку

Так як наукового обґрунтування поведінки і вигляду функції залученості користувача до певної ідеї, саме в розрізі соціальних мереж, не знайдено, вирішено розглядати варіант кусково-лінійної функції. Адже отримуючи одну і ту ж інформацію від різних адресатів, для кінцевого одержувача вона має різну інформаційну вагу. Чим більше одержувач довіряє відправнику - тим вагомішим для нього є повідомлення. Так як рівень довіри (недовіри) в моделі вже закріплений до конкретної ідеї, то інформаційну вагу (ІВ) пропонується визначати як коефіцієнт, що отримується з відношення:

ІВ = Репутація/Недовіра.

На кожній ітерації швидкість приросту залученості визначається коефіцієнтом (2.9). Функція є монотонно неспадною, максимальним значенням функції є рівень генератора визначений в параметрах моделі. Приклад того як може виглядати функція представлено на рис. 2.8.

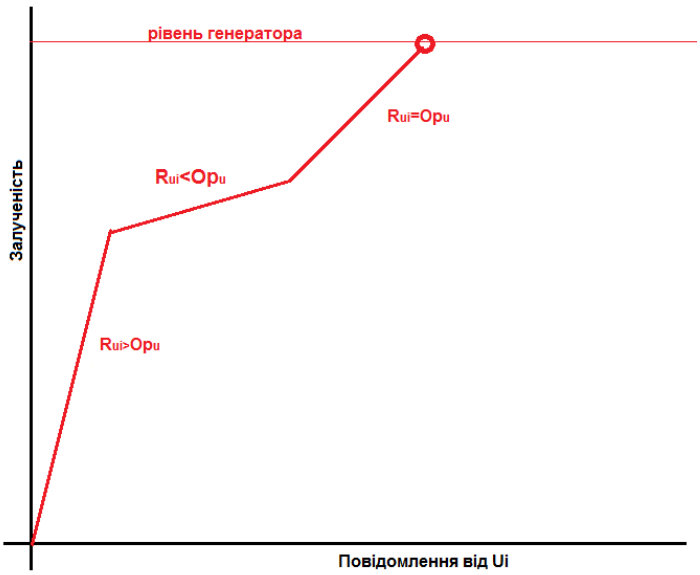


Рисунок 2.8 – Вплив характеристик атакуючого і атакованого вузла на швидкість зростання ступеню залученості

У випадку наявності у соціальній мережі конргенераторів необхідно враховувати їх впливи і тоді формула (2.8) прийме вигляд:

$$\alpha_{im} = \begin{cases} 1,\ \alpha - \text{посил від } V_i \text{ був } (V_i - \text{генератор}) \\ 0, (\text{на ітерації } m \text{ не було ніяких посилів}) \\ -1, (-\alpha) - \text{посил від } V_i \text{ був } (V_i - \text{контргенератор}) \end{cases} . \quad (2.10)$$

При наявності контргенераторів функція залученості перестає бути монотонною і може спадати у випадку, якщо вузол отримує більше повідомлень від контргенераторів. В даному випадку також визначається рівень контргенератора – порогове значення (від'ємне) після якого вузол стає контр генератором, розповсюджувати контрідею вузол починає після зниження значення залученості нижче певного рівня: $I_{v_i} < -0{,}5Ig$.

Запропонована модель враховує характеристики та параметри сегменту СМ (не враховані іншими моделями), що дозволяє більш точно моделювати СМ та знаходити при моделюванні більш ефективні стратегії інформаційного впливу, що показано на порівняльній таблиці 2.1.

Таблиця 2.1

Порівняння існуючих імітаційних моделей поширення інформаційного впливу у соціальних мережах з розробленою моделлю

Моделі	Зміна думки під впливом оточуючих агентів	Вплив структурних особливостей околу агента, та структури мережі в цілому	Різний ступінь схильності агентів до ІВ	Наявність ймовірнісних параметрів	**Врахування активності агента**	Оптимізація ІВ	**Поведінкові стратегії агентів**	Оцінка ймовірності певного результату та розподіл агентів в визначений момент часу	**Параметризація особистісних якостей агента**
Модель Грановветера[110]	+	+	+	-	-	+	-	-	-
Модель Торопова[112]	+	+/-	-	+	-	+	-	-	-
Модель Гончарова-Сироти[115]	+	+	+	-	-	+	-	+/-	-
Модель Ланде[82]	+	-	-	+	-	-	-	+	+/-
Модель Губанова[84, 86, 94]	+	+	+/-	+/-	-/+	+	**-/+**	-	-/+
Запропонована модель	+	+	**+**	**-**	**+**	-/+	**+**	-	**+**

2.3. Розробка методу генерації структури сегменту соціальної мережі з набору параметризованих кластерів різних типів для її програмного імітаційного моделювання

Проаналізувавши різноманітні підходи до генерації структури соціальної мережі та дослідження структури реальних мереж, можна говорити про певну кластеризацію. Тобто в мережі можна виокремити певні підмножини з характерною структурою зв'язків, що дозволяє відносити кожну конкретну підмножину до певного класу. Основні типи кластерів було розглянуто в п. 2.1.

Запропоновано метод генерації структури мережі, що базується на комбінуванні мережі з набору параметризованих підмножин кластерів.

В базовому наборі пропонується використовувати три кластери: група, лідерська група, кліка. Основним параметром при генеруванні кластера є кількість вузлів. В якості додаткового параметра (необхідність виникла в ході проведення певних експериментів) в параметри додано відсоток вузлів з високим рівнем інформаційного спротиву.

Структура мережі включає в себе набір базових кластерів при генерації яких задаються параметри. Для можливості редагування структури та з метою отримання мереж з наперед заданою структурою в програмну реалізацію моделі пропонується додати можливості додавання/вилучення вузлів та додавання вилучення зв'язків. Візуальне розміщення вузлів в конструкторі програмної моделі не має жодного впливу на структуру мережі, так як структура визначається лише наявними зв'язками, лінійна відстань між вузлами може бути довільною, бажано лише дотримуватись вимоги розміщення всіх вузлів в межах екрану. Але останнє теж має суто візуальне значення, ні на процес інформаційного обміну ні на результати це жодним чином не вливає. Один з розповсюджених способів підходу до генерування мережі та способу подальшого збереження – це використання матриць. Зокрема класична теорія графів пропонує матрицю суміжності та матрицю

інциденцій. Матриці досить зручні в обробці й способах збереження, але генерувати матриці великої розмірності з наявними внутрішніми підструктурами а також редагувати структуру мережі в матричному вигляді досить незручно. Враховуючи вище сказане, було вирішено використовувати візуальний конструктор структури мережі на основі набору базових параметризованих кластерів. Матриця суміжності формується в ході створення структури мережі, але лише як допоміжний інструмент.

Наявність візуального відображення структури допомагає в сприйняті структури експериментатором, дозволяє аналізувати особливості структурного положення та вносити зміни в структуру в ході експерименту. Наприклад збільшувати щільність зв'язків, додавати окремі вузли з особливими структурними характеристиками і т.д.

Так як базовим елементом мережі є вузол, а програмна модель базується на об'єктному підході, варто почати розгляд саме з нього. Вузол в програмній моделі представляється окремим класом, що має вигляд:

Лістинг 2.1 – Клас, що описує вузол мережі

```
public sealed class User
    {

        /// <summary>
///  Базові характеристики вузла мережі
        ///  Активність вузла (кількість повідомлень за 1 ітерацію)
        /// </summary>
        public int Activity { get; set; }//(A) Active
        /// Інформаційний спротив//(Op) Opposite
        /// </summary>
        public int Opposite { get; set; }
        /// <summary>
        /// Репутація//(R) Reputation
        /// </summary>
        public int Reputation { get; set; }
        /// <summary>
        /// Залученність//(I) Involvement
        /// </summary>
        public int Involvement { get; set; }//
///  Графічне представлення
        public double PointX { get; set; }
        public double PointY { get; set; }
        private Ellipse ellipse;
        public Ellipse Ellipse
        {
            get { return ellipse; }
```

```
            set { ellipse = value; }
        }//Точка
        public string Name { get; set; } //Ім’я користувача
        public List<User> FriendsList = new List<User>(); //Список контактів
        /// <summary>
///  Додаткові сервісні поля
        public int Level { get; set; }
        /// <summary>
        public List<User>ForTree = new List<User>();
        public int NumberFromMatrix { get; set; }//Порядковий номер в матриці
       }
```

Конкретні значення полів вузол отримує в момент додавання до мережі в залежності від параметрів заданих при генерації кластера, конкретної ролі вузла та інших факторів.

Далі розглянемо метод генерування одного з кластерів на прикладі лідерської групи. Лідерська група (див. п 2.2) характерна наявністю вузла, що має зв’язки з усіма іншими вузлами мережі.

Даний метод передбачає декілька складових етапів:

1 Етап. Створення масиву точок, що будуть визначати візуальне положення вузлів на екрані;

2 Етап. Створення самих вузлів (визначення індивідуальних параметрів) та додавання їх до загального масиву вузлів мережі;

3 Етап. Встановлення структурних особливостей відповідно до обраного типу кластера (створення зв’язків між вузлами);

4 Етап. Внесення змін до матриці суміжності.

Кожен тип кластера в конструкторі має обмеження на кількість вузлів зверху, при встановлені параметрів користувач може задати значення даного параметра (`int countUsers`) в запропонованих конструктором межах. Окрім кількості вузлів в метод передається центральна точка, що визначає місце розміщення кластера на екрані, положення інших вузлів кластера розраховується відносно даної точки.

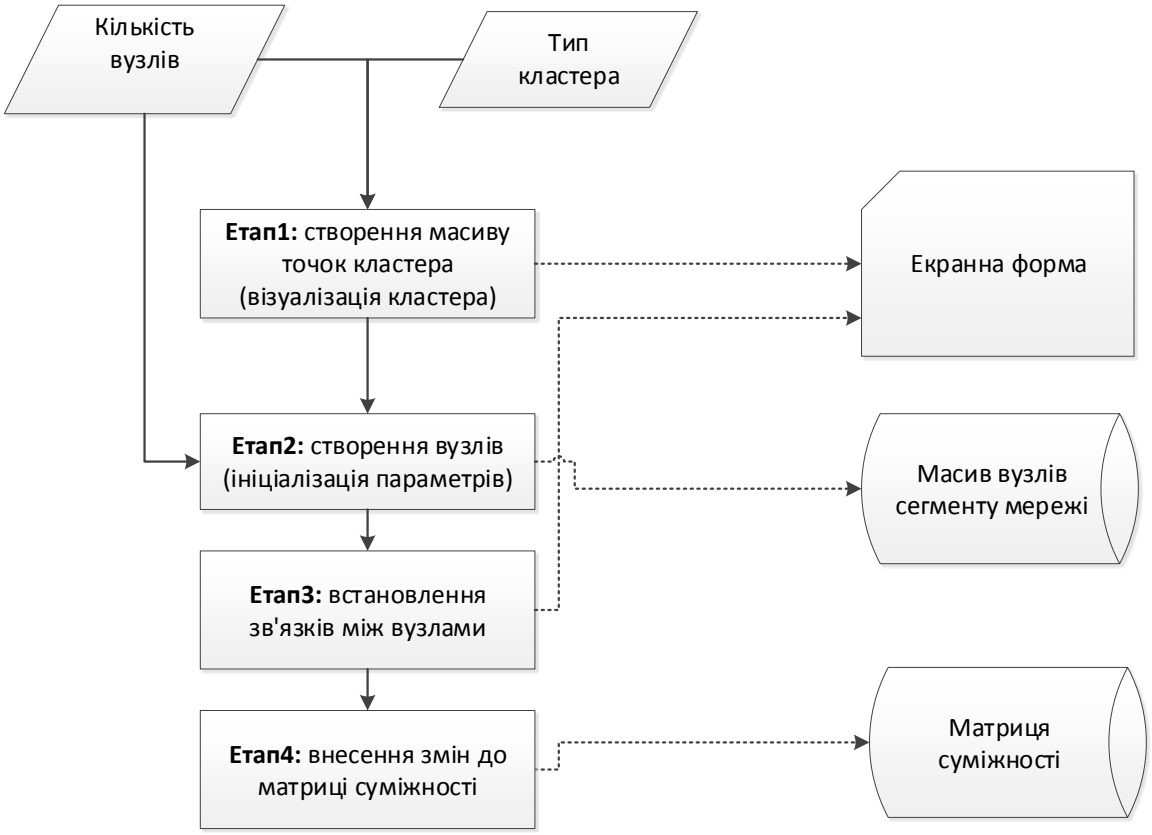


Рисунок 2.9 – Етапи методу генерування структури мережі

Окремо варто охарактеризувати лідера групи. Логічно припустити, що вузол, який є лідером групи, має досить високу (можливо найвищий рівень, відносно інших вузлів групи) репутацію. В противному випадку він не може бути лідером групи. Так як лідер групи має найбільшу кількість зв’язків і для підтримки свого статусу має постійно спілкуватись (вести інформаційний обмін) з іншими членами групи його рівень активності має бути достатньо високим. Інформаційний спротив не нижче середнього з точки зору лідерської позиції в групі.

Інші вузли (якщо не задано параметр високого інформаційного спротиву в кластері) отримують випадкові значення параметрів в допустимих межах. Тим самим реалізується рівномірне розсіювання характеристик по мережі. Залученість до ідеї до першої ітерації моделі в усіх вузлів окрім генератора рівний нулю. Так як положення генератора визначається вже після створення структури мережі, то цей параметр під час генерації не

залежно від типу кластера, а також для окремо доданих вузлів завжди рівний нулю.

Формули, що використовуються для початкової ініціалізації параметрів і-го вузла в кластері представлено нижче.

Active(V_i) = random (1, КК),

де КК – кількість контактів вузла **V_i, Reputation (V_i) = random (1, 90), Opposite (V_i) = random (10, 800), Involvement (V_i) =0.**

Для вузла, що є лідером групи, враховуючи вище описані міркування значення параметрів активності, репутації та спротиву дещо вищі, порівняно з іншими вузлами в кластері:

Active(V_i) = [0.7* КК],

де КК – кількість контактів вузла **V_i, Reputation (V_i) = 100 - random (20), Opposite (V_i) = 500 +random (500), Involvement (V_i) =0**

Лістинг 2.2 – Метод, що реалізує додавання кластеру типу «Лідерська група»

```
internal void AddLiderGroup(Point point_, int countUsers )
        {
// Перевірка знаходження центральної точки в допустимих межах
            if (point_.Y > 90 && point_.Y < 620)
            {
//Буферний масив точок, що відповідають вузлам
                Point[] masPointBuf = new[]
                {
//Створення точок, ініціалізація координат зміщення
                    new Point(0, 0),
                    new Point(10, 10),
                    new Point(20, 10),
……….
                };
//Створення масиву точок відповідно до вказаної кількості вузлів
                Point[] masPoint = new Point[countUsers];
//Цикл присвоєння місцеположення кожному вузлу
                for (int i = 0; i < countUsers; i++)
                {
                    masPoint[i] = masPointBuf[i];
                }
//Створення списку вузлів кластера
                var userList = GenarateUserList(point_, masPoint,
UserList.Count).ToList();
//Визначення випадкового вузла якому присвоюється роль лідера групи
                Random random = new Random();
                int lider = random.Next(0, countUsers);
//Встановлення значень характеристик вузлів
                for (int i = 0; i < userList.Count; i++)
                {
                    if (i==lider)
                    {
                        for (int j = 0; j < countUsers; j++)
```

```
                        {
//Якщо вузол лідер групи
                            if (i!=j)
                            {
                                userList[i].FriendsList.Add(userList[j]);
                                userList[j].FriendsList.Add(userList[i]);
                                userList[i].Activity = (int) 0.7*countUsers;
                                userList[i].Opposite = 500 + random(500);
                                userList[i].Involvement = 0;
                                userList[i].Reputation = 100 - random(20);
                            }
                        }
                    }
                    else
                    {
                        int count = random.Next(0, 2);
                        for (int j = 0; j < count; j++)
                        {
                            int user = random.Next(0, countUsers);
                            if (i != user && !userList[i].FriendsList.Any(x=>x.Name==
userList[user].Name))
                            {
                                userList[i].FriendsList.Add(userList[user]);
                                userList[user].FriendsList.Add(userList[i]);
                                userList[i].Activity = random.Next(1,
userList[user].FriendsList.countUsers);
                                userList[i].Opposite = random.Next(10,800);
                                userList[i].Involvement = 0;
                                userList[i].Reputation = random.Next(1,90);
                            }
                        }
                    }
//Внесення змін до матриці суміжності
                   AddMatrix (userList[i]);
                }
//додавання списку вузлів кластера до загального списку вузлів мережі
                UserList.AddRange(userList);
                }
        }
```

З точки зору користувача моделі (експериментатора) процес додавання кластера полягає в виборі типу, встановленні кількості вузлів (рис. 2.10) та виборі центральної точки на полі розміщення.

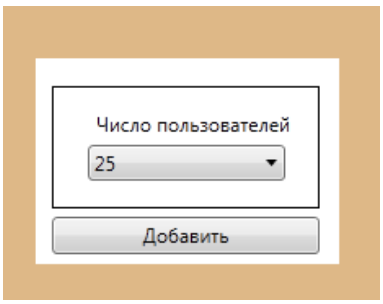
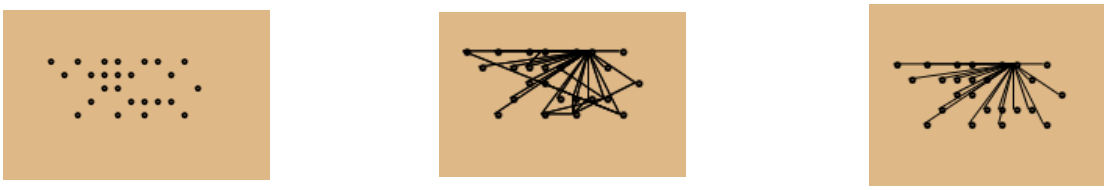


Рисунок 2.10 – Вікно встановлення кількості вузлів

Після відпрацювання алгоритму користувач бачить розміщення кластера на полі (рис. 2.11).



а) **б)** **в)**

Рисунок 2.11 – Різні режими відображення кластера: (а) Початкове відображення вузлів кластера; (б) Кластер в режимі відображення всіх зв’язків; (в) Відображення зв’язків вибраного кластера (в даному випадку лідер групи)

Аналогічно (з точністю до структурних особливостей типу кластера) працюють інші методи генерування кластерів. Приклад згенерованої мережі приведено на рис. 2.12, приклади фрагментів мережі з різних типів кластерів наведено в додатку В.

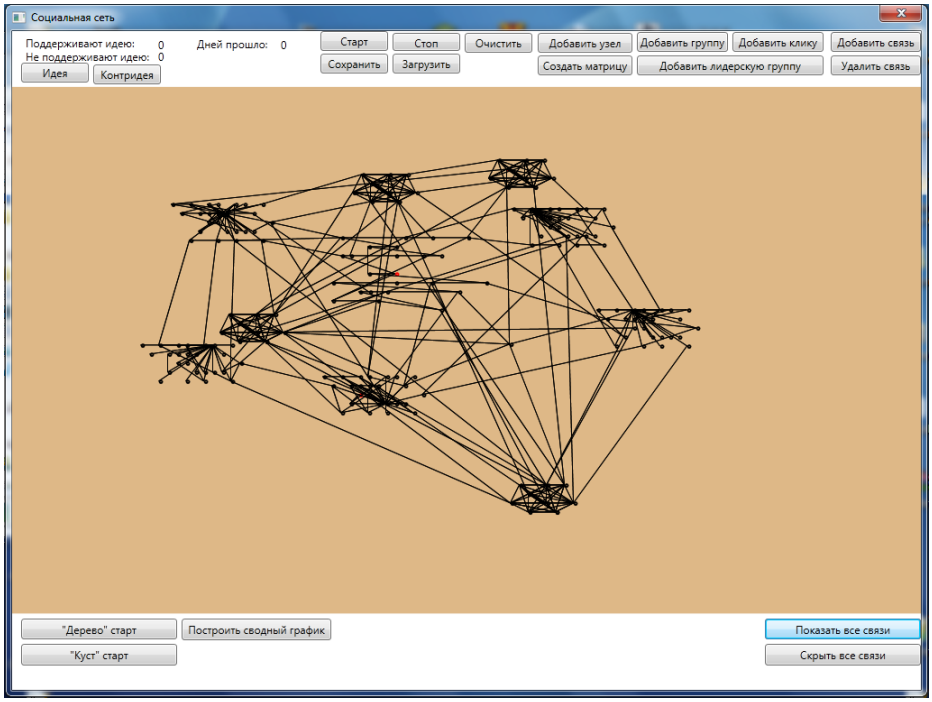


Рисунок 2.12 – Приклад сегменту мережі, що згенеровано в програмній моделі

Як показало дослідження основні роботи в напрямку моделювання соціальних мереж і мережевих структур націлені на моделювання складних мереж (табл. 2.2). Переважна більшість моделей великих мереж переслідують дві основних цілі:

- наблизити розподіл степенів вершин до емпіричних досліджень реальних мереж;

- забезпечити в генерованій мережі діаметр відповідний до реалістичного.

Інші показники й характеристики є непрямими і залежать вже від конкретних модифікацій. Наприклад моделі з вибірковим встановленням зав'язків мають суттєві відмінності кінцевих характеристик графу, ніж моделі з ймовірнісним розподілом зав'язків.

Таблиця 2.2

Порівняння існуючих методів генерації СМ з розробленим методом

Методи	Малий діаметр графу	Рівень ассортативності	Зв'язність графу	Високий рівень кластеризації	**Топологія мережі обирається (наперед заданий набір кластерів)**	**Моделювання околу окремого вузла**	Можливість неоднорідного розподілу щільності зав'язків
Эрдеша-Реньї [102, 103, 109]	+/-	-	+/-	-	-	-	+/-
Уоттса-Строгатца [104]	+	-	+	+	-	-	-
Барабаши-Альберта [105, 109, 109]	+	+	+	-	-	-	+
Боллобаша-Ріордана [106, 109]	+	+	+	-	-	-	+
Баклі-Остхуса [107, 109]	+	+	+	-	-	-	+
Чаес-Боргса [108, 109]	+	+	+	-	-	-	-
Запропонований метод	**+**	**+/-**	**+**	**+**	**+**	**+**	**+**

Порівняльна характеристика методів та моделей, що наведена в таблиці, показує, що запропоновані методи не можуть бути застосовані при досліджені сегментів мережі (малих мереж). Такі структури мають свої

особливості й суттєво відрізняються від великих мереж. В малих масштабах, зокрема показник діаметру графу та розподіл вершин по кількості зав'язків не мають суттєвого впливу на процеси розповсюдження інформації. В той же час кластерна структура (топологія), розподіл щільності зав'язків, структурне положення (оточення вибраного вузла вузлами другого та третього рівнів) вибраного вузла мають критичний вплив на досліджувані процеси. З вище сказаного можна зробити висновок, що запропоновані раніше моделі та методи не можуть бути застосовані до моделювання сегменту мережі в зв'язку з відсутністю в даних методах акцентів на важливі характеристики та показники.

Перевагами розробленого методу по відношенню до існуючих є можливість обрання топології мережі з набору кластерів різних типів та можливість моделювання околу окремого вузла (табл. 2.2).

2.4. Висновки до другого розділу

Другий розділ присвячений дослідженню структурних властивостей СМ, розробці математичної моделі поширення ІВ у сегменті СМ та розробці методу генерації структури сегменту СМ.

Аналіз існуючих моделей поширення ІВ показує, що вони не враховують ряд важливих показників та критеріїв. Більшість з розглянутих в розділі раніше запропонованих моделей не враховує таких характеристик як активність користувача і його поведінкову стратегію. У той же час дослідження в реальних СМ, дослідження в області маркетингу та реклами показують, що ефективність істотно залежить від структурного розташування вузла, його поведінки і особистісних характеристик.

Запропонована модель поширення інформації та ІВ враховує особистісні характеристики вузла, що дозволяє наблизити модель до реальної соціальної мережі. Наявність особистісних параметрів вузлів також дає можливість аналізувати вузли на шляху розповсюдження інформації та

вибудовувати різні поведінкові стратегії (правила першочергового вибору вузлів та інформаційних атак)

Порівняння моделей генерації структури мереж теж дає можливість говорити про певні недоліки. В запропонованих методах виявлено наступні недоліки: низький рівень кластеризації, неможливість наперед визначити структуру мережі. Виходячи з чого, запропоновані методи не можуть бути застосовані в випадку генерації сегменту мережі з наперед заданою структурою зв'язків.

Розроблено математичну модель поширення інформаційних впливів в сегменті соціальної мережі, яка дає можливість застосування різних поведінкових стратегій суб'єктами інформаційного впливу. Окрім безпосередньо поведінкової стратегії активного вузла модель дозволяє проводити дослідження залежності розповсюдження інформації від початкового положення вузла та структури найближчого околу активного вузла-генератора. Крім того, на базі запропонованої моделі розроблено алгоритми моделювання процесу поширення інформаційних впливів у сегментах соціальної мережі, а також алгоритми моделювання структури сегментів соціальної мережі.

Модель передбачає варіанти соціальної мережі з пасивним інформаційним спротивом, тобто коли в мережі відсутні генератори контрідеї і мережі з активним інформаційним спротивом – в мережі наявні генератори протилежної за змістом ідеї (контрідея). Цікаві результати можуть давати експерименти з дослідження протистояння генераторів ідеї та контрідеї, що діють відповідно до різних поведінкових стратегій.

Також, удосконалено метод генерації структури сегменту соціальної мережі для її програмного імітаційного моделювання, що дозволяє обирати різну кількість і типи кластерів у мережі, що, в свою чергу, дозволяє генерувати мережі з наперед визначеною структурою.

РОЗДІЛ 3.
МЕТОДИ ПРОГРАМНОГО ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ПРОЦЕСУ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА МЕТОДИ ВИБОРУ ЦІЛЬОВИХ ВУЗЛІВ СУБ'ЄКТАМИ ВПЛИВУ

В результаті огляду відомих моделей (пункт 1.4) виявлено, що переважна більшість моделей не враховує індивідуальних характеристик вузла. Серед розглянутих моделей не виявлено прикладів моделей які б враховували поведінку окремого вузла, стратегію розповсюдження інформації, яку обирає вузол в процесі інформаційного впливу. В той же час поведінка може мати суттєвий вплив на кінцевий результат та швидкість розповсюдження інформації в мережі.

3.1. Розробка базових поведінкових стратегій суб'єкта впливу у соціальній мережі під час поширення інформаційних впливів

Перед суб'єктом, що виступає генератором в мережі, виникає задача вибору цілі для інформаційної атаки. При цьому генератор повинен намагатись досягти поставленої мети в найбільш ефективний спосіб. Ціль інформаційної атаки обирається на основі поведінкової стратегії. Варто розглядати співвідношення прикладених зусиль (вартість аналізу) і ефективність та швидкість отримання результатів.

Поведінкова стратегія генератора може бути представлена як:

$$F\left(P_1 P_2 \dots P_i, \{Vj_g\}\right) = \{v_1, v_2 \dots v_n\}, \quad (3.1)$$

де $F(P_1 P_2 \dots P_i)$ – функція, що визначає поведінкову стратегію; Vj_g– множина доступних генератору вузлів, тобто підмножина вузлів всієї СМ, що входить

до кола спілкування генератора; $P_1P_2 \dots P_i$ – набір поведінкових критеріїв, $\{v\}$ – множина вибраних для атаки вузлів ($\{v\} \subset \{Vj_g\}$).

Серед поведінкових стратегій можна виділити окремі групи:

– стратегії без аналізу, що базуються на масовості інформаційних посилів в околі генератора;

– стратегії на основі аналізу показників доступних вузлів, базуються на виборі найбільш вразливого чи корисного (з точки зору подальшого розповсюдження інформації) вузла з множини доступних (аналіз вузлів в околі генератора);

– стратегії на основі аналізу структури чи положення вузла, базуються на аналізі структури в околі вузла або наявній інформації про ключове значення вузла (аналіз вузлів поза околом генератора).

Модель передбачає умову того, що у випадку залучення вузла до ідеї він успадковує від атакуючого вузла і стратегію. Тобто, якщо в мережі наявний генератора ідеї, що діє за стратегією $F1\left(P_1P_2 \dots P_i, \{Vj_g\}\right)$ і генератор контрідеї, що діє за стратегією $F2\left(P_1P_2 \dots P_i, \{Vj_g\}\right)$, то всі вузли залучені генератором ідеї діятимуть за стратегією $F1\left(P_1P_2 \dots P_i, \{Vj_g\}\right)$, а вузли залучені до контрідеї за стратегією $F2\left(P_1P_2 \dots P_i, \{Vj_g\}\right)$.

В найпростішому випадку генератор обирає вузли для атаки випадковим чином. Тоді поведінкова стратегія (умовно назвемо її «кущ») може бути описана як:

$$P_{bush} = \left\{u_i \in U_g \middle| i = random\left(\left|U_g\right|\right), |u| \leq Act_g\right\}, \qquad (3.2)$$

де $u_i \in U_g$ – доступні генератору користувачі; $i = random\left(\left|U_g\right|\right)$ – випадковий вибір номера користувача для атаки; $|u| \leq Act_g$ – кількість обраних користувачів (кількість інформаційних посилів за одну ітерацію моделі) не перевищує показника активності генератора.

З огляду на подальшу програмну реалізацію в моделі та для спрощення сприйняття суті даної поведінкової стратегії варто відобразити її у вигляді графічної схеми (рис. 3.1).

Така стратегія не вимагає жодного аналізу, і саме в цьому є її перевага – час, що був заощаджений на аналізі, може бути використано для атак. Тобто дана стратегія опирається на масовість атак за одиницю часу.

Рисунок 3.1 – Блок-схема поведінкової стратегії «кущ»

На відміну від простих стратегій можуть існувати й більш складні багатокритеріальні поведінкові стратегії. Ймовірним є той факт, що більш складна стратегія, яка використовує певний аналіз і вибір вузлів може показувати кращу ефективність. Але реалізація складних стратегій в реальній мережі вимагає певного аналізу, а відповідно і часу. Однією з цілей моделювання є проведення експерименту залежності ефективності різних поведінкових стратегій від структури сегменту мережі та початкового положення генератора в мережі.

Можливі і інші поведінки, коли цілі інформаційної атаки обираються не випадково, а з урахуванням певних характеристик. Найпростішою з точки зору аналізу та доступності характеристикою вузла для атаки є кількість його зв’язків (з точки зору соціальної мережі – кількість друзів). Логічно припустити, що вузли з великою кількістю контактів є більш перспективними для атаки і подальшого розповсюдження ідеї. У випадку вдалої атаки і переконання такого вузла канал передачі значно розширюється. Але в цьому випадку генератору необхідно затрачати певний час для аналізу – вибір вузла для атаки, відповідно кількість активних діалогів має бути зменшена по відношенню до поведінки описаної співвідношенням (3.2). Обравши перспективний вузол для атаки, генератор намагається залучити його до ідеї першочергово – тому зосереджує увагу саме на цьому вузлу (вузлах). В реальності така стратегія визначається повторюваністю звернень до одного вузла на протязі однієї ітерації. Тут проявляється сутність порогових моделей – атака на обраний вузол продовжується до тих пір поки сумарне накопичене значення залученості не перевищить певного встановленого порогового значення, після чого атакований вузол сам стає генератором і починає розповсюджувати ідею в мережі. Кількість вузлів обраних для атаки наступними генераторами (залученими до ідеї) може збільшуватись, враховуючи збільшення носіїв ідеї в мережі і сумарний вплив на атакований вузол.

У випадку цієї поведінкової стратегії (назвемо її умовно «дерево»), вона може бути описана наступним чином:

$$P_{tree} = \{u_i \in U_g \mid |U_{u_i}| \to max, |u| = 2^{l\_g}, |u| \leq K * Act_g, u_i \notin Gen\}, \quad (3.3)$$

де $u_i \in U_g$ – доступні генератору користувачі; $|U_{u_i}| \to max$ – кількість вузлів, доступних атакованому вузлу, обирається за ознакою «максимальна з наявних»; $|u| = 2^{l\_g}$ – кількість вузлів для атаки залежить від рівня генератора (l_g), починаючи від початкового генератора l_g = 0; $|u| \leq K * Act_g$– кількість обраних користувачів не перевищує показника активності генератора з деяким коефіцієнтом, певний час витрачається генератором на аналіз і пошук вузла для атаки.

Для урівноваження стратегій без аналізу, і стратегій, що використовують аналіз, встановимо К=0,5; $u_i \notin Gen$ – атака на вузол продовжується до тих пір поки вузол сам не стане генератором.

Фактично дана стратегія орієнтована на побудову підмережі розповсюдження інформаційної атаки з якомога більш швидким захватом вузлів з найбільшою кількістю контактів. Кількість вузлів залежить від рівня генератора, з збільшенням рівня генератора кількість обраних для атаки вузлів буде зростати. В такому випадку спадає інтенсивність, бо зусилля вузла-генератора розпорошуються на більшу кількість атакованих вузлів. Але це компенсується тим, що збільшення рівня вже гарантує наявність в мережі певної кількості генераторів, їхні зусилля будуть додаватися в сумарний інформаційний вплив. Сформувавши однократно список атакованих вузлів і залучивши їх до ідеї, вузлу варто змінити стратегію на «кущ». Зі списку доступних контактів вже обрано найбільш перспективні вузли, задано напрямок подальшого росту «дерева». Після залучення обраних вузлів не варто витрачати час на аналіз, тим самим підвищуючи активність (максимальна кількість інформаційних атак за ітерацію) за рахунок економії часу на аналіз. Схема даної стратегії представлена на рис. 3.2

Рисунок 3.2 – Блок-схема поведінкової стратегії з аналізом кількості контактів вузлів

Особливості структури сегменту мережі та інші показники можуть вимагати вибору інших поведінкових стратегій. Наприклад – застосування поведінкової стратегії «дерево» з використанням в якості критерію показника кількості контактів потенційної цілі можуть призводити до колізій. Так обраний для атаки вузол може мати найбільшу кількість контактів, але водночас високий рівень інформаційного спротиву. В цьому випадку на залучення до ідеї даного вузла генератором буде витрачено багато часу, що в критичному випадку не призведе до очікуваного результату. Виходом з даної ситуації є зміна критерію вибору вузла, тоді поведінкова стратегія може бути описана як:

$$P_{tree} = \left\{ u_i \in U_g \middle| O_{u_i} \to min, |u| = 2^{l\_g}, |u| \leq K * Act_g, u_i \notin G \right\}. \quad (3.4)$$

В порівнянні з (3.3) змінено лише критерій вибору вузла – обираються вузли з мінімальним рівнем спротиву.

Дана стратегія орієнтована на максимальну швидкість росту дерева за рахунок швидкого залучення вузлів. Вузли з мінімальним інформаційним спротивом будуть долучатись до ідеї за більш короткі інтервали атак. Для цього випадку варто сформувати список розмірності рівня генератора, у випадку залучення якогось з вузлів даного списку він вилучається зі списку атакованих вузлів і поповнюється новим, що обирається за тим же критерієм мінімального інформаційного спротиву серед вузлів, що залишились в списку контактів і не являються самі генераторами. Атака за цією стратегією орієнтована на кількість, стратегія гарантує більш швидке залучення вузлів в підмережу, але кінцевий результат (залучення всієї мережі) може бути ускладнений. Наприклад, за наявності контргенератора, що залучить вибрані вузли з високим рівнем репутації, може настати переломний момент коли якість (вузли з високим рівнем репутації) стануть переважати кількість (кількість залучених вузлів велика, але їх сумарний інформаційний вплив досить низький).

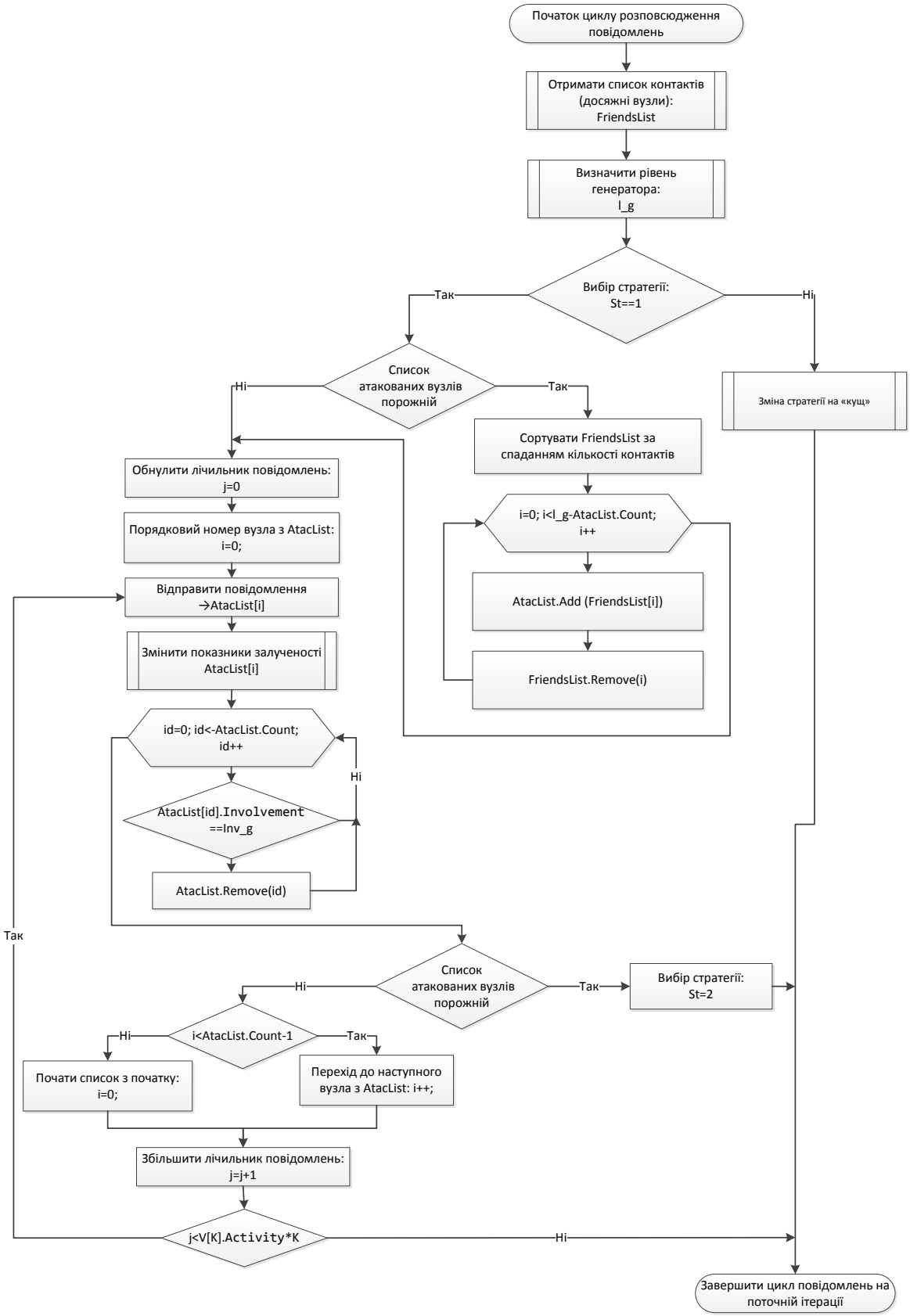


Рисунок 3.3 – Блок-схема поведінкової стратегії «дерево» з критерієм обрання цільових об’єктів за рівнем інформаційного спротиву

Багатокритеріальні поведінкові стратегії природно повинні мати вищу ефективність, але виникає питання про баланс затраченого часу на аналіз критеріїв і приріст ефективності інформаційного впливу.

3.2. Розробка методу програмного імітаційного моделювання процесу поширення інформаційних впливів у соціальній мережі з можливістю моделювання різних поведінкових стратегій суб'єктів впливу

Інформаційний вплив зазвичай здійснюється масованим повторювальним донесенням інформації про певний об'єкт, явище, персону і інше до цільової аудиторії. Для досягнення максимального ефекту в реальному житті інформація пропонується в різноманітних видах та способах представлення.

Яскравим прикладом такого впливу може бути реклама. В даному випадку можна говорити про графічне представлення інформації (зовнішня реклама, реклама в друкованих виданнях), звукове представлення інформації (реклама на радіо, звуковий ряд в великих макетах), відеореклама (реклама на TV каналах). Але основним фактором є фактор повторюваності. Навіть коли споживач уже знайомий з товаром і купує даний товар йому постійно нагадують про те, що саме такий вибір є найбільш вдалим і вигідним, додаючи набір певних аргументів та характеризуючи товар з кращої сторони. В даному прикладі товар можна розглядати як певну інформаційну ідею, виробник хоче переконати (тобто здійснити інформаційний вплив) споживача в даній ідеї.

Враховуючи фактор повторюваності та властивість інформаційного накопичення доречно в програмній моделі реалізувати розповсюдження інформації як певний ітераційний процес. На кожній ітерації активні вузли здійснюють передачу інформації вузлам в околі доступу з метою інформаційного впливу на них. Модель не розглядає абстрактну інформацію,

моделюється розповсюдження конкретної ідеї (α-ідеї), а рівень впливу визначається співвідношенням характеристик вузлів, що приймають участь в ході інформаційного обміну.

Стосовно конкретної моделі, що реалізується в роботі, існує ще ряд особливостей, серед яких варто зазначити наступні:

1. На початковому етапі моделі (нульова ітерація) рівень залученості до α-ідеї в усіх вузлів рівний 0, крім вузлів-генераторів.
2. На першій ітерації моделі інформація надсилається лише генераторами
3. Рівень одиничного інформаційного впливу визначається співвідношенням визначеним в п.2
4. На подальших ітераціях будь-який з вузлів може почати розсилання, якщо рівень залученості вузла перевищує половину рівня генератора
5. Кількість інформаційних повідомлень від конкретного вузла за одну ітерацію визначається рівнем його активності.
6. Вибір вузла для атаки визначається поведінковою стратегією.
7. Модель має графічну інтерпретацію динаміки стану мережі на поточній ітерації – вузли змінюють колір в залежності від рівня залученості. У випадку лише генераторів ідеї - від чорного до червоного, а у випадку наявності генераторів контрідеї – вузли залучені до контр ідеї відображаються зеленим.

Алгоритм, що повинен виконуватись в ході ітераційного процесу, можна словесно описати наступними кроками, блок-схема алгоритму представлена на рис. 3.4:

1. Обхід списку всіх вузлів мережі (сегменту мережі)
2. Якщо вузол активний (залученість до ідеї $I_{v_i} > 0{,}5Ig$, див. п. 2.2):
   - 2.1 Обрати вузол для інформаційної атаки
   - 2.2 Здійснити передачу інформації обраному вузлу
   - 2.3 Зменшити лічильник активності, передаючого вузла

2.4 Якщо лічильник активності більше 0, перейти до 2.1

3. Оновити список з визначенням нових активних вузлів
4. Оновити графічне відображення вузлів сегменту мережі з урахуванням зміни показників залученості на поточній ітерації.

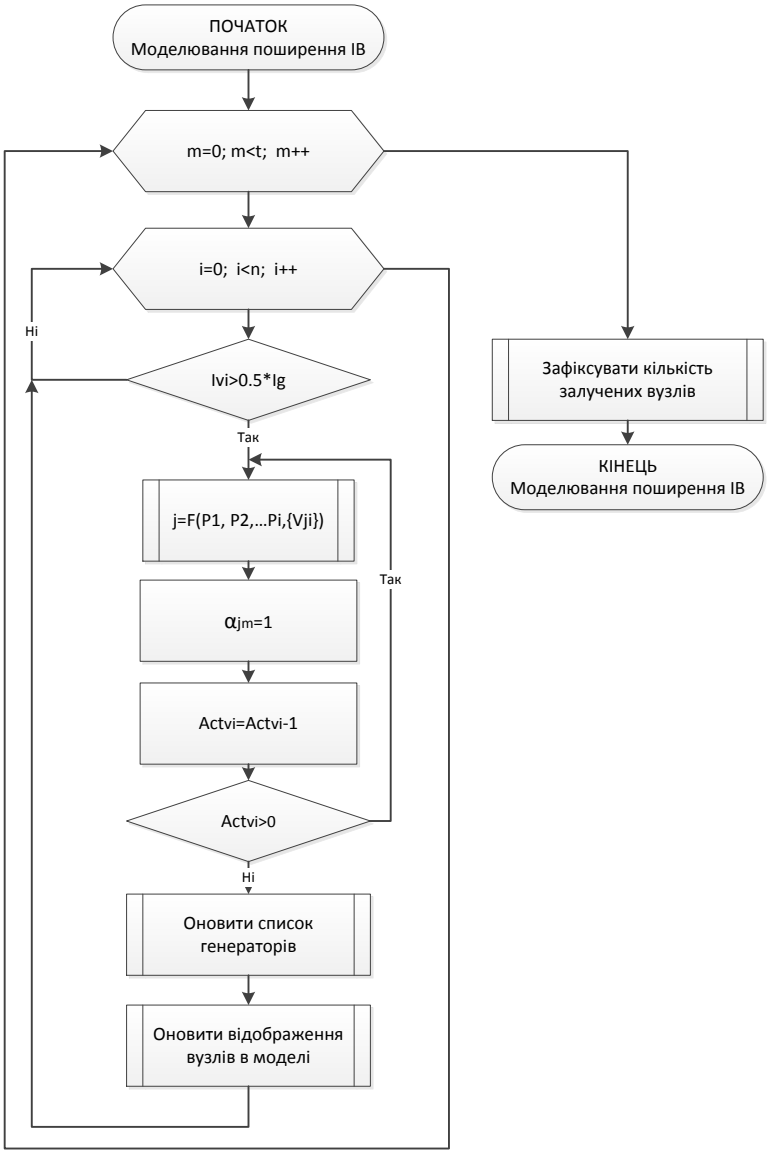


Рисунок 3.4 – Блок-схема алгоритму моделювання поширення ІВ

Програмна модель будується з використанням об’єктно-орієнтованого підходу. Всі дії вузла реалізуються як його методи, окремо існує клас, що слідкує за ітераційним процесом, відраховує ітерації та ініціює дію вузлів. Діаграма базових класів моделі представлена на рис. 3.5.

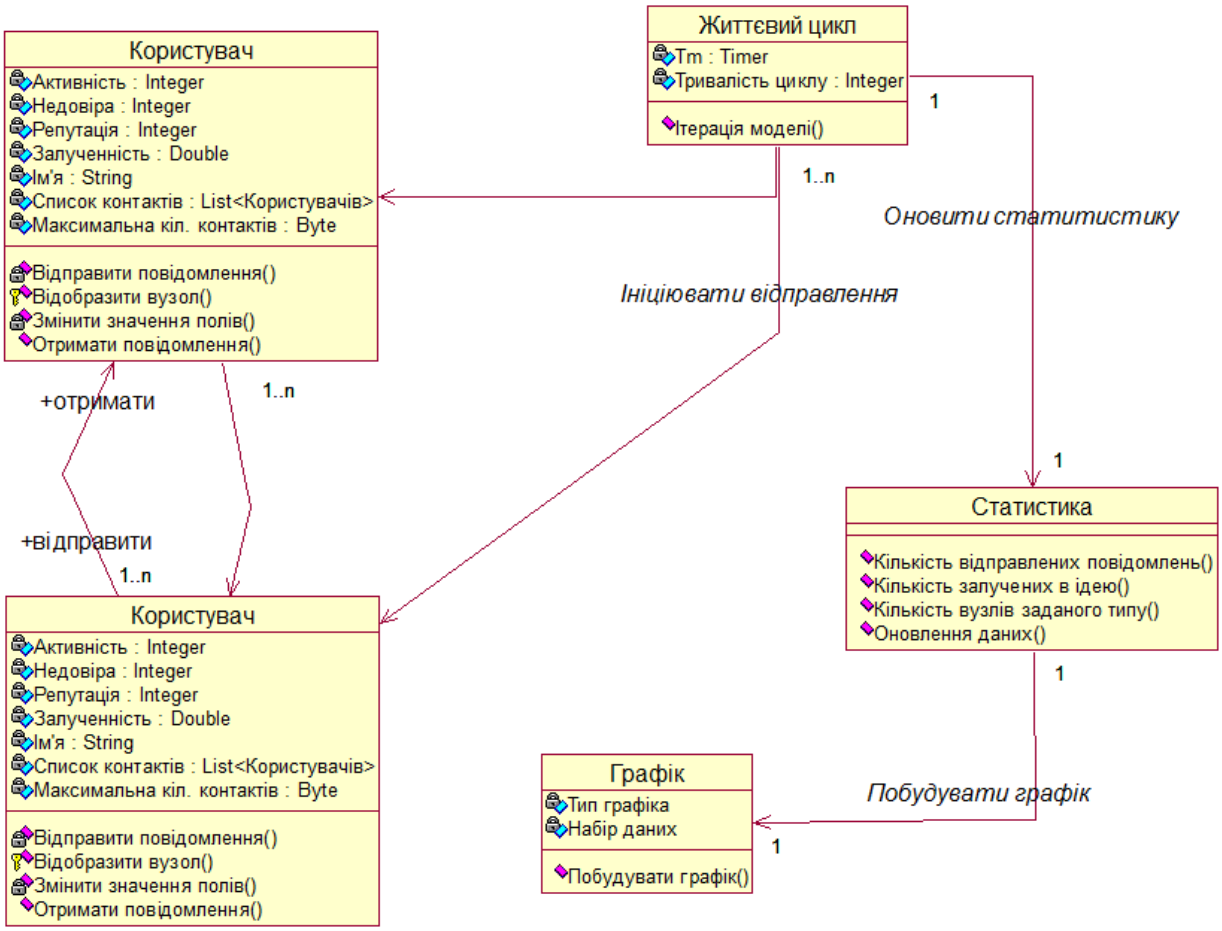


Рисунок 3.5 – Діаграма класів моделі

Далі розглянемо фрагмент коду для випадку стратегії «кущ». За даною стратегією вузол для атаки обирається випадковим чином з доступних вузлів, тобто зі списку контактів вузла, що надсилає повідомлення.

```
public void ShowMessageBush()
        {
            try
            {
                Random rng = new Random();
                //Отримуємо список всіх вузлів мережі
                var users = UserList;
                //Проходимо по списку вузлів
                for (int i = 0; i < users.Count; i++)
                {
                   //Якщо вузол активний
                    if (users[i].Involvement> 0.5*Ig)
                    {
                   //Цикл, що відраховує повідомлення в залежності від активності вузла
                        for (int j= 0; j < users[i].Activity; j++)
                        {
                      //Отримуємо індекс випадкового «друга» (вузол зі списку контактів)
                            int index = rng.Next(0, users[i].FriendsList.Count);
                      //Вираховується коефіцієнт впливу
```

```
                        int damage = (int)
users[i].Reputation/users[i].FriendsList[index].Opposite;
                    //Зміна рівня залученності
                     users[i].FriendsList[index].Involvement += damage;
                   //Перевірка на перевищення показника
                              if (users[i].FriendsList[index].Involvement > 255)
                              {
                                  users[i].FriendsList[index].Involvement = 255;
                              }
                              else if (users[i].FriendsList[index].Involvement < -255)
                              {
                                  users[i].FriendsList[index].Involvement = -255;
                              }
                    //Оновлення списків залучений вузлів
                              if (userSupportList.Contains(users[i]))
                              {
                                  userSupportList.Remove(users[i]);
                              }
                              if (!userUnsupportList.Contains(users[i]))
                              {
                                  userUnsupportList.Add(users[i]);
                              }
                          }
                  //Оновлення кольору відображення відповідно до рівня залученості
                  SolidColorBrush color = new SolidColorBrush();
                  if (users[i].FriendsList[index].Involvement > 0)
                  {
                   color.Color = Color.FromArgb(255,
                   Convert.ToByte(users[i].FriendsList[index].Involvement), 0, 0);
                   users[i].FriendsList[index].Ellipse.Stroke = color;
                    }
                  else
                  {
                  color.Color = Color.FromArgb(255, 0,
                  Convert.ToByte(users[i].FriendsList[index].Involvement * -1), 0);
                 users[i].FriendsList[index].Ellipse.Stroke = color;
                          }}
                      Owner.lbCount.Content = userSupportList.Count;
                  }
              }
          }
```

Для спрощення сприйняття результатів, а також їх аналізу в модель, окрім графічного відображення динаміки залученості в мережі, додано можливість отримання динамічного графіка, що відображає кількість залучених вузлів на кожній ітерації. Графік дозволяє порівнювати швидкість росту залученості від початкових параметрів, порівнювати ефективності стратегій і інші показники. На рисунку 3.5 представлено відображення вузлів та графік залученості на певній ітерації роботи моделі.

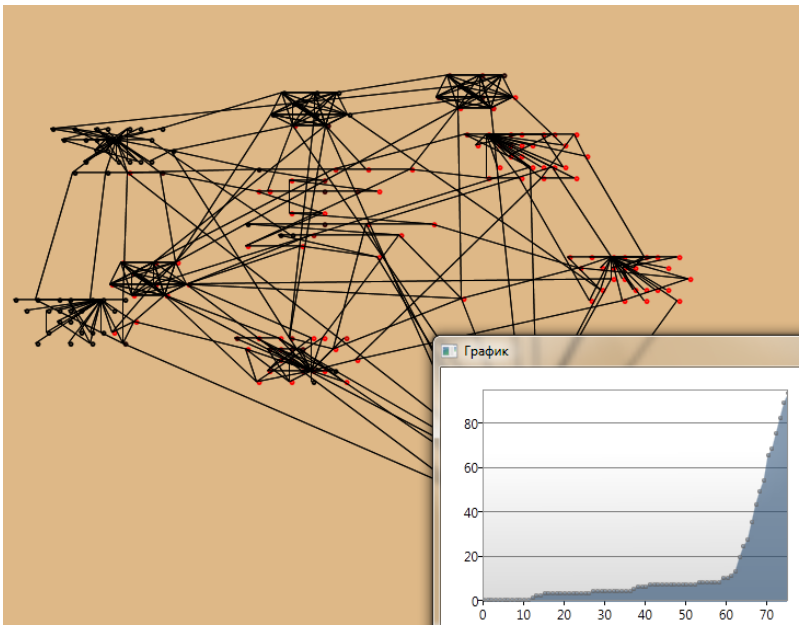


Рисунок 3.5 – Графічне відображення стану мережі на і-й ітерації моделі

3.3 Розробка методу вибору цільових вузлів суб'єктами впливів на основі методу аналізу ієрархій у соціальній мережі під час інформаційних протиборств

Метод аналізу ієрархій – це математична процедура для ієрархічного зображення елементів з метою визначення суті деякої проблеми. Метод полягає в декомпозиції проблеми на більш прості складові частини, а також в обробці суджень особи або осіб, що приймають рішення (ОПР) на підставі парних порівнянь пріоритетів (критеріїв) доцільності. Це дозволяє оцінити рівень взаємодії елементів ієрархії [92].

Ієрархія - тип багаторівневої структури, що передбачає поділ системи на підсистеми по заданих класифікаційною ознаками.

МАІ передбачає кілька етапів:

1. Побудова відповідної ієрархії задачі прийняття рішень.
2. Попарне порівняння всіх елементів ієрархії.
3. Математична обробка отриманої від ОПР інформації (пошук власних векторів матриць попарного порівняння альтернатив).

4. Усунення неузгодженості матриць попарних порівнянь (якщо це необхідно).

Передумовами застосування вищезазначених етапів є:

- вибрано скінченну підмножину альтернатив серед всіх можливих варіантів, в якості альтернатив обираються найбільш прийнятні (на думку ОПР) варіанти з точки зору розв’язуваної задачі та очікуваного результату;

- встановлено набір критеріїв за якими будуть оцінюватися альтернативи.

Коротко охарактеризуємо зміст етапів MAI.

Перший етап передбачає попереднє ранжування критеріїв, в результаті якого вони розташовуються в порядку спадання важливості (значимості).

На другому етапі відбувається попарне порівняння критеріїв за важливістю за дев'ятибальною шкалою зі складанням відповідної матриці (таблиці) розмірності $n_x n$, де n – кількість вибраних критеріїв. Система парних відомостей призводить до результату, який може бути представлений у вигляді обернено симетричною матриці. Елементом матриці a (i, j) є інтенсивність прояву елемента ієрархії (тобто визначення впливу даного критерію на прийняття рішення) **i** щодо елемента ієрархії **j**, що оцінюється за шкалою інтенсивності від 1 до 9, де оцінки мають наступний сенс:

– рівна важливість - 1;

– помірна перевага - 3;

– значна перевага - 5;

– сильна перевага - 7;

– дуже сильна перевага - 9;

– в проміжних випадках ставляться парні оцінки: 2, 4, 6, 8

Матриця парних суджень має вигляд:

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 1/a_{12} & 1 & a_{23} & \dots & a_{2n} \\ 1/a_{13} & 1/a_{23} & 1 & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 1/a_{1n} & 1/a_{2n} & 1/a_{3n} & \dots & 1 \end{pmatrix}, \quad (3.5)$$

де a_{ij} – міра переваги об'єкта a_i в порівнянні з об'єктом a_j.

Якщо в прийнятті рішень бере участь декілька експертів, тоді в матрицю заноситься геометричне середнє різних оцінок в якості загальної оцінки суджень [6].

Таких матриць в ході аналізу створюється (n + 1) матриця, де n - кількість критеріїв: матриця порівняння критеріїв (попарне порівняння, (3.5)) і n матриць попарного порівняння альтернатив за обраним критерієм (A, K1, K2, K3 ... Kn). Розмірність даних матриць mxm, де m – кількість альтернатив, серед яких необхідно обрати найкращий варіант.

На третьому етапі відбувається нормалізація матриці, нормалізована оцінка вектора пріоритетів.

Для пошуку власних векторів може використовуватися метод, заснований на наближених оцінках. Можна знаходити власні вектори вирішуючи СЛАР одержувану з рівняння (3.6).

Нехай число λ і вектор x∈L, x ≠ 0 такі, що

$$Ax = \lambda x. \quad (3.6)$$

Тоді число λ називається власним числом лінійного оператора A, а вектор x власним вектором цього оператора, відповідним власному числу λ.

У скінченномірному просторі L_n векторна рівність (3.6) еквівалентна матричній рівності:

$$(A - \lambda E)X = 0, X \neq 0. \quad (3.7)$$

Звідси випливає, що число λ є власним числом оператора A в тому і тільки тому випадку, коли детермінант det (A-λE) = 0, тобто λ є корінь

многочлена p (λ) = det (A-λE), який називається характеристичним многочленом оператора A. Тут E – одинична діагональна матриця.

$$det(A-\lambda E)=\begin{vmatrix} a_{11}-\lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn}-\lambda \end{vmatrix}=0. \qquad (3.8)$$

Стовпчик координат X будь-якого власного вектора відповідного власному числу λ є нетривіальним розв'язком однорідної системи (3.8).

Але на практиці використовуються більш спрощені методи, наприклад можуть бути застосовані формули (3.9-3.10). Елементи шуканого власного вектора можуть бути знайдені як нормовані середні геометричні числа елементів, які стоять у відповідному рядку вихідної матриці

Формула пошуку власних векторів буде мати вигляд:

$$w_i=\sqrt[n]{\prod_{j=1}^{n} a_{ij}} \ . \qquad (3.9)$$

$$v_i=\frac{w_i}{\sum_{i=1}^{n} w_i}, \qquad (3.10)$$

Узагальнені пріоритети будуть розраховані за допомогою матриці порівняння альтернатив:

Таблиця 3.1

Матриця порівняння альтернатив

	К1	К2	К3	Узагальнені критерії
Критерії	*μ1*	*μ2*	*μ3*	
А1	v_{11}	v_{12}	v_{13}	λ1
А2	v_{21}	v_{22}	v_{23}	λ2
А3	v_{31}	v_{32}	v_{33}	λ3

Тут v_{ij} – отримуємо за формулою (3.10), а μ_i – власний вектор матриці порівняння критеріїв. Далі глобальні пріоритети альтернатив (або узагальнені пріоритети) розраховуються за формулою:

$$\lambda_k = \sum_{i=1}^{n} \mu_i a_{ki}\,, \tag{3.11}$$

де μ_i – власний вектор матриці порівняння критеріїв.

Так як метод MAI не може бути повністю формалізований, через необхідність залучати експертів для оцінки альтернатив за критеріями, на результати методу можуть впливати суб'єктивні чинники - неуважність експертів, помилки оцінок і т.п.. Для перевірки узгодженості суджень експертів була запропонована методика, яка заснована на оцінці відношення однорідності (ВО) матриць попарних порівнянь. Для отримання оцінок запропоновані наступні формули:

$$BO = \frac{IO}{M(IO)}\,, \tag{3.12}$$

де IO – індекс однорідності, який обчислюється за формулою (3.13), $M(IO)$ – середнє значення індексу однорідності випадковим чином складеної матриці парних порівнянь, що базується на експериментальних даних, значенням якого є таблична величина, вхідним параметром виступає розмірність матриці (табл. 3.2).

Таблиця 3.2

Середнє значення індексу однорідності (значення визначені експериментальним шляхом [5, 6])

n	1	2	3	4	5	6	7	8	9	10	11
***M*(*IO*)**	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

$$IO = \frac{\lambda_{\max} - n}{n-1}\,, \tag{3.13}$$

де $\lambda_{\max}$ – максимальне власне значення; n – порядок матриці попарних порівнянь (кількість критеріїв чи альтернатив).

Для розрахунку максимального власного значення матриці існують різні

підходи, один з підходів передбачає використання формули (3.14):

$$\lambda_{\max} = e^T AW, \tag{3.14}$$

де e^T – одиничний вектор розмірності n; A – матриця попарних порівнянь; W – головний (нормалізований) власний вектор матриці A.

Замість ВО і ІО іноді застосовують терміни ОУ (оцінка узгодженості) і ІУ (індекс узгодженості).

Після отримання значення ВО його порівнюють з значенням 0,10, матриця суджень вважається узгодженою якщо ВО <= 0,10. Хоча така оцінка не є однозначною - матриця з оцінкою ВО більше 0,10 насправді може бути узгодженою. Тобто, оцінка ВО це певний маркер, що дозволяє звернути увагу експерта і, можливо, переглянути (перевірити) оцінки.

Найкраща альтернатива визначається за максимальним значенням глобального пріоритету.

В ході експериментів, проведених в роботі, було виявлено необхідність вибору вузла для початкової атаки та суттєву залежність кінцевого результату від правильності такого вибору.

Задача вибору цільового вузла для атаки є задачею вибору в умовах багатокритеріальної оцінки з необхідністю залучення експертів для оцінки альтернативи за певними критеріями, що не підлягають формалізації. Для полегшення розв’язання даної задачі (з урахуванням її формулювання) можна запропонувати використання вище розглянутого методу - MAI.

Для застосування методу необхідна його певна адаптація.

Альтернативи: Вузол_1, Вузол_2…Вузол_n. (множина обраних вузлів потенційно корисних з точки зору розповсюдження інформації)

Критерії варто розділити на: залежні від оцінки експерта і кількісні – незалежні від суб’єктивної експертної оцінки.

До кількісних (незалежних від експерта) критеріїв можна віднести:

- кількість контактів;

- активність (усереднена кількість повідомлень за одиницю часу).

Для ранжуваня альтернатив за даним критерієм пропонується використати формулу (3.16):

$$R(K_{vi}) = \left[9 \cdot \frac{K_{vi}}{Max(K_{vi})} \right], \tag{3.15}$$

де K_{vi} – оцінка і-ї альтернативи за критерієм K_v; $Max(K_{vi})$ – максимальне значення оцінки за критерієм K_v, серед оцінок всіх альтернатив.

Тобто альтернатива з максимальним числовим значенням за критерієм K_v отримає зведену оцінку – 9, а для інших альтернатив отримаємо діапазон зведених оцінок (0..9). При попарному порівнянні альтернатив по критерію беремо різницю оцінок відповідних альтернатив.

До експертних оцінок варто віднести:

- схильність до α-ідеї;
- структурне положення;
- репутація.

В аналізі реальної соціальної мережі експерт має справу з особистостями, і може визначати схильність до α-ідеї як суму неопосередкованих проявів (теми, якими цікавиться людина, участь в обговореннях, конкретні пости та публікації, тощо). В такий же спосіб експертом оцінюється і репутація. В моделі данні чинники формалізовано характеристиками вузла – інформаційний спротив ((Op) **Opposite)** і репутація ((R) **Reputation**) (див. пункт 2.2.1), тому в експерименті ці критерії теж будуть експертно-незалежними.

При експертній оцінці структурного положення варто оцінювати не лише умову, що вузол є мостом (наприклад), але й аналіз околу вузла: кількість контактів всередині різних структурних угрупувань, показники вузлів-контактерів, загальне відношення до α-ідеї структурної підгрупи, де вузол-міст має зв’язки. Адекватність експертної оцінки за даним критерієм дуже важлива, структурне положення – найбільш складний для оцінки критерій.

Найбільш сприятливий результат очікується у випадку оптимальної збалансованості критеріїв. Наприклад, залучення вузла з високим показником репутації, але , й високим рівнем спротиву буде досить ускладненим, що позначиться на динаміці розповсюдження. А вузол з високою активністю й несприятливим структурним положенням матиме мінімальний вплив на розповсюдження в цілому.

Для кореляції балансу пропонується ввести компенсуючі критерії:

1) $\frac{R}{Op}$ – відношення критеріїв на основі властивостей вузла репутації та спротиву;

2) Act*Str– добуток критеріїв на основі властивостей вузла активності та структурного положення.

Перевірка запропонованого методу на програмній моделі

Ефективність і доцільність запропонованого методу перевірена серією експериментів на моделі. Проведено експеримент, попередньо оцінивши перспективи вузлів на основі методу аналізу ієрархій. Експеримент проводиться з використанням програмної моделі, що описана в статтях [11-13]. Для експерименту в моделі створено сегмент соціальної мережі, що містить декілька кластерів (рис. 3.6).

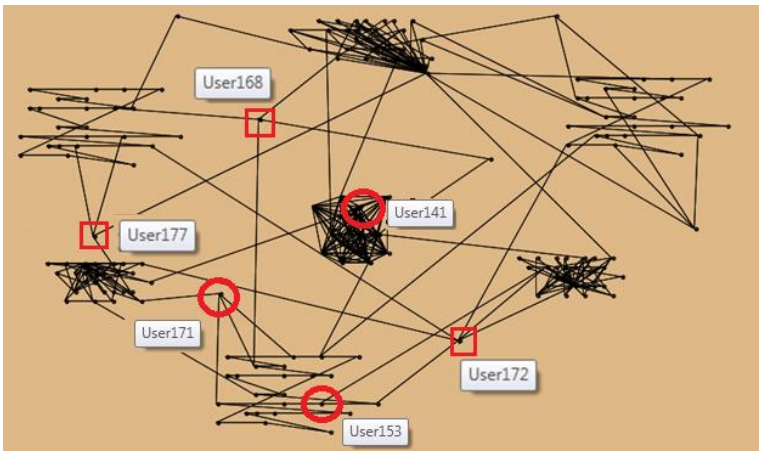


Рисунок 3.6 – Сегмент соціальної мережі згенерований для тестування запропонованого методу

Були проведені обчислення для вибору вузлів для інформаційного

впливу на основі методу MAI, та визначені три альтернативи, це вузли: №168, №172, №177 (зв'язки вузлів відображено в додатку В, рис. В.3-В.6).

Перспективні альтернативи обрані методом MAI виділено на рис. 1 квадратами, колами виділено вузли, що були обрані випадково та потім будуть розглядатись в експерименті для порівняння.

Проілюструємо приклад розрахунків методом MAI для порівняння перспективності вузлів №168, №172, №177.

Кількісні показники, експертна оцінка положення, та нормалізовані показники наведено в таблиці 3.3.

Таблиця 3.3

Оцінки альтернатив за критеріями

Критерії	**Вузли мережі**					
	№ 177	**№ 172**	**№ 168**	**№ 177**	**№ 172**	**№ 168**
	Кількісні показники			***Зведені показники***		
Кількість зв'язків	4	6	4	6	9	6
Активність (Act)	5	3	4	9	5	7
Спротив (Op)	23	20	12	5	5	9
Структурне положення (Str)	6	5	9	6	5	9
Репутація (R)	30	54	67	4	7	9
R/Op	1,3	2,7	5,6	2	4	9
Act * Str	40	18	36	8	4	9

В таблиці 3.4 наведено ранжування критеріїв.

Таблиця 3.4

Ранжування критеріїв

Критерії		**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**
Кількість зв'язків	**K1**	1	0,25	5	0,17	3	2	0,14
Активність (Act)	**K2**	4	1	6	0,33	5	3	0,2
Спротив (Op)	**K3**	0,2	0,17	1	0,17	0,5	0,2	0,13
Структурне положення (Str)	**K4**	6	3	6	1	5	3	0,2
Репутація (R)	**K5**	0,33	0,2	2	0,2	1	0,2	0,17
R/Op	**K6**	0,5	0,33	5	0,33	5	1	0,25
Act * Str	**K7**	7	5	8	5	6	4	1

Як показали попередні експерименти й дослідження, найбільший влив на результат поширення мають активність (особливо в сегментах з щільними зв'язками) та структурне положення. Зазначмо, що структурне положення має в більшості випадків суттєвіший вплив на результат, ніж активність. Відповідно найвпливовішими критеріями (в порядку спадання) є:

– збалансовуючий критерій:Act*Str;

– структурне положення (оцінюється експертом);

– активність (кількісний незалежний показник).

Приклад порівняння альтернатив за одним з критеріїв наведено нижче (табл. 3.5-3.6).

Таблиця 3.5

Матриця парних порівнянь альтернатив відносно критерію К1

	№ 168	**№ 172**	**№ 177**
№ 168	1	0,333333	1
№ 172	3	1	3
№ 177	1	0,333333	1

Вектори матриці
v_0 = 0,2
v_1 = 0,6
v_2 = 0,2

$\lambda_{max} = 3,\ BO = 2{,}46716227694479E-16$

Нижче наведено матрицю отримання узагальнених пріоритетів.

Таблиця 3.6

Матриця порівняння альтернатив

Вузли	**Критерії**						
	К1	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**
	0,074084	**0,149205**	**0,02413**	**0,216401**	**0,034732**	**0,081467**	**0,419981**
№ 168	0,2	0,285714	0,625013	0,581552	0,730645	0,739594	0,46647
№ 172	0,6	0,142857	0,1365	0,109452	0,080961	0,093813	0,100498
№ 177	0,2	0,571429	0,238487	0,308996	0,188394	0,166593	0,433032

Узагальнені пріоритети:

λ_0 = 0,479914570940781

λ_1 = 0,145406604199733

λ_2 = 0,374678824859486

Отже, МАІ серед запропонованих альтернатив визначив найкращим

вибором для атаки вузол **№ 168**. Наступною за пріоритетом альтернативою є вузол **№ 177**, а потім вузол **№ 172.**

Було проведено експеримент на програмній моделі та порівняння отриманих результатів з оцінками альтернатив по MAI.

В експерименті вибрані альтернативні вузли використовувалися як початкові суб'єкти розповсюдження інформації, в якості поведінкової стратегії вузлів використовуватись стратегія «Кущ» – стратегія поведінки, що базувалася на випадковому виборі вузлів для атаки серед контактів суб'єкту впливу, детально дана стратегія описана в статті [6].

Враховуючи особливості стратегії «Кущ», а саме в кінцевій стадії розповсюдження інформаційного впливу залишається невелика кількість вузлів соціальної мережі, до яких розповсюджувана інформація досить довго не буде надходити, будемо оцінювати швидкість захоплення 90% вузлів сегменту мережі. Загальна кількість вузлів в сегменті, що було згенеровано для експерименту – 178, тож будемо оцінювати швидкість захоплення 160 вузлів, за умови початкової атаки від обраного сегменту впливу. Для кожного з альтернативних вузлів проводимо серію з 10 експериментів і усереднюємо результат. Окрім вузлів вибраних серед перспективних альтернатив (вузли №168, №172, №177) проведемо таку ж серію експериментів для трьох випадково вибраних вузлів, що не належать до множини перспективних альтернатив через гірші показники власних властивостей і порівняємо результати. А саме, вузли:

– №153 – вузол вибраний випадково серед вузлів кластеру типу група;

– №141 – вузол вибраний випадково серед вузлів кластеру типу кліка з максимальною кількістю зв'язків в сегменті мережі, що розглядається;

– №171 – вузол вибраний випадково серед вузлів, що є мостами між декількома кластерами.

Розміщення вузлів, що розглядались в експерименті, представлено на рис. 3.6.

Експеримент на моделі показав наступні результати (табл. 3.7).

Таблиця 3.7

Результати експерименту

Вузол	Номер експерименту										Середнє значення
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
	Кількість ітерацій до захоплення 90% вузлів сегменту мережі										
№168	147	142	151	142	138	152	142	147	152	144	146
№177	152	154	154	158	161	151	160	154	150	152	155
№172	166	168	172	174	168	164	166	168	174	172	169
№153	198	201	205	186	198	200	204	198	190	202	198
№141	169	159	156	162	165	158	162	160	162	151	160
№171	184	192	186	186	190	182	196	182	189	184	187

Як видно з результатів експерименту, вузли обрані на основі методу MAI дозволяють за меншу кількість часу поширити інформаційний вплив серед 90% вузлів сегменту соціальної мережі. Також метод MAI вірно визначив пріоритетність обраних альтернатив. Серед вибраних альтернатив по MAI було обрано першим за пріоритетом вузол №168, другим – №177 та третім – №172. Експеримент на програмній моделі підтвердив, що вибір вузла №168, з поміж інших, попередньо обраних, альтернатив є найкращим варіантом, з точки зору ефективності розповсюдження інформації в сегменті мережі. Ефективність атаки з вузлом №168 на 6% вища, ніж з вузлом №177, і на 14% вище від вузлом №172. Також вузли, обрані методом MAI, показали в середньому на 16% кращі результати, ніж вузли обрані випадковим чином серед виграшних структурних позицій соціальної мережі.

Перевагами розробленого методу є (табл. 3.8):

– Врахування структурного положення вузлів соціальної мережі.

– Врахування зв’язків вузлів СМ з перспективними кластерами.

– Врахування інформаційного спротиву оточення вузла СМ.

– Адаптивність методу під особливості сегменту СМ.

Таблиця 3.8

Порівняння існуючих методів вибору цільових вузлів для інф. атаки в ході інформаційного протиборства з розробленим

Методи	Не витрачається час на аналіз	**Враховується структурне положення**	Враховується кількість зав'язків	Враховується репутація вузла	**Враховуються зв'язки з перспективними кластерами**	**Враховується інформаційний спротив оточення**	**Адаптивність методу під особливості сегменту СМ**	Реалізується без залучення експертів
Випадковий вибір вузла	+	-	-	-	-	-	-	+
Вибір вузла з найбільшою кількістю зав'язків	+/-	-	+	-	-	-	-	-
Вибір вузла – «лідера думок» [110, 111]	-	-	+	+	-	-	-	+/-
Розроблений метод – вибір вузла з застосуванням МАІ	-	+	+	+	+	+	+	-

3.4. Висновки до третього розділу

Розроблено базові поведінкові стратегії суб'єктів інформаційного впливу у соціальній мережі під час інформаційних протиборств, що дозволяють ефективно моделювати процес розповсюдження інформаційних впливів при різних стратегіях вибору множини об'єктів інформаційного впливу.

Удосконалено метод програмного імітаційного моделювання процесу поширення інформаційних впливів у соціальній мережі, що дозволяє обирати різну структуру сегменту соціальної мережі та різні поведінкові стратегії суб'єктів інформаційного впливу.

Розроблено метод вибору цільових вузлів суб'єктами інформаційних впливів на основі методу аналізу ієрархій у соціальній мережі під час інформаційних протиборств, який дозволяє за меншу кількість часу поширити інформаційний вплив серед вузлів сегменту соціальної мережі.

Запропонована математична модель може використовуватись як базис для створення програмної моделі для проведення експериментів та отримання різного роду статистик. Основною перевагою запропонованої моделі є можливість дослідження впливу на розповсюдження інформації поведінки окремого вузла, чого не передбачають інші досліджені моделі. Окрім безпосередньо поведінкової стратегії активного вузла модель дозволяє проводити дослідження залежності розповсюдження інформації від початкового положення вузла та структури найближчого околу активного вузла-генератора. Запропоновані поведінкові стратегії вузлів опираються на наявну інформацію про сегмент мережі. Враховуючи особливості конкретного сегменту (структурні особливості, щільність зв'язків, велика кількість з високим рівнем інформаційного спротиву та інш.) соціальної мережі можна обирати найбільш прийнятну для даного сегменту поведінкову стратегію. Вибір правильної стратегії розповсюдження інформації дає можливість суттєво підвищити швидкість її розповсюдження.

Іншим важливим фактором для підвищення швидкості розповсюдження інформаційних впливів в соціальній мережі є вибір вузла, через який початково розпочинається розповсюдження (початковий генератор). Деякі автори, що вивчали дане питання, пропонують застосовувати для розповсюдження інформаційних впливів «лідера думок». В роботі запропоновано метод вибору початкового вузла на основі застосування методу аналізу ієрархій. Підхід вимагає більш глибокого аналізу сегменту мережі та залучення експертів для оцінки сегменту за вибраними критеріями, але вибір початкового вузла за запропонованим методом дозволяє отримати кращі результати та підвищити швидкість розповсюдження інформації в сегменті мережі.

РОЗДІЛ 4.
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНИХ ПОВЕДІНКОВИХ СТРАТЕГІЙ СУБ'ЄКТІВ ВПЛИВУ У СОЦІАЛЬНИХ МЕРЕЖАХ ПІД ЧАС ІНФОРМАЦІЙНИХ ПРОТИБОРСТВ

4.1. Порівняння ефективності застосування різних базових поведінкових стратегій суб'єктами впливу у соціальних мережах під час поширення інформаційних впливів

Для перевірки ефективності запропонованих поведінкових стратегій проведено експерименти на розробленій програмній моделі. Була змодельована мережа з кластерів різних типів (групи, лідерські групи, додаткові вузли і зв'язки), вигляд мережі представлено на рис. 4.1. Вузол генератор поміщено в розрідженій зоні мережі (виділено на рис. 4.1). Загальна кількість вузлів мережі – 150.

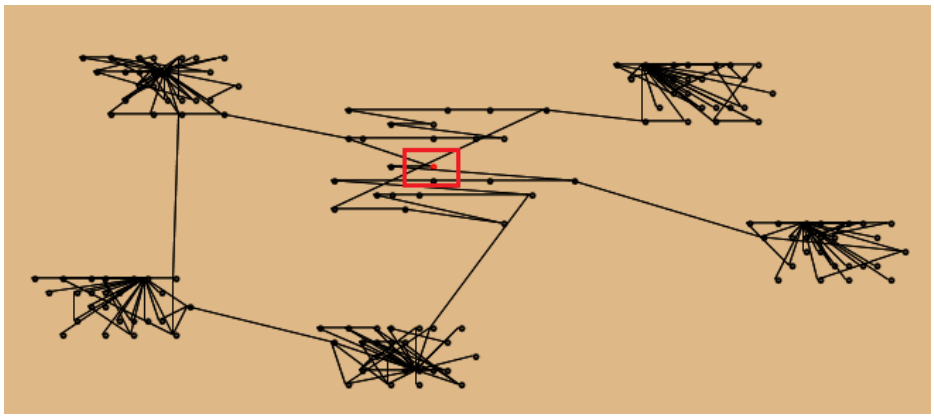


Рисунок 4.1 – Змодельований сегмент мережі для експерименту (150 вузлів)

Моделювання з застосуванням різних поведінкових стратегій дало результати, представлені на рис 4.2. («1» – дерево, «2» кущ).

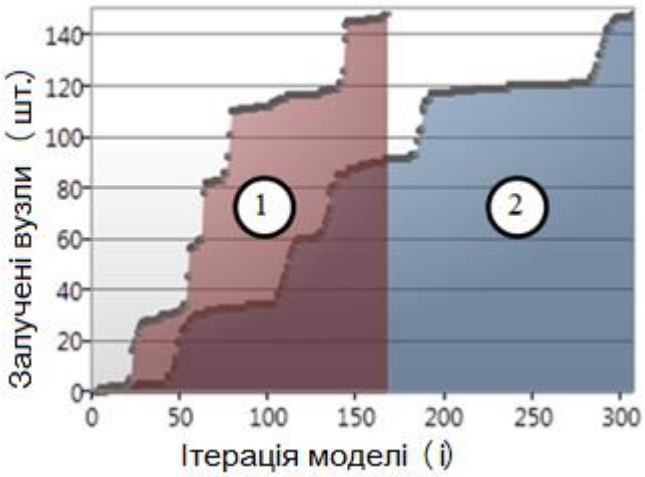


Рисунок 4.2 – Графіки залучення вузлів до ідеї за різними стратегіями генераторів

Я видно з графіків (рис. 4.2) для розповсюдження ідеї всією мережею за стратегією «дерево» знадобилося близько 170 ітерацій, на цій же часовій відмітці «кущ» захопив близько 60% вузлів.

Ситуація дещо змінюється при зростанні щільності зв’язків в мережі, на рис. 4.3 показано графік при збільшені щільності зв’язків на 40% та доповнені мережі декількома вузлами - містками між окремими кластерами (кількість вузлів - 160).

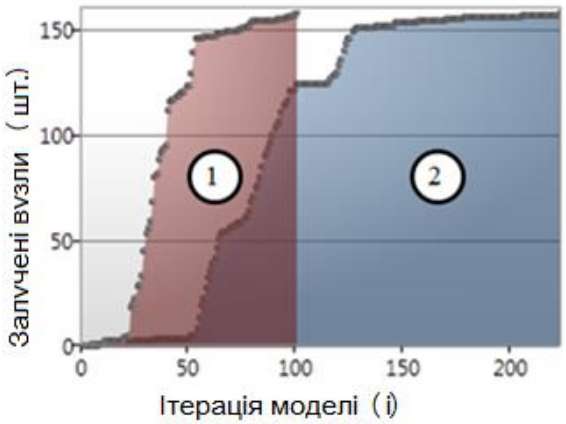


Рисунок 4.3 – Графіки залучення вузлів до ідеї за різними стратегіями генераторів після підвищення щільності зв’язків

Для перевірки гіпотези про вплив щільності зв’язків на ефективність поведінкових стратегій було суттєво збільшено щільність, за рахунок

додавання вузлів і зв’язків, а також додавання кластерів з високою щільністю (кліки). Після внесення змін мережа мала наступний вигляд (рис. 4.4), кількість вузлів – 200, позиція генератора не змінювалась.

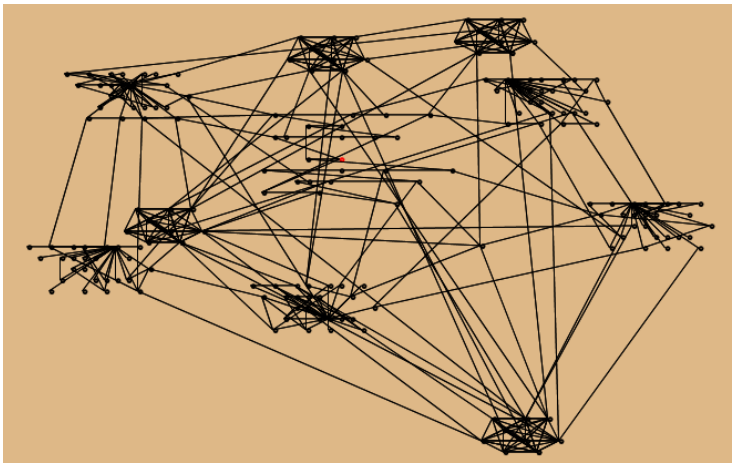


Рисунок 4.4 – Структура сегменту після підвищення рівня щільності за рахунок введення інших вузлів та додавання зв’язків

На цьому варіанті мережі стратегії «кущ» і «дерево» показали майже однакові результати (рис. 4.5). Після 100-ї ітерації обидві стратегії захопили практично всі вузли мережі. Невелика кількість незахоплених вузлів стратегією «кущ» (на які було затрачено ще близько 100 ітерацій) пояснюється випадковим, а не вибірковим підходом до вибору вузла для атаки в стратегії «кущ».

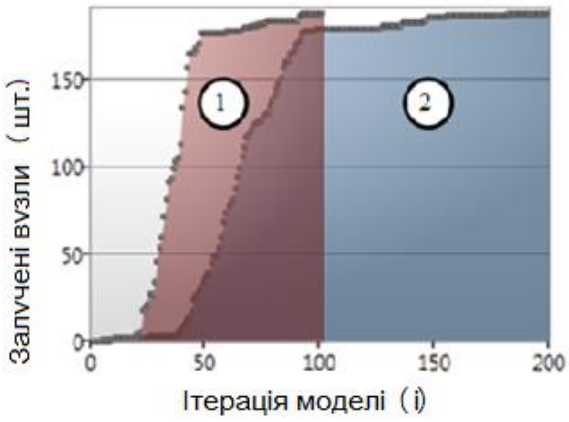


Рисунок 4.5 – Результати експерименту після значного підвищення щільності зв’язків

Загалом стратегія «дерево» показала кращі результати, але в ході

експерименту виявлено, що поведінкова стратегія «дерево» має певні колізії. Так, наприклад, на першому – другому рівнях (на інших рівнях вже не так критично) вибір за критерієм максимальності зв'язків атакованого вузла може обрати вузли з високим рівнем інформаційного спротиву (Opposite). В такому випадку час затрачений на переконання буде суттєво зростати.

Аналізуючи результати отримані в ході експериментів можна зробити висновок про те, що стратегія «дерево» буде мати суттєву перевагу при середній щільності зв'язків. При низькій щільності (кожен з вузлів має невелику кількість контактів) стратегія «кущ» з великою ймовірністю може випадково обирати потрібний вузол і за рахунок вищої активності в наслідок заощадження часу на аналіз буде переважати стратегію, що опирається на аналіз навколишніх вузлів. При високій щільності зв'язків значно підвищується кількість альтернативних шляхів ефективної інформаційної атаки і вирішальним фактором є лише активність вузла генератора.

Отримані в ході експерименту результати показують наступне:

(1) - реакцію моделі на різні типи поведінкових стратегій;

(2) - зменшення ефективності стратегії з вибором за критерієм в порівнянні з випадковим вибором при збільшенні щільності зв'язків мережі;

(3) - графік захоплення вузлів має ступінчасту структуру;

(4) - різкий ріст кількості захоплених вузлів спостерігається після залученості близько 10-15 % від загальної кількості вузлів.

Дані результати можна розглядати як доказ адекватності і відповідності моделі.

(1) та (2) – логічні і передбачувані результати, (3) – різке зростання кількості залучених вузлів спостерігається при появі генераторів в щільних дільницях мережі. На рис. (до графіка 1) представлено структуру на основі 5 кластерів, що мають суттєво більшу щільність зв'язків по відношенню до будь-якої іншої вибраної підмножини (кластери видно візуально), а графік на рис. 1 має п'ять яскраво виражених сходинок. Після підвищення щільності зв'язків мережі, тобто певного вирівнювання щільності по відношенню до

структури представленої на рис. 1, і графік (рис. 3) це демонструє – явно виражених сходинок вже не має, а швидкість зростання графіка збільшилась.

(4) – результаті отримані в моделі співпадають з результатами отриманими вченими політехнічного університету Ранссела ра [7], що проводили дослідження на статистиках отриманих з реальних мереж і отримали результаті на рівні: 10% залучених вузлів визначають інформаційні настрої та прихильність всієї мережі і породжують вирішальні впливи.

4.2. Дослідження ефективності застосування однакових поведінкових стратегій суб'єктами впливу у соціальних мережах при різних характеристиках об'єктів впливу

Попередні експерименти виявили, що при високій щільності зв'язків досліджувані стратегії («кущ» та «дерево») дають досить близькі кінцеві результати. Експеримент проводився зі зміною параметра щільності зв'язків, але не враховувався параметр рівня інформаційного спротиву.

Варто припустити, що при підвищеному рівні інформаційного спротиву в сегменті мережі (існує значна підмножина вузлів, що мають високий рівень інформаційного спротиву (О) **Opposite,** див. П 2.2) стратегія «дерево», з аналізом рівня спротиву навколишніх вузлів, повинна мати суттєві переваги над стратегією «кущ», з випадковим вибором вузла для атаки. Перевага стратегії «дерево» буде виражатись в більш швидкому накопиченні критичної маси залучених до ідеї вузлів, і, як наслідок, оптимізації залучення сегменту в часі.

Для перевірки даного припущення пропонується наступний експеримент:

1. Створюється сегмент мережі з певною визначеною внутрішньою структурою, але з різним відсотком вузлів з високим рівнем інформаційного спротиву (10%, 25%, 50%);

2. Проводиться серія парних експериментів з використанням стратегій «дерево» та «кущ», визначаючи початкове положення генератора в областях сегменту з різним рівнем щільності

3. Визначається кількість захоплених вузлів за фіксовану кількість ітерацій моделі (365 ітерацій – умовний рік в моделі)

В ході експерименту оцінюється швидкість захоплення вузлів сегменту мережі та співвідношення: ЗАХОПЛЕНІ ВУЗЛИ – КІЛЬКІСТЬ ІТЕРАЦІЙ. Стратегія «дерево» визначає сталу детерміновану поведінку і для сегменту мережі з фіксованими параметрами вузлів буде постійно давати однакові результати, за умови визначеного початкового положення вузла-генератора. Стратегія «кущ» обирає вузол для атаки випадковим чином і результати, в серії експериментів, можуть суттєво відрізнятись.

Перед проведенням експерименту необхідно оцінити достовірність результатів отриманих в ході експерименту на моделі. У ряді задач потрібно не тільки знайти для параметра а відповідне чисельне значення, а й оцінити його точність і надійність. Потрібно визначити рівень похибки заміни досліджуваного параметра а його точковою оцінкою ã (точкова оцінка - оцінка, яка визначається одним числом) і з яким ступенем впевненості можна очікувати, що похибка знаходиться в наперед заданому діапазоні. Такого роду завдання особливо актуальні при малому числі спостережень, коли точкова оцінка ã значною мірою випадкова.

Щоб мати уявлення про точність і надійність оцінки ã, в математичній статистиці використовуються так звані довірчі інтервали і довірчі ймовірності. У випадку даного експерименту ã - довірлива величина, що визначає кількість вузлів захоплених за обмежену кількість ітерацій (365 іт.), при умові що розповсюдження відбувається за стратегією «кущ»

Для оцінки розглядається інтервал:

$$\text{Т}\ (\tilde{a} - \varepsilon, \tilde{a} + \varepsilon), \qquad (4.1)$$

який із заданою надійністю β накривав би невипадкове значення параметра генеральної сукупності a, такий інтервал називається довірчим.

Поняття надійність і довірча ймовірність рівнозначні. Зазвичай величину довірчої ймовірності приймають в межах від 0.95 до 0.99.

Знаходження довірчих інтервалів розраховується враховуючи, що математичне очікування, дисперсія і сама оцінка розподілена по нормальному закону.

В даному випадку ε – це відхилення, що вимірюється в кількості вузлів кінцевого результату, від довірливого значення. Приймемо ε =5, в такому випадку довірливий інтервал буде шириною в 10 вузлів. Величина ε визначає розмір можливої похибки.

Наближений метод знаходження інтервалу полягає в тому, що в виразі для ε невідомого параметри замінюють їх точковими оцінками при порівняно невеликому числі дослідів n (близько 10-20) цей прийом зазвичай дає задовільні по точності результати.

Імовірність того, що оцінка не перевищить інтервал ε – підпорядковується нормальному закону:

$$P(|\tilde{a} - a| \leq \varepsilon) = \Phi\left(\frac{\varepsilon}{\sqrt{2} * \sigma_{\tilde{a}}}\right) = \beta. \quad (4.2)$$

В формулі (4.2) a – значення кількості захоплених вузлів, отримане в поточній серії експерименту.

З (4.2) отримаємо такий вираз:

$$\frac{\varepsilon}{\sqrt{2} * \sigma_{\tilde{a}}} = \Phi(\beta)^{-1}, \quad (4.3)$$

де ε - точність оцінки; $\Phi(\beta)^{-1}$ - функція Лапласа.

Вираз (4.3) дозволяє розрахувати точність оцінки:

$$\varepsilon = \sigma_{\overline{m}} * t_{\beta}, \quad (4.4)$$

де $\sigma_{\overline{m}}$ – середньоквадратичне відхилення; t_β – розподіл Лапласа.

Використавши формулу:

$$\sigma_{\overline{m}} = \frac{\sigma}{\sqrt{n}} = \frac{\varepsilon}{t_\beta}. \quad (4.5)$$

Можна оцінити кількість експериментів, які необхідно провести для отримання довірчих результатів:

$$n = (\frac{t_\beta * \sigma}{\varepsilon})^2. \quad (4.6)$$

Таблиця 4.1

Розподіл Лапласа tβ

β	0,9	0,95	0,975	0,99
t_β	1,643	1,960	2,247	2,576

Оцінимо мінімальну кількість експериментів, які потрібно провести для знаходження кількості вузлів захоплених за фіксовану кількість ітерацій за стратегією «кущ», для отримання довірливого значення досліджуваної величини. Отримати математичне очікування для даної величини досить складно, але можна отримати оцінку математичного очікування - як середнє арифметичне отриманих в ході експериментів значень випадкової величини.

Для однієї з конфігурацій сегменту мережі проведено серію експериментів з використанням стратегії «кущ», отримано наступні результати за 365 ітерацій (умовний рік в ітераціях моделі):

Таблиця 4.2

Результати серії експериментів

№ Експ.	1	2	3	4	5	6	7	8	9	10
Кіл. вузлів	124	132	64	131	129	122	129	131	129	68

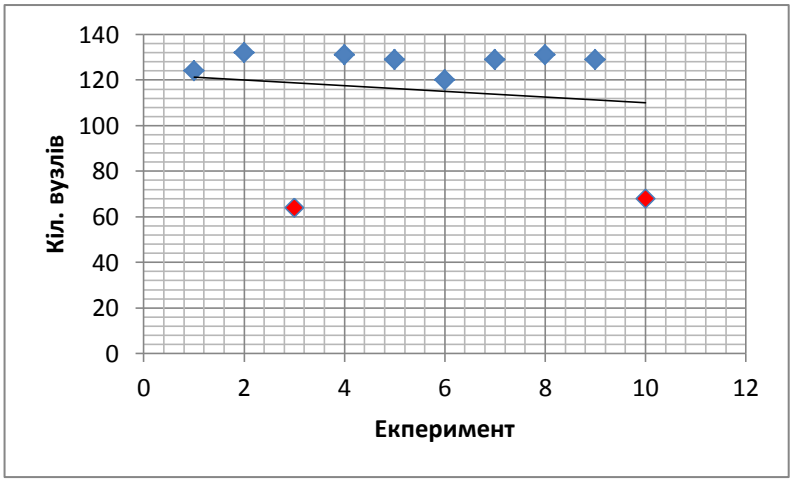


Рисунок 4.6 – Результати серії з 10 експериментів

Як бачимо результати експериментів №3 і №10 суттєво відрізняються від інших. Цей факт може пояснюватись тим, що на початкових ітераціях стратегія «кущ» обрали цілями атаки вузли з високим рівнем спротиву, що суттєво уповільнило процес інформаційного розповсюдження. В оцінку математичного очікування данні результати враховувати не будемо. Відповідно отримаємо оцінку математичного очікування: 128

Найбільше відхилення від оцінки математичного очікування отримали (не враховуючи відкинутих результатів №3 і №10) в експерименті №6, відхилення рівне 8. Використовуючи формулу (4.6) та ε=5, t_β = 1,643 отримаємо:

$$n = (\frac{1,643*8}{5})^2=7$$

Так як по суті серії експериментів не відрізняються будемо вважати отриману оцінку кількості необхідних експериментів справедливою для всіх експериментів в серії. Результати, що перевищують розмір довірливого інтервалу оцінки більше ніж в 2 рази не враховуються.

Для проведення експерименту в програмній моделі створено сегмент мережі з наступною внутрішньою структурою (рис. 4.7), сегмент включає 155 вузлів: 1 кліка, 3 лідерських групи, 3 групи, 3 вільних вузли.

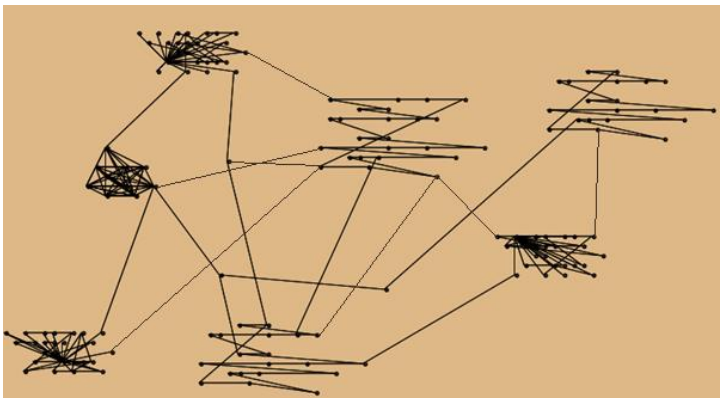


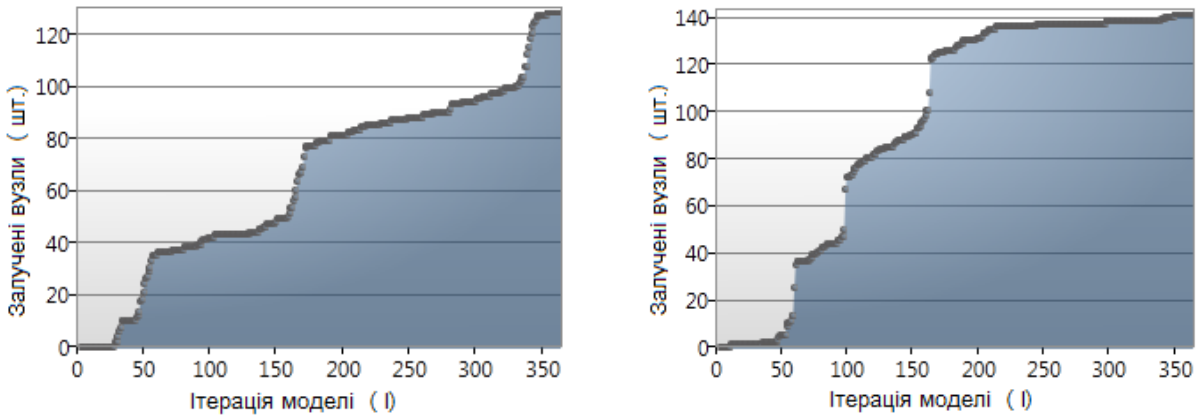
Рисунок 4.7 – Структура мережі для експерименту

Експеримент 1.1 (відсоток вузлів з високим рівнем спротиву – 10%).

Початкове розміщення генератора в зоні з високою щільністю зв’язків (кластер кліка).

Результати стратегії «кущ»: 119, 132, 116, 131, 129, 136, 128 ~ 127 вузлів.

Результати стратегії «дерево»: 142 вузла



а) б)

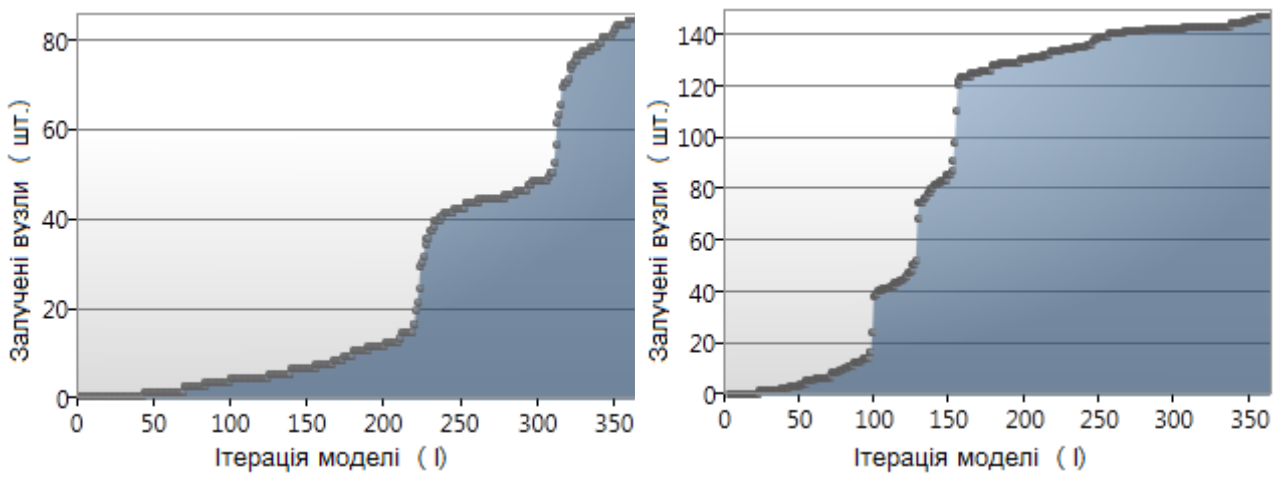
Рисунок 4.8 – Захоплення вузлів (а)-«кущ», б)-«дерево»)

Експеримент 1.2 (відсоток вузлів з високим рівнем спротиву – 10%).

Початкове розміщення генератора в зоні з середньою щільністю зв’язків (кластер «лідерська група»).

Результати стратегії «кущ»: 86, 84, 92, 78, 78, 95, 83 ~ 85 вузлів.

Результати стратегії «дерево»: 148 вузлів.



а) б)

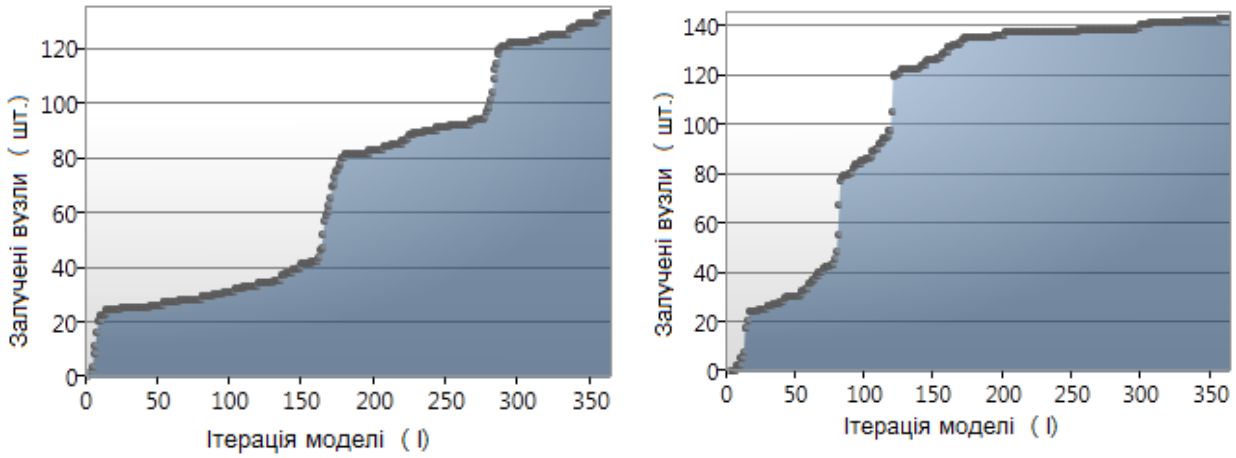
Рисунок 4.9 – Захоплення вузлів (а)-«кущ», б)-«дерево»)

Експеримент 1.3 (відсоток вузлів з високим рівнем спротиву – 10%).

Початкове розміщення генератора в зоні з низькою щільністю зв’язків (кластер «група»).

Результати стратегії «кущ»: 128, 136, 141, 127, 135, 139, 131~ 134 вузла.

Результати стратегії «дерево»: 147 вузлів.



а) б)

Рисунок 4.10 – Захоплення вузлів (а)-«кущ», б)-«дерево»)

Для продовження серії експериментів використовується сегмент мережі тієї ж структури (рис. 4.6) але в серії №2 кількість вузлів з високим

рівнем інформаційного спротиву – 25%, в серії №3 – 50%. Зведемо всі отримані результати в одну таблицю.

Таблиця 4.3

Зведені результати всіх серій експериментів

ВзВРС	**стратегії**	**висока**	**середня**	**низька**
10%	«кущ»	127	85	134
	«дерево»	142	148	147
	приріст	*12%*	*74%*	*10%*
25%	«кущ»	124	80	128
	«дерево»	140	147	144
	приріст	*13%*	*84%*	*13%*
50%	«кущ»	50	51	53
	«дерево»	80	80	80
	приріст	*60%*	*57%*	*51%*

** курсивом виділено перевага «дерева» в відсотках при вибраних параметрах*

** ВзВРС – вузли з високим рівнем спротиву*

Графічно результати експерименту представлені на наступних графіках (рис. 4.10 – 4.11).

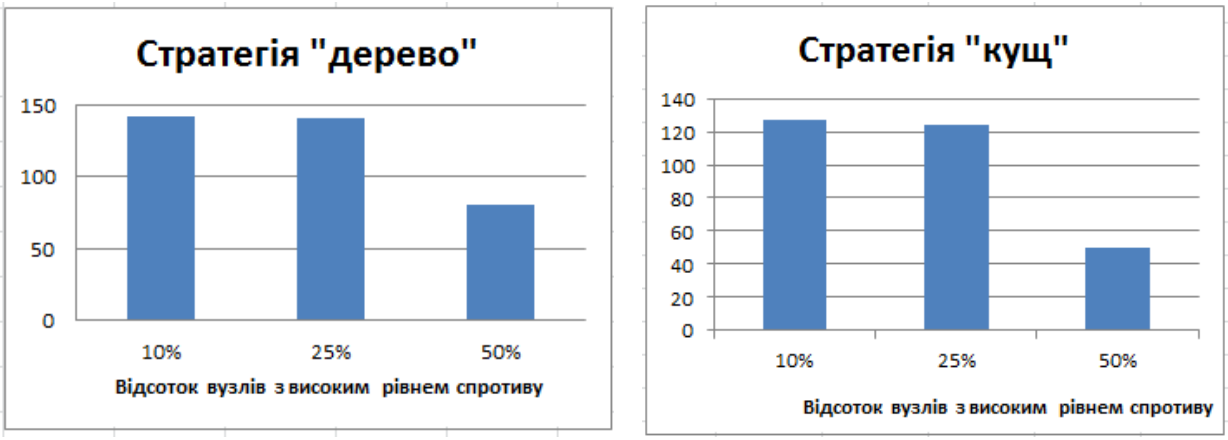


Рисунок 4.11 – Зниження результативності стратегій з збільшенням відсотка вузлів з високим рівнем спротиву

Графіки (та данні в табл. 4.3) показують, що при збільшені відсотка ВзВРС з 10% до 25% стратегії практично не втрачають результативності. При збільшені відсотка ВзВРС до 50% стратегія «кущ» зменшила результативність більше ніж в 2 рази – з 124 до 50 (60%), стратегія «дерево» теж втратила, але не так суттєво: з 140 до 80 (43%).

В усіх випадках стратегія «дерево» мала перевагу. Найбільш суттєва перевага в 84% була отримана при умовах: 25% ВзВРС та початкове розміщення генератора в зоні з середньою щільністю зв’язків.

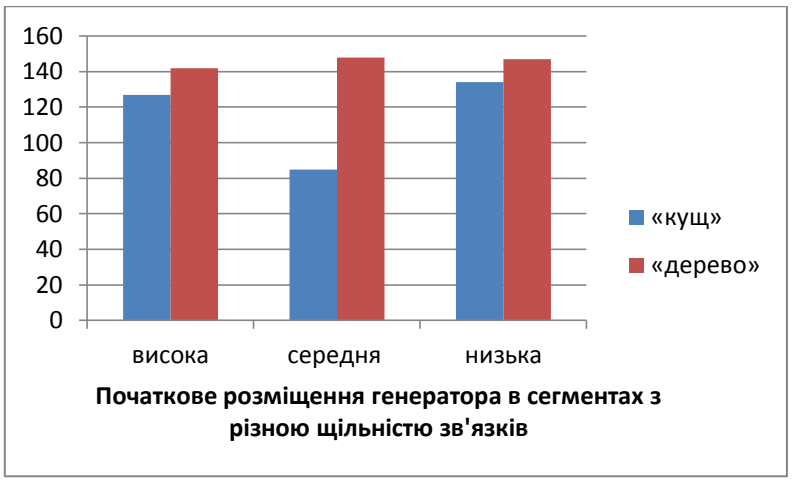


Рисунок 4.12 – Порівняння стратегій при розміщенні генератора в зонах з різною щільністю

Графіки переваги стратегії «дерево» над стратегією «кущ» у відсотках показано на графіках (рис. 4.13).

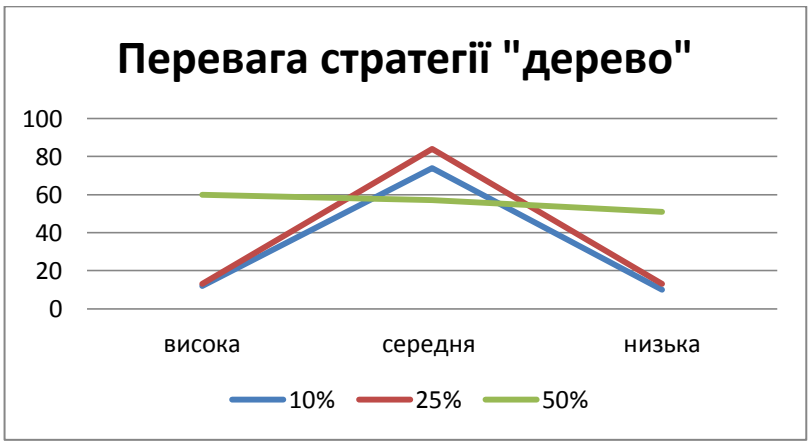
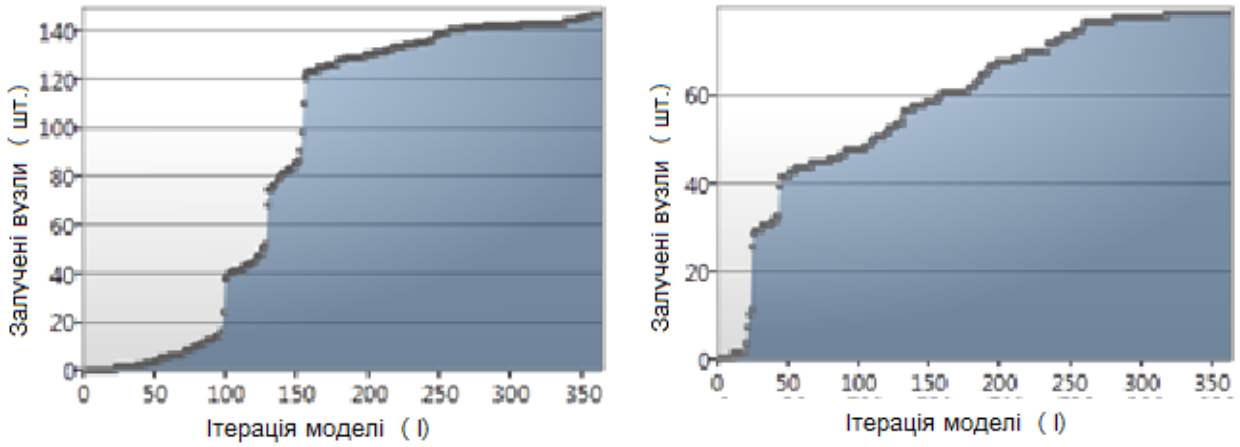


Рисунок 4.13 – Переваги стратегії «дерево» у відсотках

Загалом стратегія «дерево» з аналізом показника інформаційного спротиву навколишніх вузлів показала кращу стабільність на фоні зростання відсотка вузлів з високим рівнем інформаційного спротиву та, як наслідок, зростання загального рівня пасивного інформаційного спротиву сегменту мережі. З збільшенням відсотка ВзВРС швидкість залучення вузлів до ідеї

спадає, періоди стабільної кількості залучених учасників видовжуються, зникає чіткість «сходинок» (при появі активних вузлів в зонах високої щільності зв’язків).



а) б)

Рисунок 4.14 – Стратегія «дерево» при різних параметрах експерименту

а) ВзВРС -10% (генератор в зоні середньої щільності)

б) ВзВРС -50% (генератор в зоні середньої щільності)

Перевагу стратегії «дерево» з аналізом показника спротиву при даних параметрах експерименту можна також проілюструвати в порівнянні з стратегією «дерево», але з критерієм по кількості вузлів (див. формулу (3.3)).

Графік залученості вузлів при умовах: ВзВРС -50%, генератор в зоні середньої щільності стратегія «дерево» з аналізом кількості зв’язків представлено на рис. 4.14.

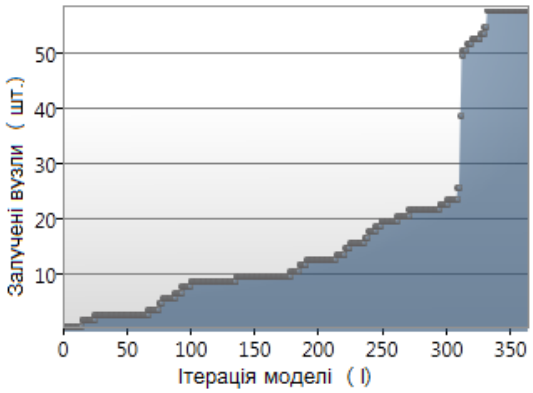


Рисунок 4.15 – Стратегія «дерево» з аналізом кількості зв’язків

Аналізуючи графік 4.15 та порівнюючи його з 4.14 (б), можна зробити висновки:

- «дерево» з аналізом показника спротиву (у випадку сегменту з великим відсотком ВзВРС) дозволяє швидше накопичити критичну масу залучених вузлів, сумарний атакуючий потенціал яких може побороти інформаційний спротив незалученнях вузлів: графік в початковій стадії стрімкий, в пізніх стадіях - більш плавний але з постійним видимим зростанням.

- «дерево» з аналізом кількості зв'язків (у випадку сегменту з великим відсотком ВзВРС) повільно накопичує критичну масу, бо стикається в своєму виборі з вузлами, що мають високий спротив, на початковому етапі втрачається багато часу на залучення. В пізніх стадіях потенціал залучених вузлів з великою кількістю зв'язків починає спрацьовувати, але така стратегія не встигає залучити велику кількість вузлів за обмежену кількість ітерацій: графік в початковій стадії зростає повільно, в пізніх стадіях – можливі різкі зростання.

4.3. Дослідження ефективності застосування однакових поведінкових стратегій суб'єктами впливу у соціальних мережах при різних структурних параметрах сегменту соціальної мережі

В ході одного з експериментів отримано результати, що яскраво свідчать про значимість структурного положення та структури зв'язків залученого вузла на подальше розповсюдження інформації.

Зокрема на рисунку 4.16 представлено фрагмент мережі з двома активними вузлами в початковій фазі (червоним відмічається генератор ідеї, зеленим – генератор контр ідеї), загальна кількість вузлів в сегменті - 150. Обидва генератори знаходяться в розрідженій відносно зв'язків зоні, кількість початкових контактів в них однакова – по 3 зв'язки в кожного. Проведений експеримент показує, що контргенератор досить швидко

захоплює сегмент мережі (рисунок 4.17), після 86 ітерацій моделі спостерігається стабілізація з розподілом захоплення: прихильники ідеї -8 вузлів, контрідея – 142 вузли.

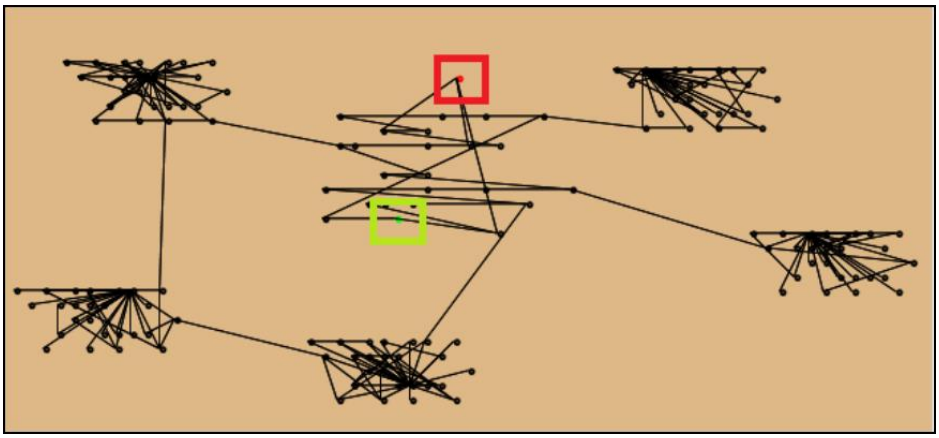


Рисунок 4.16 – Початкове розміщення генераторів

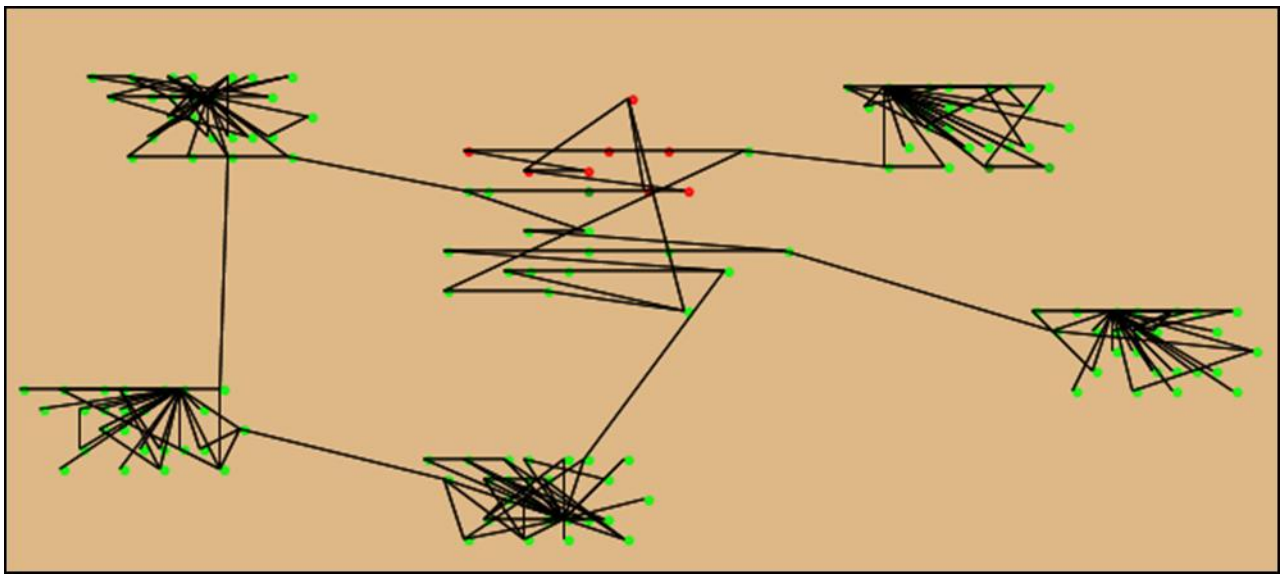


Рисунок 4.17 – Розподіл прихильників після стабілізації процесу інформаційного обміну та впливу (86 ітерацій)

В наступному експерименті для вузла генератора було додано один зв’язок (рисунок 4.18). Корективи полягають в тому, що тепер генератор має прямий зв’язок з вузлом, який виступає зв’язковою ланкою між окремими

кластерами в мережі. Тобто вузол виділений на рис. 4.18 являється вузлом-мостом.

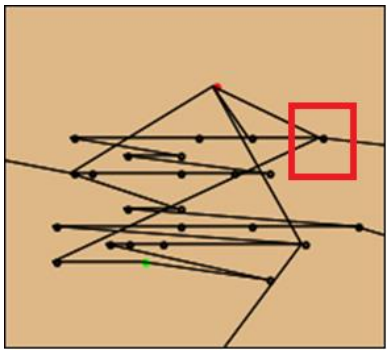


Рисунок 4.18 – Додатковий зв’язок генератора з вузлом-мостом

Після внесення таких змін кінцевий результат кардинально змінюється, вже після 36 ітерацій генератор захвачує майже всі вузли сегменту, розподіл захоплення: прихильники ідеї -148 вузлів, контрідея – 2 вузли. Кінцевий вигляд мережі після стабілізації представлено на рис. 4.19.

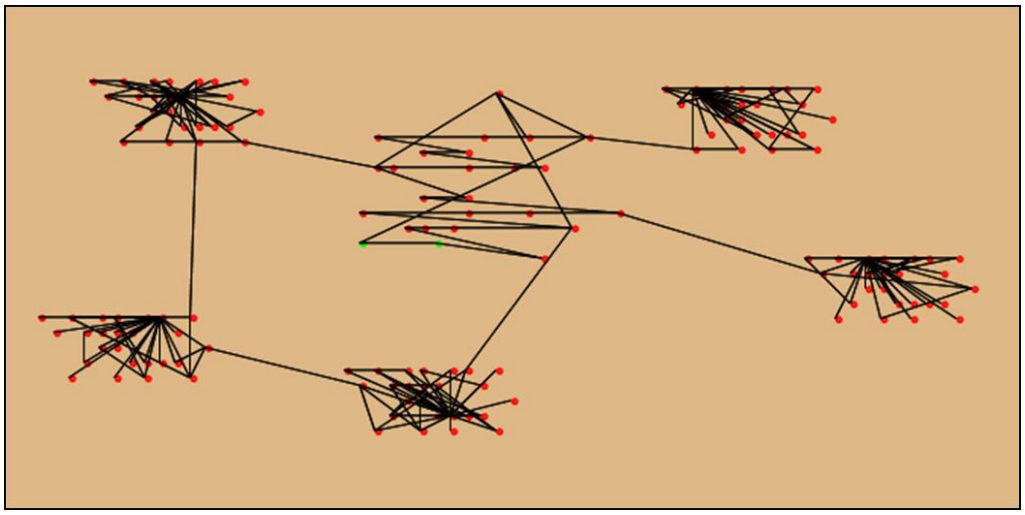


Рисунок 4.19 – Результат захоплення вузлів після внесення коректив відносно початкового набору зв’язків

В розглянутому вище прикладі вузол (виділений на рис. 4.18) виступає вузлом –мостом. З точки зору математичної формальної теорії графів вузли такого типу описуються як точки зв’язності.

Граф G (описаний у вигляді (1.1)) містить точку зв’язності ***a***, якщо для деякої пари вершин ***v*** і ***w*** всі шляхи з ***v*** в ***w*** проходять через ***a***. Видалення

точки зв’язності (точки розриву) розбиває граф, принаймні, на 2 незв'язні частини.

На множині ребер E графа G можна визначити відношення еквівалентності: $e_1 \cong e_2$, якщо $e_1 = e_2$ або обидва ребра лежать в одному циклі.

Нехай $E_1, E_2, ..., E_k$ - класи еквівалентності ($E_i \cap E_j = \varnothing$) і $V_1, V_2, ..., V_k$ - відповідні їм множини вершин. Тоді $G_i = (V_i, E_i)$ - це двохзв’язні компоненти G

Лемма, що визначає двохзв’язні компоненти, точки зв’язності і їх властивості (запропонована Ахо):

1. Графи G_i - двохзв’язні $\forall i$.

2. $\forall i \neq j$ множина $V_i \cap V_j$ містить не більше однієї вершини.

3. v - точка зв’язності $G \Leftrightarrow v \in V_i \cap V_j$ для деяких $i \neq j$.

=> Точки зв’язності поділяють грав на двохзв’язні компоненти.

Запропоновано ряд алгоритмів для пошуку точок зв’язності, і хоча подальше дослідження не пов’язане виключно з точками зв’язності, оцінимо, принаймні, теоретичну можливість відшукання таких вузлів в графі.

Один з простих алгоритмів знаходження точок зв’язності базується на методі пошуку в глибину. Якщо алгоритм не знаходить відповідних точок - то граф буде двохзв’язним. Тобто алгоритм можна розцінювати і як критерій визначення двохзв’язності.

Алгоритм можна описати наступним чином:

1. Виконується обхід графа в глибину, при цьому для всіх вершин v фіксується значення глибинної нумерації dfnumber [v] введених автором Ахо [88], що по суті ці числа фіксують послідовність обходу вершин в прямому порядку глибинного остовного дерева

2. Для кожної вершини фіксується число low[v], що відповідає мінімуму чисел dfnumber нащадків вершини v, включно з самою вершиною і предків w вершини v, для яких існує зв’язок (x,w). Відповідно low[v] визначається як мінімум чисел:

а) $NV[v]$ значення в початковому вузлі

б) $LOW[x]$ всіх нащадків x вершини v;

в) $NV[w]$, вершин предків вершини v, для яких існує ребро (v,w)

3. Точки зв’язності визначаються наступним чином:

а) v - корінь і має більше 1 нащадка (піддерева пов'язані тільки через v).

б) v - не корінь і для деякого його нащадка x немає зворотних ребер, що з'єднують x і\або його нащадків з предками v.

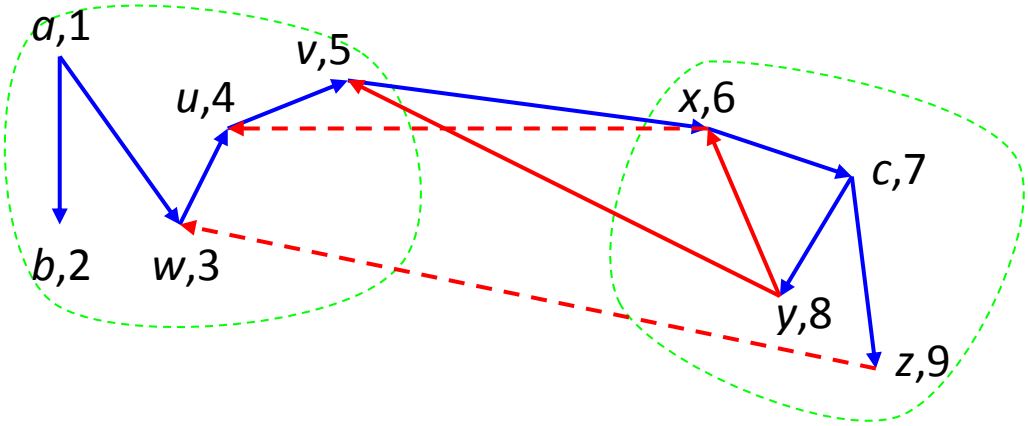


Рисунок 4.20 – Розбиття графа точкою зв’язності

Нехай при пошуку в глибину вершин присвоєна нова нумерація в порядку їх обходу. Тоді, якщо x - нащадок v, (x,w)- зворотне ребро і $NV[w] < NV[v]$, то w - предок v.

Визначимо функцію «нижньої оцінки»:

$$LOW[v] = \min(NV[v], NV[w], LOW[x])$$

$\exists$ зворотне ребро (x,w), де x - нащадок v (або $x = v$), а w - предок v (не «батько» (найближчий предок) при $x = v$, тому що (x,w) - зворотне ребро).

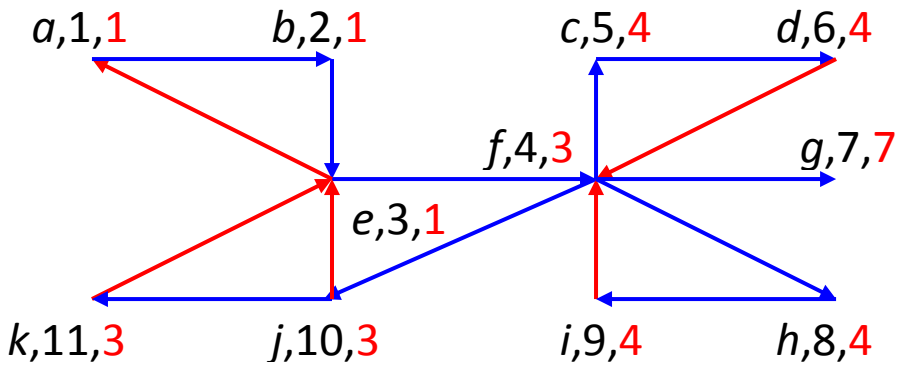


Рисунок 4.21 – Приклад отримання глибинних оцінок

(на рисунку значення NV - чорні, LOW - червоні).

З точки зору СМ і моделі, що розглядається в роботі, точка зв'язності це вузол-міст, який пов'язує різні кластери (окремі групи, спільноти). Зрозуміло, що у випадку незалученності подібного вузла до ідеї втрачається (з точки зору впливу) ціла підмножина вузлів, бо зв'язок з даною підмножиною існує лише через вузол-міст.

Цей приклад яскраво ілюструє важливість структурного положення вузла в процесі інформаційного впливу. З огляду на це варто розглянути й провести експерименти з поведінковими стратегіями орієнтованими на атаку конкретного вузла.

Набір цільових вузлів не обмежується лише критеріями зв'язності, в кожному конкретному випадку, в якості цільового вузла можуть розглядатись різні варіанти. Наприклад, наперед відомо, що деякий вузол є лідером групи, однозначно такий вузол повинен першочергово потрапляти в множину цільових вузлів атаки. Залучення такого вузла до ідеї і перетворення його в генератора ідеї матиме суттєвий вплив на динаміку розповсюдження й кінцевий результат.

Дослідження не ставить за мету розробку методів визначення значущого вузла, вважаємо, що генератор має інформацію про певний вузол і його важливість наперед визначена. В ході дослідження на моделі спробуємо, експериментальним шляхом, встановити можливі шляхи до визначеного вузла та їх ефективність на процес інформаційного впливу в цілому.

Доречним представляється знаходження найкоротшого шляху в графі з метою якомога швидшого захоплення важливого вузла та залучення його до агентів впливу. Якщо розглядати мережу суто формально (як граф) то існують декілька відомих алгоритмів пошуку найкоротшого шляху: алгоритм Форда-Белмана, алгоритм Флойда, алгоритм Дейкстри. Всі ці алгоритми переборні з різними оцінками ефективності за функцією O(n). Але їх втілення в реальній мережі може бути досить ускладненим. З одного боку, враховуючи глобалізацію, постійне зростання кількості користувачів мереж та зростання щільності зв'язків – все це фактори, що значно підвищують ймовірність знаходження такого шляху. Тим більш, що мова йде про вузол з особливим структурним положенням, вузол - міст повинен мати зв'язки як мінімум між двома кластерами. З огляду на ці факти ймовірність існування шляху вузлів від генератора до цільового вузла-моста досить висока, при цьому така ж висока ймовірність існування певної множини таких шляхів і, відповідно, серед них знайдеться найкоротший. Але в реальності пошук такого шляху й його використання для інформаційної атаки на цільовий вузол може бути ускладненим, наприклад - наявністю на цьому шляху вузлів-контргенераторів, що взагалі (за умовами моделі, та й в реальній ситуації) унеможливлює використання даного шляху.

З іншого боку, за умови наявності певної множини шляхів, знаходження певної кількості альтернативних шляхів (не найкоротших, але таких, що в кінцевому випадку приводять до цільового вузла) досить ймовірна. Відповідно – метою є вибір одного з субоптимальних шляхів за певним критерієм.

Далі розглянемо експеримент порівняння досягнення цільового вузла різними шляхами та його результати.

Для вибору шляхів встановимо наступні критерії.

Стратегія 1: пошук найкоротшого по кількості вузлів шляху

Стратегія 2: пошук шляху по мінімальній рівно зваженій сумі показників інформаційного спротиву вузлів на шляху. Дана стратегія може бути формально описана наступним чином:

V_t - вузол - ціль атаки;

$W_{ti} = \{V | V_{i1} \to V_{i2} \to V_{i3} \dots \to V_t\}$ – множина вузлів, що утворюють один з можливих альтернативних шляхів до цільового вузла, при цьому винятковою вимогою є належність вузла V_{i1} (початок шляху) до контактних вузлів генератора;

W – множина, що включає всі знайдені альтернативні шляхи W_{ti}, як підмножини.

Тоді за стратегією 2 найбільш перспективним шляхом атаки є така послідовність вузлів, що

$$W_{ti} \in W \mid \frac{\sum_{i=1}^{n} O_{pv_i}}{n} \to min, \tag{4.7}$$

де n – кількість вузлів в альтернативному шляху, що належить до множини всіх можливих шляхів від вузла генератора до цільового вузла атаки, а сума показників рівня інформаційного спротиву найменша в порівнянні з іншими альтернативними шляхами.

Стратегія 3: пошук шляху по максимальній рівно зваженій сумі показників репутації вузлів на шляху.

Раніше в експериментах звертали увагу і на показник репутації вузлів, тому третя стратегія буде опиратись на аналіз даного показника. ЇЇ формальний опис може бути представлено так:

$$W_{ti} \in W \mid \frac{\sum_{i=1}^{n} R_{v_i}}{n} \to max. \tag{4.8}$$

З огляду на раніше зазначені проблеми використання оптимального (найкоротшого) шляху, дану стратегію в експеримент включати не будемо.

Натомість порівняємо ефективності стратегій атаки цільового вузла з раніше розглянутими стратегіями «дерево», «кущ».

Розглянемо сегмент мережі (рис. 4.22). Вузол, позначений на рис. 4.22 як «цільовий» (має порядковий індекс 120), є яскраво вираженим мостом. Навіть візуально можна визначити, що кластери «1» і «2» пов’язані з іншими кластерами лише через даний вузол-міст.

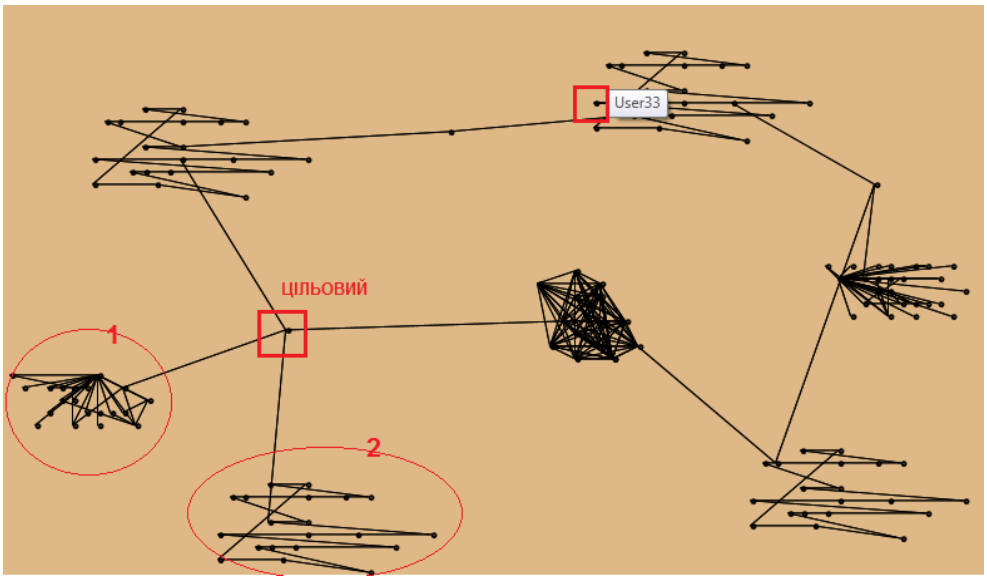


Рисунок 4.22 – Структура сегменту мережі для експериментів

Експеримент 1.

Проведемо експеримент з використанням різних стратегій з наступними передумовами (кількість вузлів 140):

1) Вузол-генератор – вузол з індексом 33;

2) При використанні стратегій атаки на цільовий вузол в якості цільового використовується вузол з індексом 120

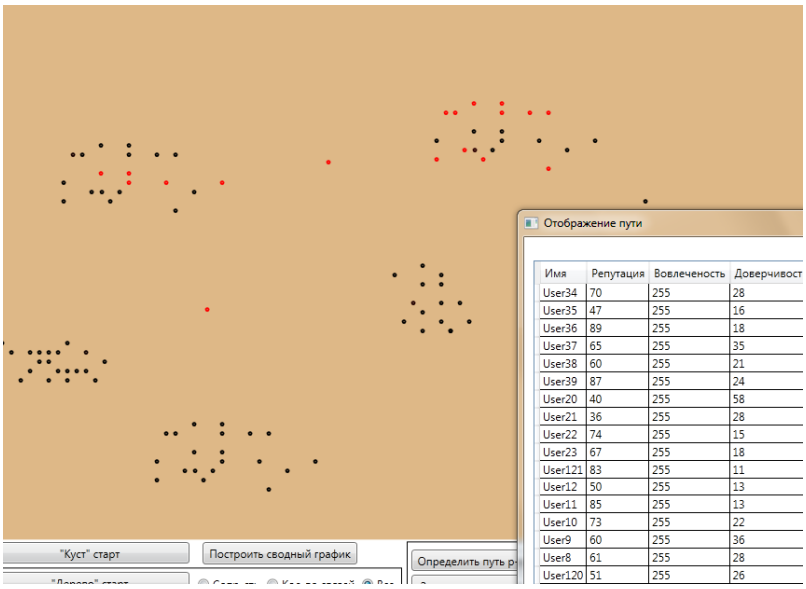


Рисунок 4.23 – Залучення вузлів на шляху до цільового (стратегія атаки на цільовий вузол по мінімальній зваженій сумі інф. спротиву)

Результати проведення декількох серій експерименту (на розглянутому (рис. 4.23) сегменті мережі і інших) занесемо в таблицю, числові показники – кількість вузлів захоплених за 365 ітерацій моделі.

Таблиця 4.4

Результати експериментів атаки на вибраний вузол (Г33_Ц120) в порівнянні з іншими стратегіями

№	Стратегія	Серія 1.1	Серія 1.2	Серія 1.3
1	Атака цільового вузла по мінімальній зваженій сумі інф. спротиву	124	133	137
2	Атака цільового вузла по максимальній зваженій сумі репутації	124	128	120
3	Стратегія «Кущ»	108	98	112
4	Стратегія «Дерево» (кількість зв’язків)	122	122	122

Як видно з таблиці 4.4 поведінкова стратегія атаки на цільовий вузол має мінімальну перевагу над стратегією «Дерево», в середньому перевага склала 1%. При цьому атака на цільовий вузол по шляху з максимальною зваженою сумою репутації в деяких випадках навіть програвала стратегії «Дерево». В порівнянні з стратегією «Кущ» атака на цільовий вузол склала в середньому 15% переваги.

Така несуттєва перевага стратегії атаки на цільовий вузол може бути пояснена двома причинами:

1) Невелика кількість зв’язків в початкового вузла (вузла-генератора) – в проведеному експерименті вузол-генератор (вузол з індексом 33) має всього два зв’язки, саме цим і пояснюється невеликий розрив між результатами отриманими за різними стратегіями. Навіть обираючи вузол випадково (стратегія «Кущ»), існує висока ймовірність (2 вузла – 50%) обрати найефективніший напрямок розповсюдження інформації.

2) Неправильний вибір цільового вузла – даний експеримент показує, що лише структурне положення вузла (вузол-міст) цілком не визначає вартість вузла з точки зору ефективності розповсюдження інформації.

Для підтвердження гіпотез, щодо причин 1)-2) проведемо ще кілька експериментів. В попередньому експерименті одним з вирішальних факторів став фактор низької щільності зв’язків в зоні вузла-генератора, розглянемо варіант сегменту мережі з більшою варіативністю шляхів за рахунок більшої кількості вузлів та вищої щільності зв’язків. Структура сегменту мережі представлено в додатку 2 (рис. 1). Сегмент включає 175 вузлів, в сегменті виділено 7 кластерів: 3 групи, 3 лідерських групи, кліка.

Експеримент 2.

Початкові передумови: вузол-генератор – вузол з індексом 77 (лідер однієї з груп) (див. додаток А3, рис. 2). Цільовий вузол атаки – вузол з індексом 172 (вузол-міст, що пов’язує 5 із семи кластерів сегменту). При виборі таких початкових умов всі стратегії захоплювали всі 175 вузлів але за різну кількість ітерацій, числові дані в таблиці – кількість ітерацій протягом яких захоплено всі вузли

Результати експерименту представлено в таблиці 4.5

Таблиця 4.5

Результати експериментів атаки на вибраний вузол (Г77_Ц172) в порівнянні з іншими стратегіями

№	Стратегія	Серія 2.1	Серія 2.2	Серія 2.3	Середнє
1	Атака цільового вузла по мінімальній зваженій сумі інф. спротиву	144	140	148	144
2	Атака цільового вузла по максимальній зваженій сумі репутації	164	152	168	162
3	Стратегія «Кущ»	344	286	328	319
4	Стратегія «Дерево» (кількість зв'язків)	182	182	182	182
5	Стратегія «Дерево» (спротив)	162	162	162	162

Представимо дані в вигляді діаграми (рис. 4.24). В цьому варіанті вартість цільового вузла виявилась значно вищою, що і призвело до суттєвої переваги стратегії атаки на цільовий вузол в порівнянні з іншими стратегіями. Так в порівнянні з стратегією «кущ» перевага атаки на цільовий вузол по шляху з мінімальною сумою більше 100%, по відношенню до стратегії «Дерево» (по інф. спротиву) - 12%, по відношенню до стратегії «Дерево» (по кількості зв'язків) – 21%.

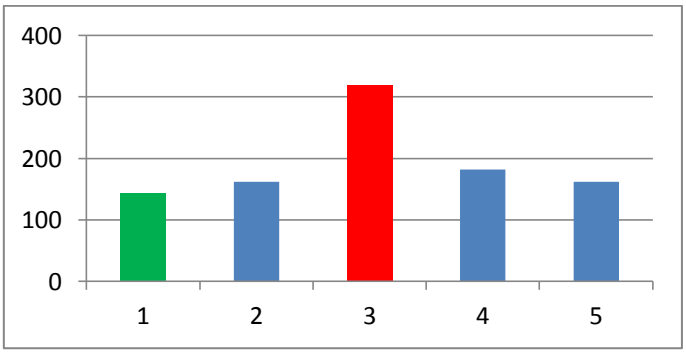


Рисунок 4.24 – Порівняння ефективності стратегій за результатами експерименту №2 (нумерація результатів відповідає табл. 4.5)

Експеримент 3.

Початкові передумови: вузол-генератор – вузол з індексом 150 (один з вузлів групи 3, в розрідженій зоні з високим рівнем інформаційного

спротиву) (див. додаток А3, рис. 2). Цільовий вузол атаки – вузол з індексом 77 (лідер групи ЛідГр1). При виборі таких початкових умов жодна з стратегій не захопила всі 175 вузли (за 365 ітерацій), числові дані в таблиці – кількість захоплених вузлів за 365 іт.

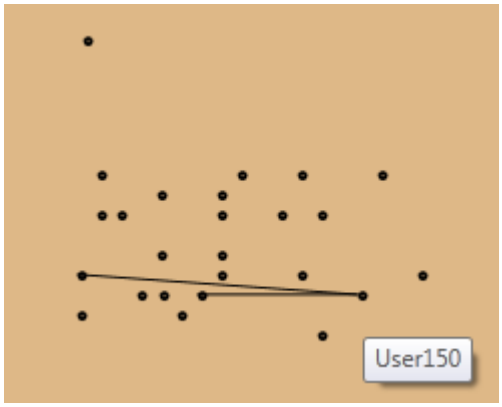


Рисунок 4.25 – Вузол-генератор (передумови експерименту 3)

Результати експерименту представлено в таблиці 4.6

Таблиця 4.6

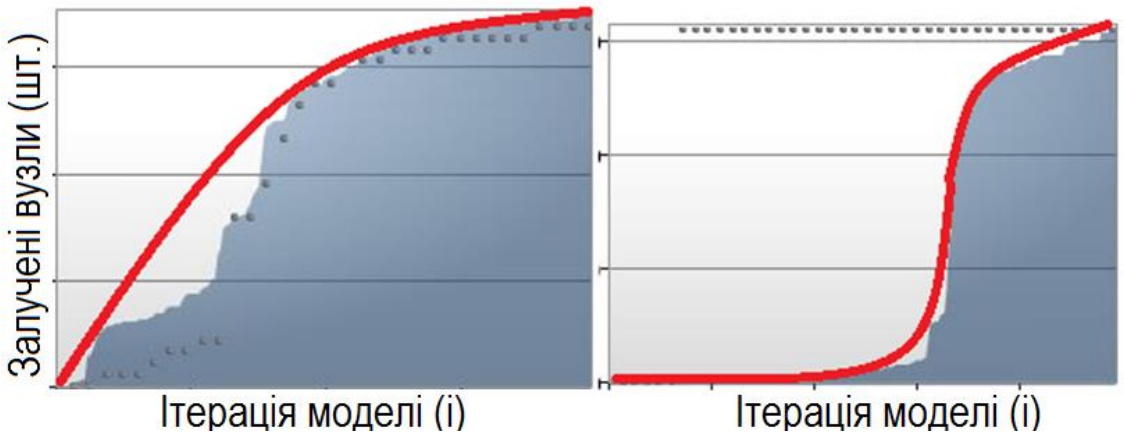
Результати експериментів атаки на вибраний вузол (Г150_Ц150) в порівнянні з іншими стратегіями

№	Стратегія	Серія 3.1	Серія 3.2	Серія 3.3	Середнє
1	Атака цільового вузла по мінімальній зваженій сумі інф. спротиву	172	178	170	174
2	Атака цільового вузла по максимальній зваженій сумі репутації	164	159	168	162
3	Стратегія «Кущ»	154	160	141	152
4	Стратегія «Дерево» (кількість зв’язків)	161	161	161	161
5	Стратегія «Дерево» (спротив)	172	172	172	172

Так як початковий вузол (вузол-генератор) було розміщено в зоні з високим інформаційним спротивом – очікувано найкращі результати показали стратегії, що аналізують показник спротиву. Так за 365 ітерацій моделі стратегія атаки цільового вузла по шляху з мінімальною зваженою сумою спротиву і стратегія «Дерево» (по інф. спротиву) показали дуже

близькі результати, відповідно – 174 і 172 вузли. Найгірші результати показала стратегія «Кущ» (152 вузли), що може бути пояснено особливостями передумов – низька щільність зв’язків і високий рівень спротиву.

Показовим також є аналіз виду графіків, що відображують залежність кількості захоплених вузлів від ітерації моделі. В більшості проведених в роботі експериментів стратегія кущ показувала наступну залежність (рис. 4.26а), стратегії ж з аналізом здебільшого показували наступну залежність (рис. 4.26 б).



а) б)

Рисунок 4.26 – Апроксимація графіків за різними стратегіями

Таку поведінку графіків можна пояснити особливостями стратегій. «Кущ» - стратегія, що не включає жодного аналізу і обирає вузол для атаки випадково, зростання графіка більш рівномірне, етапи більш різкого зростання з’являються тільки при потраплянні активних вузлів в кластери з високою щільністю зв’язків. При таких умовах, а також враховуючи високу активність вузлів при даній стратегії, захоплення вузлів відбувається швидше.

Стратегії з аналізом передбачають вдвічі нижчу активність (див формула 3.3). На початкових ітераціях захоплення вузлів (їх кількість) значно нижча в порівнянні з стратегією «Кущ». Це період залучення важливих, з точки зору стратегії, вузлів. Їх кількість невелика, але коли їх сумарна

вартість добігає певної межі (залежить від структури та характеристик вузлів сегменту) відбувається різкий скачок функції.

В кінцевій фазі спостерігається суттєве зниження швидкості росту. Для стратегії «Кущ» це пояснюється тим, що залишається певна кількість вузлів з невеликою кількістю зв'язків (вузли, що мають 1-2 зв'язки з іншими вузлами), в які досить складно націлити атаку при випадковому виборі цільового вузла. Для стратегій з наявністю аналізу в кінцевій фазі залишаються найбільш несприятливі вузли (наприклад вузли з високим рівнем спротиву). Але стратегія з аналізом має перевагу перед такими вузлами, бо весь накопичений потенціал інформаційної атаки направлено на дані вузли, а стратегія «Кущ» може взагалі оминати вузли, що ще не залучені до ідеї протягом певного часу.

Стратегії «Дерево» показують найкращий рівень стабільності незалежно від початкового положення генератора, стратегія атаки на цільовий вузол суттєво залежить не лише від початкового положення генератора, але й, в першу чергу, від правильності оцінки вартості цільового вузла. Стратегія «Кущ» найбільш нестабільна, але показує досить високі результати при сприятливих умовах (висока щільність зв'язків в зоні генератора, низький рівень інформаційного спротиву).

4.4. Висновки до четвертого розділу

На базі запропонованої у другому розділі математичної моделі розроблено алгоритми програмного імітаційного моделювання процесу поширення інформаційних впливів у сегментах соціальної мережі, а також алгоритми генерації структури сегментів соціальної мережі.

Також, розроблено алгоритми програмного імітаційного моделювання різних поведінкових стратегій суб'єктів інформаційного впливу у соціальній мережі та здійснено порівняння їх ефективності.

Проведено експерименти для порівняння ефективності застосування

різних базових поведінкових стратегій суб'єктами впливу у соціальних мережах під час поширення інформаційних впливів.

Експерименти описані в пункті 4.1 доводять адекватність запропонованої моделі. Модель прогнозовано реагує на зміну параметрів. Результати, отримані в ході експериментів, про критичну кількість залучених вузлів для стрімкого росту кількості прихильників в мережі співпадають з результатами отриманими вченими політехнічного університету Ранселара [7], що проводили дослідження на статистиках отриманих з реальних мереж і отримали результаті на рівні: 10% залучених вузлів визначають інформаційні настрої та прихильність всієї мережі і породжують вирішальні впливи.

В наступних пунктах (п 4.2-4.3) проводились експерименти порівняння результатів швидкості розповсюдження інформації в сегменті при різних початкових умовах (щільність зв'язків, кількість вузлів в мережі з високим рівнем інформаційного спротиву, початкове розміщення генератора) та при використанні різних стратегій.

Стратегії «Дерево» показують найкращий рівень стабільності незалежно від початкового положення генератора, стратегія атаки на цільовий вузол суттєво залежить не лише від початкового положення генератора, але й, в першу чергу, від правильності оцінки вартості цільового вузла – правильного вибору поведінкової стратегі за конкретних умов. Стратегія «Кущ» найбільш нестабільна, але показує досить високі результати при сприятливих умовах (висока щільність зв'язків в зоні генератора, низький рівень інформаційного спротиву). В той же час стратегія «Кущ» найбільш проста з точки зору реалізації, вона не вимагає проведення початкового аналізу мережі та аналізу навколишніх вузлів при виборі цільового вузла для атаки.

Застосування запропонованого методу вибору цільових вузлів суб'єктами інформаційних впливів на основі методу аналізу ієрархій у соціальній мережі під час інформаційних протиборств показало в середньому на 16% кращі результати, ніж вузли обрані випадковим чином серед

виграшних структурних позицій соціальної мережі. Також, було розроблено відповідні практичні рекомендації щодо вибору поведінкових стратегій суб'єктів інформаційного впливу у соціальній мережі під час інформаційних протиборств.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв’язання актуальної та важливої науково-технічної задачі підвищення швидкості розповсюдження інформаційних впливів в сегменті мережі.

У процесі виконання дисертаційної роботи отримані такі наукові та практичні результати:

1. Проаналізовано методи та моделі поширення інформаційних впливів у соціальній мережі в умовах інформаційного протиборства, аналіз дозволив виявити як комбіновані комплексні моделі, що мають підвищити адекватність і відповідність програмного моделювання реальним процесам, так і моделі, орієнтовані на дослідження конкретних характеристик. Аналіз показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла та поведінку суб’єктів при поширенні інформації, стратегію поширення інформації, яку обирає вузол в процесі інформаційних впливів.

2. Вперше розроблено математичну модель поширення інформаційних впливів в сегменті соц. мережі, яка дає можливість застосування різних поведінкових стратегій суб’єктами ІВ на основі аналізу особистісних характеристик вузлів, що обираються для атаки. В ході розробки моделі вперше формалізовано поняття «поведінкова стратегія» та запропоновано приклади базових поведінкових стратегій суб’єктів інформаційних впливів у соціальних мережах, що дозволяють ефективно моделювати різні підходи до вибору цільових вузлів суб’єктами інформаційного впливу.

3. Удосконалено метод генерації структури сегменту соціальної мережі, що дозволяє обирати кількість і типи кластерів сегменту соціальної мережі. Запропонований підхід дає можливість генерувати сегменти мереж з наперед заданою структурою зв’язків та наявними сталими підмножинами вузлів (групи, лідерські групи, кліки)

4. Набув подальшого розвитку метод оптимального вибору цільового вузла для атаки в ході поширення впливів суб'єктом мережі на основі методу аналізу ієрархій та застосування поведінкових стратегій на основі наявних даних про мережу під час інформаційних протиборств. Застосування поведінкових стратегій суб'єктів інформаційних впливів на основі аналізу даних про мережу дозволяє підвищити швидкість поширення інформації в середньому на 70% в порівнянні з випадковим вибором вузлів для атаки. Вибір оптимального цільового вузла дозволяє за меншу кількість часу поширити ІВ серед вузлів сегменту мережі. Швидкість поширення ІВ через вузли, обрані за запропонованим методом, в експериментах на моделі, в середньому на 16% вища, ніж швидкість через вузли, обрані випадковим чином серед виграшних структурних позицій СМ. В порівнянні з запропонованим іншими авторами методом поширення ІВ через «лідера думок» приріст швидкості поширення ІВ через вузол вибраний по методу MAI склав 6%.

5. Проведене експериментальне дослідження програмної моделі підтверджує адекватність застосування запропонованих методів з точки зору підвищенні швидкості поширення ІВ.

Результати дисертації впроваджені і використовуються у діяльності ТОВ «Сайфер БІС» та ЦНТУ, що підтверджено відповідними актами впровадження.

СПИСОК ЛІТЕРАТУРИ

1. Вебер К.С. Сравнительный анализ социальных сетей / К.С. Вебер, А.А. Пименова // Вестник Тамбовского университета. Серия: естественные и технические науки. – 2014. – № 2 (19). – С. 634 – 636.

2. Пелещишин А.М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія / А. М. Пелещишин, Ю.О. Сєров, О.Л. Березко, О.П. Пелещишин, О.Ю. Тимовчак-Максимець, О.В. Марковець; за заг. ред. А.М. Пелещишина. – Львів: Видавництво Львівської політехніки, 2012. – 368 с.

3. Сєров Ю.О. Аналіз комунікативних процесів у Веб-спільнотах середовища Веб 2.0 / Ю.О. Сєров, А.М. Пелещишин, К.О. Слобода // Східно-Європейський журнал передових технологій. – 2009. – № 1/2 (37). – С. 38 – 41.

4. Адаськов О.І. Рекомендації щодо проведення інформаційних заходів в мережі Інтернет в інтересах виконання завдань інформаційно-психологічних операцій / О.І. Адаськов // збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2014. – Вип. 45. – С. 57 – 67.

5. Муратова Н.Ф. Интернет-СМИ как отдельный вид в системе средств массовой информации: лексическое и этимологическое обозначения понятия // Филологические науки. Вопросы теории и практики, – № 2 (6). – С. 118-120.

6. Панченко Е. Интеграция Интернет-СМИ и социальных сетей в Рунете: Новая публичная сфера или пространство контроля? / Е. Панченко // Digital Icons: Studies in Russian, Eurasian and Central European New Media – 2011. – № 5. – С. 87 – 118.

7. Смирнов А.И. Глобальная безопасность в цифровую эпоху: стратагемы для России / А.И. Смирнов, В.Р. Григорьев, И.Н. Кохтюлин, Б.В. Куроедов, О.В. Сандаров. – М. : ВНИИ геосистем, 2014. – 394 с.

8. Пирцхалава Л.Г., Хорошко В.А., Хохлачева Ю.Е. Шелекст М.Е. Информационное противоборство в современных условиях: [Монография] / Под редакцией профессора В.А. Хорошко. – К.: ЦП «Коммпринт», 2019. – 226 с.

9. Мелешко Є.В., Константинова Л.В., Улічев О.С. Дослідження властивостей інформації та методів її поширення з точки зору інформаційної безпеки в соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 3(35). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2015. – С. 98-106.

10. Улічев О.С. Дослідження моделей розповсюдження інформації та інформаційних впливів в соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 4(50). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2018. – С. 147-151.

11. Улічев О.С. Математична модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. - Кропивницький: ЦНТУ, 2018. - Вип. 31. - С. 165-174.

12. Улічев О.С., Мелешко Є.В. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах // Збірник наукових праць " Сучасні інформаційні системи". Випуск 2(2). – Харків: ХПІ. – 2018. – С. 35-39.

13. Ulichev O., Meleshko Ye., Sawicki D., Smailova S. Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors // Proc. SPIE 11176, Wilga, Poland (ISSN: 0277-786X). – 2019. – Number article: 111761T. (SCOPUS).

14. Ulichev O., Meleshko Y., Khokh V. The computer simulation method of a social network structure for the research of dissemination processes of informational influences // Scientific and Practical Cyber Security Journal (SPCSJ) 4(3). – Georgia, Tbilisi, 2019. – P. 34-47.

15. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження робастності рекомендаційних систем з колаборативною фільтрацією до інформаційних атак // Наукове видання Кібербезпека: освіта, наука, техніка.– Київ: КУБГ, 2019. Т.1 № 5. – С. 95-104.

16. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження відомих моделей атак на рекомендаційні системи з колаборативною фільтрацією // Збірник наукових праць Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – №. 5 (57). – С. 67-71.

17. Ulichev O., Meleshko Y., Smirnov O., Khokh V. The method of choosing objects for informational influence in social networks during information campaign based on the analytic hierarchy process // 1st International workshop on cyber hygiene & conflict management in global information networks, National Aviation University, Kyiv, Ukraine, 2019 (SCOPUS). [прийнято до публікації]

18. Улічев О.С. Генерування моделі соціальної мережі для дослідження впливу її структури на розповсюдження інформаційних впливів // Збірник тез II Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». м. Кропивницький. 20-22 квітня 2017 р. – Кропивницький: ЦНТУ. – 2017. – С. 103-104.

19. Улічев О.С., Мелешко Є.В. Програмна модель соціальної мережі та стратегій поширення інформаційно-психологічних впливів // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». м. Кропивницький. 19-20 квітня 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 136-220.

20. Улічев О.С., Мелешко Є.В. Математична модель розповсюдження інформації в сегменті соціальної мережі // Матеріали Двадцятого Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 13-14 квітня 2018 року. – Кропивницький: КЛА НАУ. – 2018. – С. 68-72.

21. Улічев О.С., Мелешко Є.В. Програмна модель розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Збірник

тез VIII Міжнародної науково-технічної конференції «ITSEC», м. Київ, 16-18 травня 2018 року. – Київ: НАУ. – 2018. – С. 34-35.

22. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез Сьомої міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 17-19 травня 2018 р. – Львів: Національний університет "Львівська політехніка". – 2018. – С. 29-30.

23. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Збірник тез X Всеукраїнської науково-практичної конференції «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем(SITS'2018)»,21-23 червня 2018 року. – Миколаїв-Коблево: НАУ та МІПРО. – 2018. – С. 77–79.

24. Мелешко Є.В., Шингалов Д.В., Улічев О.С. Дослідження Баєсових мереж довіри як засобів для моделювання динамічних процесів у складних мережах // Збірник тез XVII Міжнародної науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем», 20-22 листопада 2019 року. – Дніпро: ДНУ. – 2019. – С. 284-285.

25. Мелешко Є.В., Хох В.Д., Улічев О.С. Методи тестування робастності рекомендаційних систем з колаборативною фільтрацією // Всеукраїнська науково-практична Інтернет-конференція «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» 13-14 листопада 2019 р. – м. Кропивницький: ЦНТУ. – 2019. С. 88-89.

26. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження методів підвищення робастності рекомендаційних систем до інформаційних атак // Матеріали VI Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», 19 – 22 лютого 2020 р. – м. Київ: Вид-во Європейського університету, 2020. – С. 65-70

27. List of virtual communities with more than 100 million active users [Electronic resourse]. – Mode of access: http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users. – Title from the screen.

28. Висоцька В.А. Моделювання етапів життєвого циклу комерційного web-контенту / В.А. Висоцька, Л.Б. Чирун, Л.В. Чирун // Вісник Національного університету "Львівська політехніка". – 2011. – № 715 : Інформаційні системи та мережі. – С. 69 – 87.

29. Орлов А.Ю. Организация виртуального сообщества в сети Интернет/А.Ю. Орлов // Информационные технологии. – 2008. – № 8. – С. 15 – 19.

30. Пелещишин А.М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія / А.М. Пелещишин, Ю.О. Сєров, О.Л. Березко, О.П. Пелещишин, О.Ю. Тимовчак-Максимець, О.В. Марковець; за заг. ред. А. М. Пелещишина. – Львів: Видавництво Львівської політехніки, 2012. – 368 с.

31. Почепцов Г. Контроль над разумом / Г. Почепцов. – К: ВД Києво-Могилянська академія, 2012. – 350 с.

32. Ридель В.В. Компьютерное моделирование // Методические указания учебной дисциплины, Москва, 2017

33. Закон України «Про інформацію» від 2 жовтня 1992 р.: із змінами, внесеними Законом України від 2 грудня 2010 р. : за станом на 1 березня 2015 р. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12/ed20110113. – Назва з екрану.

34. Конституція України : прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. із змінами, внесеними Законом України від 21 лютого 2014 р. : за станом на 1 березня 2015 р. / [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к/96-вр. – Назва з екрану.

35. Кримінально-процесуальний кодекс України : за станом на 1 грудня 2005 р. / Верховна Рада України. – Офіц. вид. – К. : Парлам. вид-во, 2006. – 207 с. – (Бібліотека офіційних видань).

36. Хоган Б. (2013) Анализ социальных сетей в Интернете // Интернет-журнал о современной фундаментальной науке Postnauka.ru, URL: https://postnauka.ru/longreads/20259

37. Харари Ф. Теория графов / Ф. Харари. - М.: Мир, 1973. - 300 с.

38. Оре О. Теория графов / О. Оре // - М.: Наука 1980. - 336 с.

39. Erdős P. Graph theory and probability // Canadian Journal of Mathematics. – 1959. – Т. 11. – С. 34-38.

40. Kauai H.I., Freeman L.C. (1979) Centrality in social networks conceptual clarification. Social Networks, 1(3). – С. 215–239.

41. Хайдер Ф. (1958) Психология межличностных отношений. Теория структурного баланса

42. Морено Я.Л. Социометрия: Экспериментальный метод и наука об обществе / Пер. с англ. А. Боковикова, под научной редакцией Золотовицкого Романа Александровича (инициатора издания), — Москва: Академический Проект, 2001, ISBN 5-8291-0110-6

43. Сазанов В.М. Социальные сети как новая общественная сфера.. – М.: Лаборатория СВМ, 2010. – 180 с.

44. Хоган Б. (2013) Анализ социальных сетей в интернете

45. Seidman S.B., & Foster B.L. (1978). A graph-theoretic generalization of the clique concept. Journal of Mathematical Sociology, 6, – С. 139–154.

46. Moody J., White D.R. (2003). Structural cohesion and embeddedness. American Sociological Review, 68(1), – С. 103–128.

47. Wellman B., Hogan B., Berg K. et al. (2006). Connected lives: The project. In P. Purcell (Ed.), The networked neighborhood (P. 161–216).

48. Карпенко О. Украинцы в социальных сетях: масштабное исследование «Яндекса» // Украинский журнал об Интернет-бизнесе Ain.ua,

URL: https://ain.ua/2014/08/21/ukraincy-v-socialnyx-setyax-masshtabnoe-issledovanie-yandeksa/

49. Количество украинских пользователей в Facebook выросло на 1,5 миллиона за две недели // Новостной портал Украины Delo.ua, URL: https://delo.ua/tech/kolichestvo-ukrainskih-polzovatelej-v-facebook-vyroslo-na-15-mi-331422/ © delo.ua

50. Гаркуша Ю.О. Інформаційна безпека сучасного українського суспільства / Ю.О. Гаркуша // Право і суспільство. - 2016. - № 2(2). - С. 133-139.

51. Мирошниченко А. Почему устарели СМИ? Потому что новость нельзя не узнать [Электронный ресурс] / А. Мирошниченко. - 2011. - Режим доступу до ресурсу: www.slon.ru/pochemu_ustarel_smi_potomu_chto_novosti_nelzya_ne_uznat-693227.xhtml

52. Гуменюк Н. Майдан Тахрір. У пошуках втраченої революції / Н. Гуменюк - Київ: Політична критика, - 2015.

53. Бочаров Ю. Киберпреступность и кибертерроризм. Новая глобальная угроза государственному строю. [Электронный ресурс] / Ю. Бочаров. - 2011. - Режим доступу до ресурсу: www.elections-ices.org/russian/publications/textid:12835

54. Спільнота MDK на ВКонтакті заробляє до $1 млн. на рік. [Электронный ресурс]. - 2014. - Режим доступу до ресурсу: http://watcher.com.ua/spilnota-mdk-na-vkontakti-zaroblyae-do-1-mln-na-rik.html

55. Князева Е. Особенности сбора информации в исследованиях социальных сетей [Электронный ресурс] / Е. Князева. - 2014. - Режим доступу до ресурсу: http://www.ffsn.bsu.by/ffsn.files/caf/k-sk/personal-sk/knyazeva/Knyazeva-doc/1_Knyazeva-doc.pdf

56. Гумінський Р. Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет-середовищі соціальних мереж. / Р. Гумінський - Київ: УДК 004.738.5+004.773.2 - 2016.

57. Указ Президента №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»»

58. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти / П. Шевчук Науковий вісник. «Демократичне врядування» – 2014. – Вип. 13

59. ТОП-7 цитат Путина об Украине [Электронный ресурс]. — Режим доступу : http://politiko.ua/blogpost69917.

60. Андреева Г.М. Социальная психология. – М.: Аспект Пресс, 2008. 149 с.

61. Комусевич Х. Многомерная алгоритмика для поиска когезионные подсетей / Х. Комусевич, Институт информатики, Фридрих-Шиллер-Университет Йена, - 2016.

62. Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432 с.

63. Тоискин В. Классификация социальных сетей интернет как элементов социальных структур / В. С. Тоискин, В. В. Красильников, "Заочные электронные конференции" - 2010, [Електронний ресурс]. – Режим доступу: www.econf.rae.ru/pdf/2012/10/1688.pdf.

64. Бергер Й. Заразливий. Психологія вірусного маркетингу / Пер. з англ. Олени Замойської. – К.: Наш Формат, 2015. – 224 с.;

65. Соловей В.Д. Абсолютное оружие. Основы психологической войны и медиаманипулирования / В.Д. Соловей. – Москва: Издательство "Э", 2015. – 320 с.;

66. Лайнбарджер П.М.Э. Психологическая Война. Теория и практика обработки массового сознания / Пер. с англ. Ламановой. – М.: ЗАО Центрполиграф, 2014. – 445 с.

67. Колодин Д.В. Информационное влияние в социальных сетях в виртуальной реальности // Вестник Челябинского государственного университета. 2014. № 11 (340). Вып. 32. С. 59–63.

68. Зиммель, Г.К теории познания социальной науки // Социология : хрестоматия для вузов. 2-е изд. М. : Академ. Проект, 2004. С. 20–32.

69. Deutsch, M.A. Study of Normative and Information Social Inuences upon Individual Judgment / M. Deutsch, H. B. Gerard // Journ. of Abnormal and Social Psychology. 1955. № 51;

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

71. Батура Т.В. Методы анализа компьютерных социальных сетей // Вестник НГУ. – 2012. – Т. 10. – Вып. 4. – С. 13–28. URL: http://lib.nsu.ru:8080/jspui/bitstream/nsu/250/1/02.pdf (дата звернення: 21.08.17).

72. Воронкин А.С. Практические основы аналитического исследования персональной учебной среды в открытом онлайн курсе // Образовательные технологии и общество (Educational Technology & Society). – 2013. – Т. 16. – № 4..

73. Davern M. Social Networks and Economic Sociology: A Proposed Research Agenda for a More Complete Social Science // American Journal of Economics & Sociology. 1997. Vol. 56. Is. 3. P. 287–302.

74. Морено Я.Л. Социометрия: Экспериментальный метод и наука об обществе. – М.: Академический Проект, 2004. – 320 с.

75. Фісенко Т. Дослідження соціальних Інтернет-мереж у працях зарубіжних вчених у 1930-2000 рр.: комунікативний вимір // Проблеми та перспективи розвитку науки на початку третього тисячоліття у країнах СНД: матеріали І Міжнародної науково-практичної інтернет-конференції (Переяслав-Хмельницький, 26-28 лютого 2012 р.). – Переяслав-Хмельницький, 2012. – С. 260–262.

76. Barnes J.A. Class and committees in a Norwegian Island Parish // Human Relations. – 1954. V. 7. – P. 39–58. URL: http://pierremerckle.fr/wp-content/uploads/2012/03/Barnes.pdf (дата звернення 21.08.2017).

77. Erdos P., Renyi A. On the evolution of random graphs // Publ. Math. Inst. Hungar. Acad. Sci. – 1960. V. 5. – P. 17–61.

78. Батура Т.В. Модели и методы анализа компьютерных социальных сетей//Программные продукты и системы 2013. № 3 С. 130-137.

79. Kermack W.O., McKendrick A.G. A Contribution to the Mathematical Theory of Epidemics // Proc. of the Royal Society A: Mathematical, Physical and Engineering Sciences. 1927. No. 115 (772). 700 p. DOI:10.1098/rspa.1927.0118. JSTOR 94815.

80. Горковенко Д.К. Сравнительный анализ моделей эпидемии и клеточного автомата при моделировании распространения информации в социальных сетях // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2017. Т. 10. № 3. С. 103–113. DOI: 10.18721/JCSTCS.10309

81. Kempe D., Kleinberg J., Tardos E. Maximizing the Spread of Influence through a Social Network / Proceedings of the 9-th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. - 2003. - p. 137-146.

82. Ландэ Д.В., Грайворонская А.Н., Березин Б.А. Мультиагентная модель распостранения информации в социальной сети// Системи збереження та масового розповсюдження даних: Реєстрація, зберігання і обробка даних, 2016, Т.18, №1

83. Чураков А.Н. Анализ социальных сетей // Социологические исследования. 2001. № 1. С. 109–121.

84. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели информационного влияния и информационного управления в социальных сетях // Проблемы управления. 2009.

85. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели репутации и информационного управления в социальных сетях // Управление большими системами. 2009.

86. Чхартишвили А.Г. Теоретико-игровые модели информационного управления. – М.: ПМСОФТ, 2005.

87. Динаміка рейтингів політичних партій // Київський міжнародний інститут соціології, URL: http://kiis.com.ua

88. Ахо А.В., Хопкрофт Д.Э., Ульман Д.Д. Структуры данных и алгоритмы.: Пер. с англ. : Уч. пособие. – М.: Издательский дом «Вильямс», 2007. – 400 с.

89. Сакман Г. Решение задач в системе человек — ЭВМ. — М.: Мир, 1973.—351 с.

90. Андрейчиков А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике — М.: Финансы и статистика, 2000. — 368 с.: ил. ISBN 5-279-02188-1.

91. Саати Т., Кернс К. Аналитическое планирование. Организация систем: Пер. с англ. – М.: Радио и связь, 1991. – 224 с.

92. Саати Т. Принятие решений. Метод анализа иерархий /Т. Саати. – М. : Радио и связь, 1993. – 278 с.

93. Теория принятия решений. Учебно-методическое пособие для студентов ЗГИА всех специальностей / Матузко Ю.О. – Запорожье: ЗГИА, 2009. – 70 с.

94. Губанов Д.А., Калашников А.О., Новиков Д.А. Теоретико-игровые моделии нформационного противоборства в социальных сетях // Управление большими системами. Выпуск 31, - М.: Институт проблем управления им. В.А. Трапезникова Российской академии наук, 2011

95. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели репутации и информационного управления в социальных сетях // Математическая теория игр и ее приложения. 2009. Том 1. Выпуск 2. С. 14-37.

96. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства.– М.: Издательство физико-математической литературы, 2010.

97. Евсеев А. Ю., Лабуш Н. С., Пую А. С. Информационные технологии и терроризм: теория и современная практика. СПб: Роза мира, 2005.

98. Грищук Р.В., Мамарєв В.М., Молодецька-Гринчук К.В. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблогу Twitter) [Текст] / Р. В. Грищук, В. М. Мамарєв, К. В. Молодецька-Гринчук // Інформаційні технології та комп'ютерна інженерія. – 2017. – № 2. – С. 12-19.

99. Додонов А.Г., Ландэ Д.В. Живучесть информационных систем. – К.: Наук. думка, 2011. – 256 с.

100. Расторгуев С. П. Информационная война / С. П. Ра- сторгуев. – М. : Радио и связь, 1999 – 416 с.

101. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

102. Erdös P., Rényi A. On the evolution of random graphs // Magyar Tudományos Akademia Matematikai Kutato Intezetenek Közlemenyei [Publications of the Mathematical Institute of the Hungarian Academy of Sciences]. — 1960. — Т. 5.

103. Watts D.J.; Strogatz, S. H. (1998). «Collective dynamics of “small-world” networks» (PDF). Nature. 393 (6684): 440–442. Bibcode:1998Natur.393..440W. doi:10.1038/30918. PMID 9623998.

104. Barab´asi L.-A., Albert R., Jeong H. Scale-free characteristics of random networks: the topology of the world-wide web. Physica, A281, 69–77, 2000.

105. Bollobás B., Riordan O. Mathematical results on scale-free random graphs // Handbook of graphs and networks. Weinheim: Wiley-VCH, 2003. P. 1-34.

106. Buckley P.G., Osthus D. Popularity based random graph models leading to a scale-free degree sequence. Discrete Mathematics, 282:53–63, 2004.

107. Bollobás B., Borgs C., Chayes T., Riordan O.M. Directed scale-free graphs. ProceedingSODA '03 Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms, P. 132–139, 2003.

108. Берновски М.М., Кузюрин Н.Н. Случайные графы, модели и генераторы безмасштабных графов// М.М. Берновски, Н.Н. Кузюрин, Труды Института системного программирования РАН, текст научной статьи по специальности «Математика», - 2012

109. Райгородский А.М. Модели случайных графов и их применение // Труды МФТИ. – 010. –Т. 2, №4. – С. 130-140.

110. Granovetter M.S. Threshold Models of Collective Behavior // The American Journal of Sociology. 1978. Vol. 83, No. 6. P. 1420-1443

111. John Von Neumann J., Burks A.W. Theory of Self-Reproducing Automata. University of Illinois Press, Urbana and London, 1966

112. Торопов Б.А. Модель независимых каскадов распространения репоста в онлайновой социальной сети // Кибернетика и программирование. – 2016. – № 5. – С. 199 - 205. DOI: 10.7256/2306-4196.2016.5.20624 URL: https://nbpublish.com/library_read_article.php?id=20624

113. Schiff J. L. Cellular Automata: A Discrete View of the World.—New York: Wiley, 2007.

114. John Von Neumann J., Burks A.W. Theory of Self-Reproducing Automata. University of Illinois Press, Urbana and London, 1966

115. Гончаров И. В., Паринов П. А., Сирота П. А. Моделирование процессов информационно-психологического воздействия в социальных сетяхвестник // ВГУ, серия: Системный анализ и информационные технологии, 2018, № 2. – С. 93-104.

Додаток А. Акти впровадження дисертаційних досліджень

САЙФЕР
Системи захисту інформації

ТОВ «САЙФЕР ПРО»
ЄДРПОУ 42125815
Адреса: 04107, м. Київ, вул. Нагірна, 25-27
Тел./Факс: (044) 484-46-17, 484-46-12
E-mail: info@cipher.com.ua
http://www.cipher.com.ua

№ 48/19 від «14» листопада 2019 р.

АКТ
про впровадження результатів дисертаційної роботи
Улічева Олександра Сергійовича
«Модель та методи розповсюдження інформаційних впливів у соціальних мережах в умовах інформаційного протиборства»
на здобуття наукового ступеня кандидат технічних наук

Комісія у складі голови – директора товариства з обмеженою відповідальністю «САЙФЕР ПРО», Охріменко А.О., членів комісії – керівника проектів кандидата технічних наук Боровікова О.М., провідного розробника Бойко С.Т., склала цей акт про те, що у діяльності ТОВ «САЙФЕР ПРО» реалізовано наступний результат наукових досліджень Улічева О.С.:

Здобувачем було удосконалено метод генерації структури сегменту соціальної мережі, що за рахунок комбінування структури соціальної мережі з набору параметризованих кластерів і вибору їх структурних особливостей, дозволяє генерувати мережі з наперед заданою топологією і структурними особливостями. Удосконалено метод програмного імітаційного моделювання поширення інформаційних впливів у соціальній мережі, який за рахунок застосування запропонованої математичної моделі поширення інформаційних впливів в сегменті соціальної мережі дає можливість моделювати різні поведінкові стратегії суб'єктів інформаційного впливу.

Програмна реалізація алгоритму побудованого на основі удосконаленого методу генерації структури сегменту соціальної мережі у модулі оцінки ризиків за банківськими операціями системи дистанційного управління банківськими рахунками через мережу Інтернет «ELPay»

Результати дослідження, отримані Улічевим О.С., дали можливість оцінки доцільності впровадження складних поведінкових моделей агентів, в залежності від характеристик і показників конкретного сегменту соціальної мережі, що, в кінцевому результаті, сприяло підвищити точність прийняття рішень на надання кредитів.

Голова комісії
Директор ТОВ «САЙФЕР ПРО» А.О. Охріменко

Члени комісії:
Керівник проектів к.т.н. О.М. Боровіков

Провідний розробник С.Т. Бойко

ЗАТВЕРДЖУЮ:
Проректор з наукової роботи
Центральноукраїнського національного
технічного університету
_____ О.М. Левченко
«20» квітня 2020 р.

АКТ
про впровадження результатів дисертаційної роботи
Улічева Олександра Сергійовича
у Центральноукраїнському національному технічному університеті
"МОДЕЛЬ ТА МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА"
на здобуття наукового ступеня кандидат технічних наук

Основні результати наукових досліджень Улічева Олександра Сергійовича, одержані під час виконання дисертаційної роботи на здобуття наукового ступеня кандидата технічних наук, апробовані та впроваджені у науково-дослідних роботах кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету. Також результати одержані у його дисертаційній роботі використані у навчальному процесі при викладанні дисциплін "Інформаційна безпека держави", "Спеціальні розділи математики для інформаційної безпеки" та "Прогнозування та моделювання в соціальній сфері". Зокрема, в навчальному процесі кафедри використано наступні результати наукових досліджень:

1. Математична модель поширення інформаційних впливів у сегменті соціальної мережі, яка за рахунок параметризації особистісних характеристик вузлів мережі, а саме – введення параметрів вузла: активність, репутація, залученість до ідеї, інформаційний спротив, дає можливість застосування різних поведінкових стратегій суб'єктами інформаційного впливу на основі аналізу параметрів атакованих вузлів;
2. Метод генерації структури сегменту соціальної мережі, який за рахунок комбінування структури мережі з набору параметризованих кластерів і вибору їх топологічних особливостей, дозволяє генерувати мережу з наперед заданою структурою;
3. Програмна модель для моделювання динаміки розповсюдження інформації в сегменті мережі з різними показниками та структурними особливостями

Застосування результатів дисертаційних досліджень Улічева Олександра Сергійовича дозволило підвищити рівень засвоєння навчального матеріалу за рахунок можливості візуалізації процесів розповсюдження інформації та інформаційних впливів.

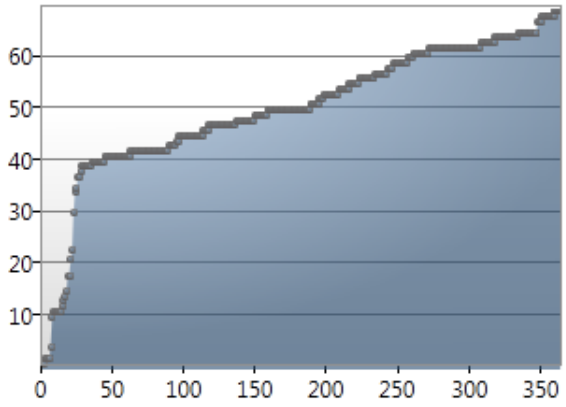
Голова комісії
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного
технічного університету
доктор технічних наук, професор О.А. Смірнов

Члени комісії:
доцент кафедри кібербезпеки та програмного забезпечення
кандидат технічних наук О.М. Дрєєв

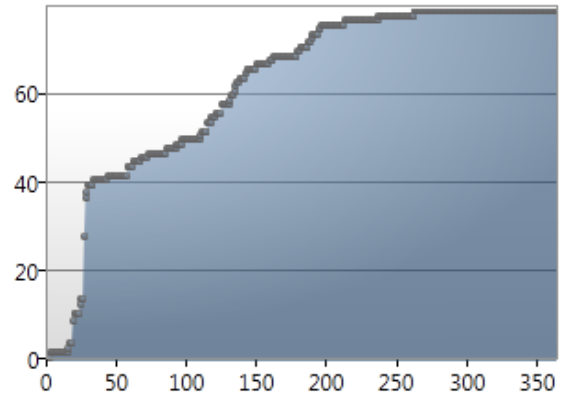
доцент кафедри кібербезпеки та програмного забезпечення
кандидат технічних наук, доцент В.В. Босько

Додаток Б. Діаграми залучення вузлів соціальної мережі при використанні різних стратегій поширення інформаційних впливів

Залучення вузлів з використанням різних стратегій (а)-«кущ», б)-«дерево») в сегменті з низькою щільністю зв’язків

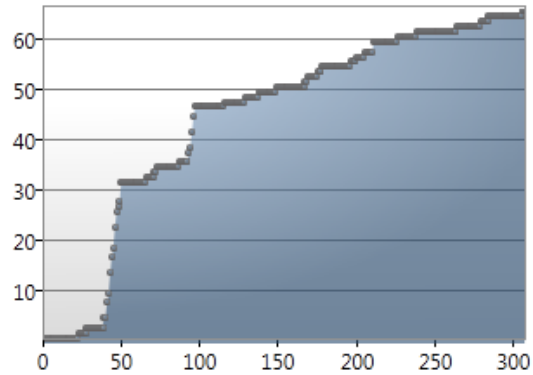


а) Залучено вузлів - 67

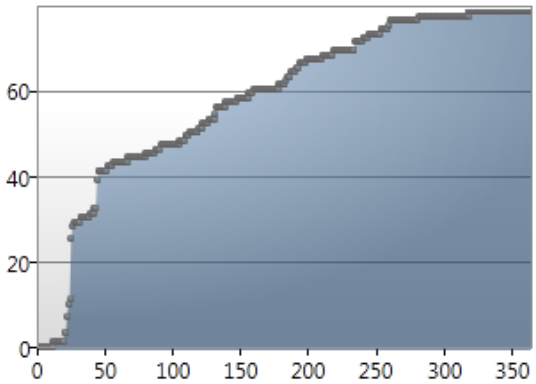


б) Залучено вузлів - 80

Рисунок Б.1 - Експеримент 1

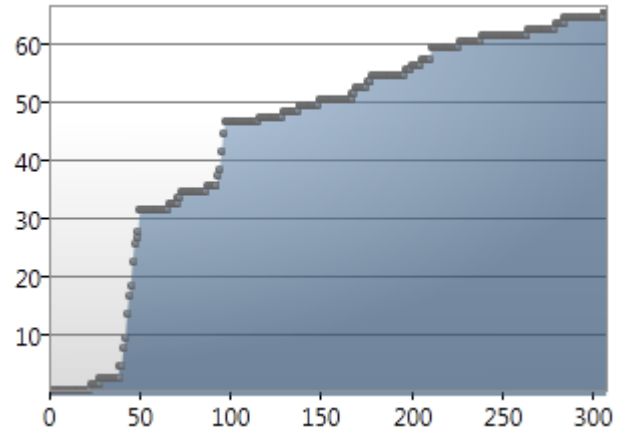


а) Залучено вузлів - 65

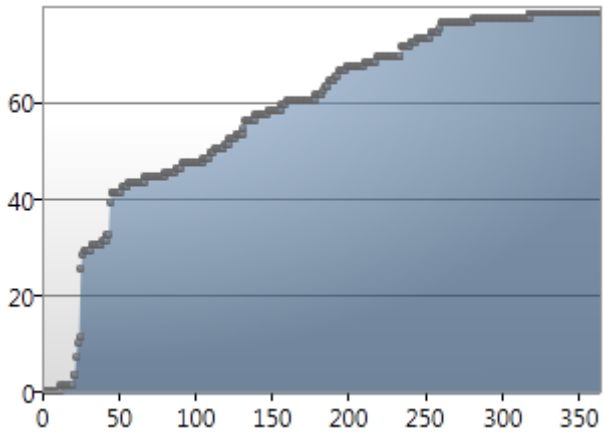


б) Залучено вузлів - 80

Рисунок Б.2 - Експеримент 2



а) Залучено вузлів - 64

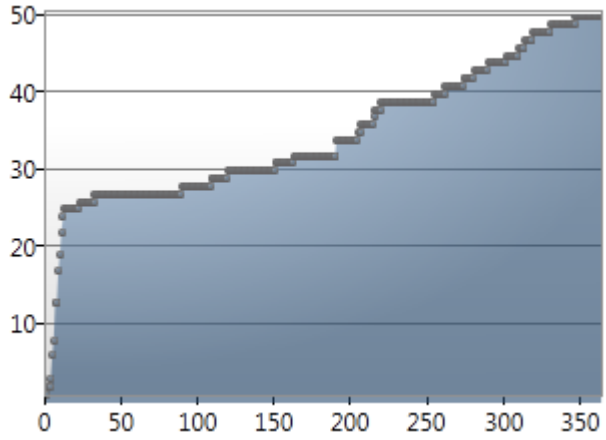


б) Залучено вузлів - 80

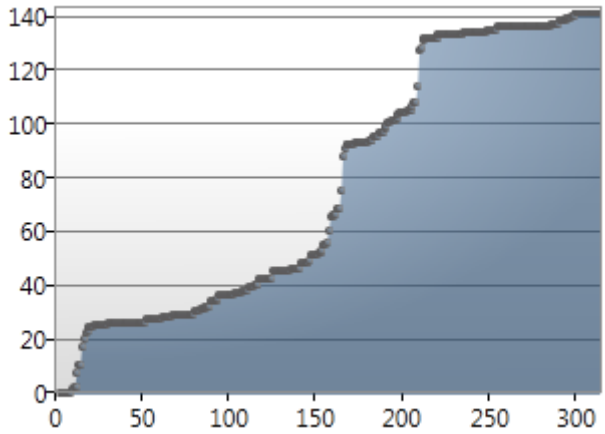
Рисунок Б.3 - Експеримент 3

Продовження додатку Б

Залучення вузлів в сегменті з високим рівнем інформаційного стпротиву з використанням різних стратегій (а)-«кущ», б)-«дерево») в сегменті з низькою щільністю зв’язків

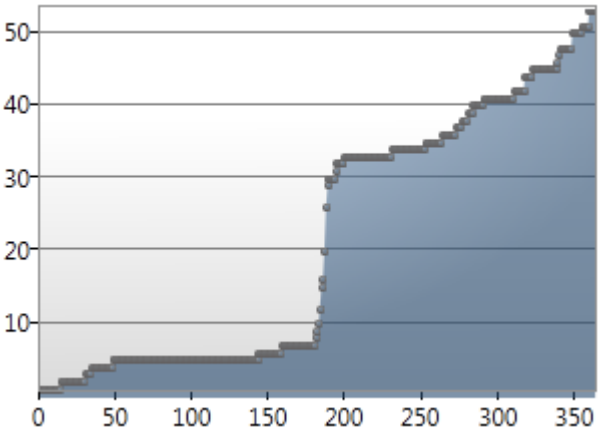


а) Залучено вузлів - 50

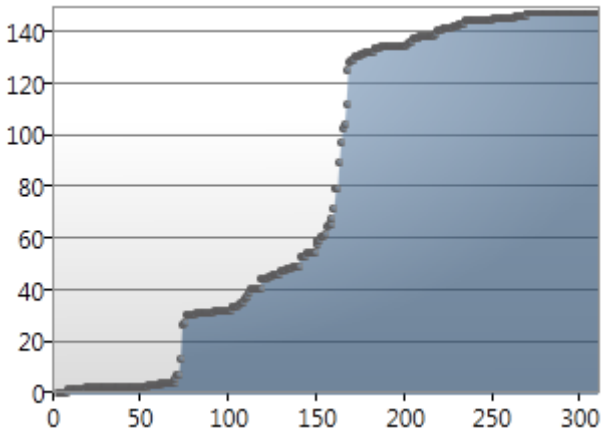


б) Залучено вузлів - 142

Рисунок Б.4 - Експеримент 1



а) Залучено вузлів - 53



б) Залучено вузлів - 142

Рисунок Б.5 - Експеримент 2

Додаток В. Приклади моделювання структури соціальних мереж у програмній імітаційній моделі

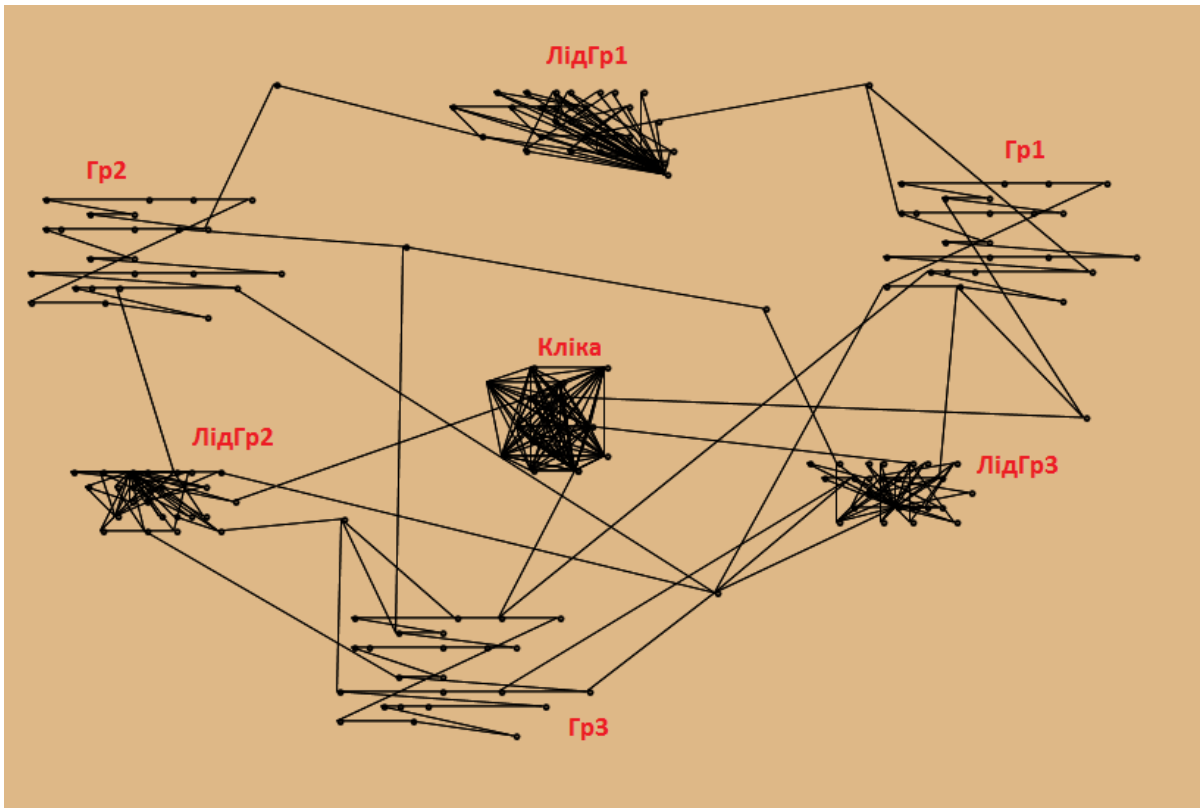


Рисунок В.1 – Модеювання мережі з набору кластерів

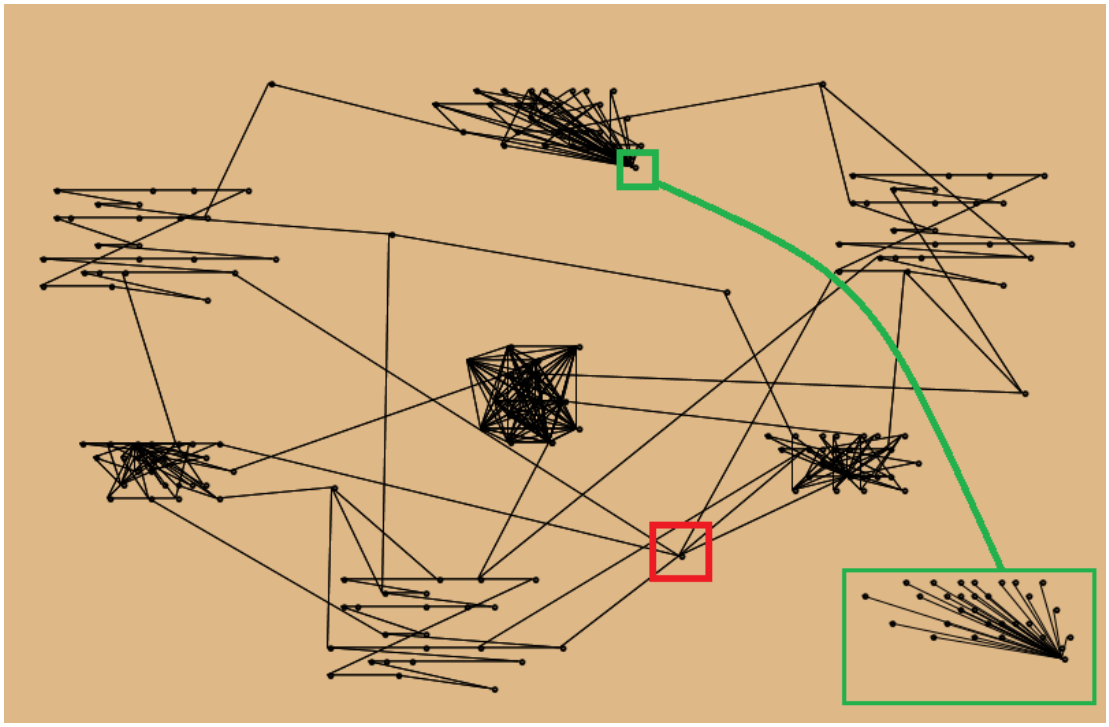


Рисунок В.2 – Вибір початкових вузлів розповсюдження ІВ

Продовження додатку В

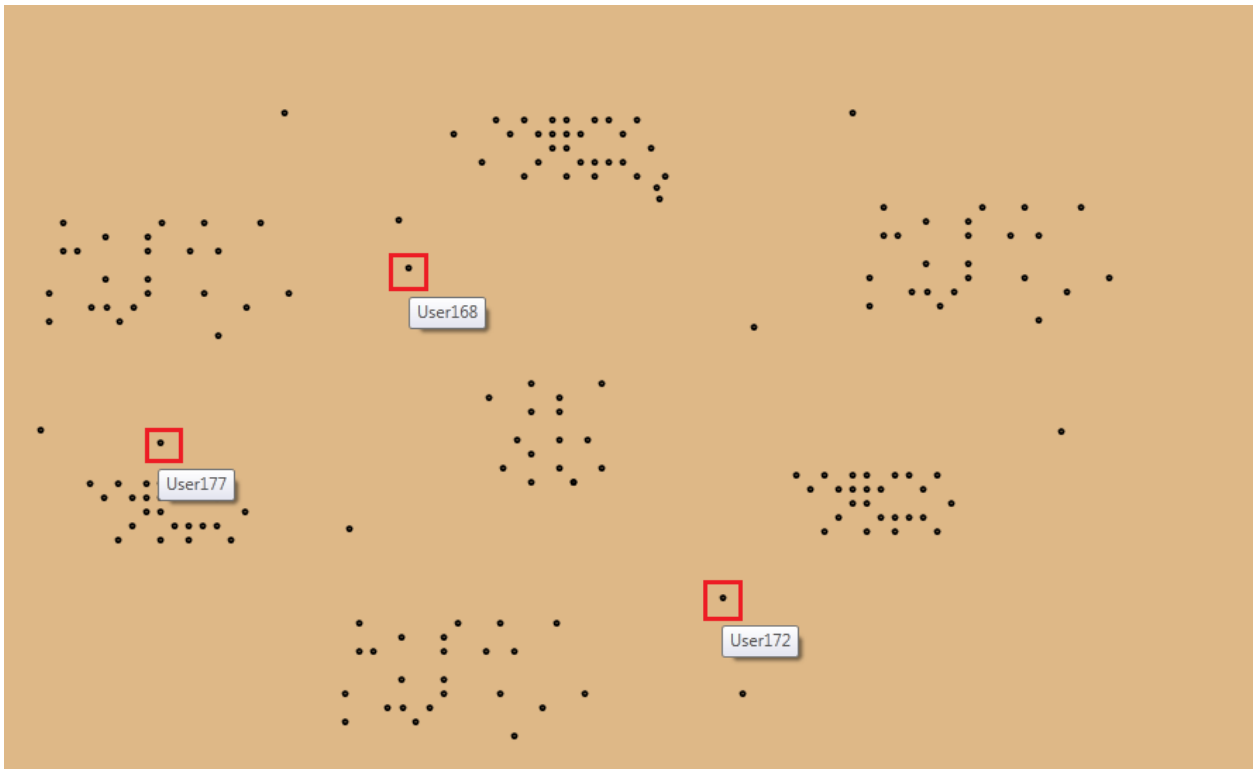


Рисунок В.3 – Вибір альтернатив для порівняння за методом MAI

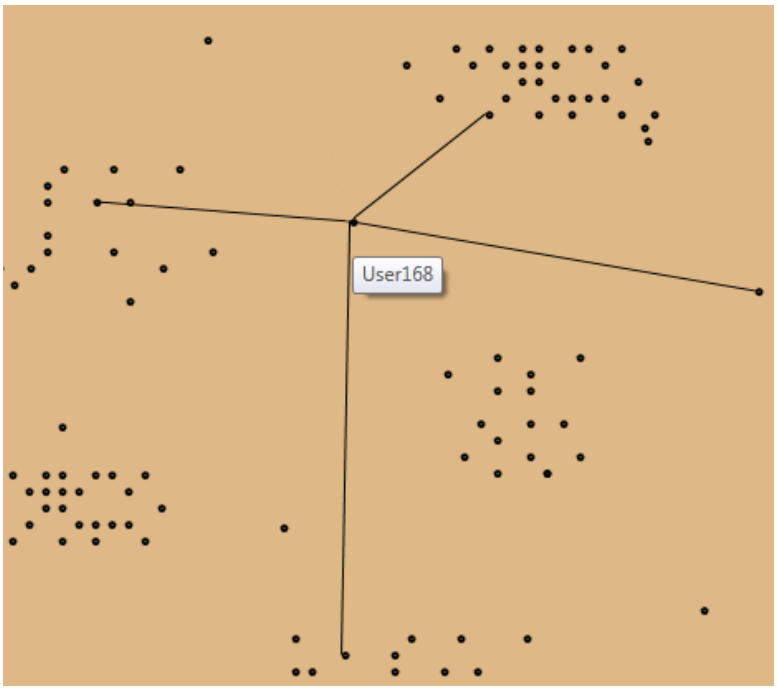


Рисунок В.4 – Відображення зв’язків вузла №168

Продовження додатку В

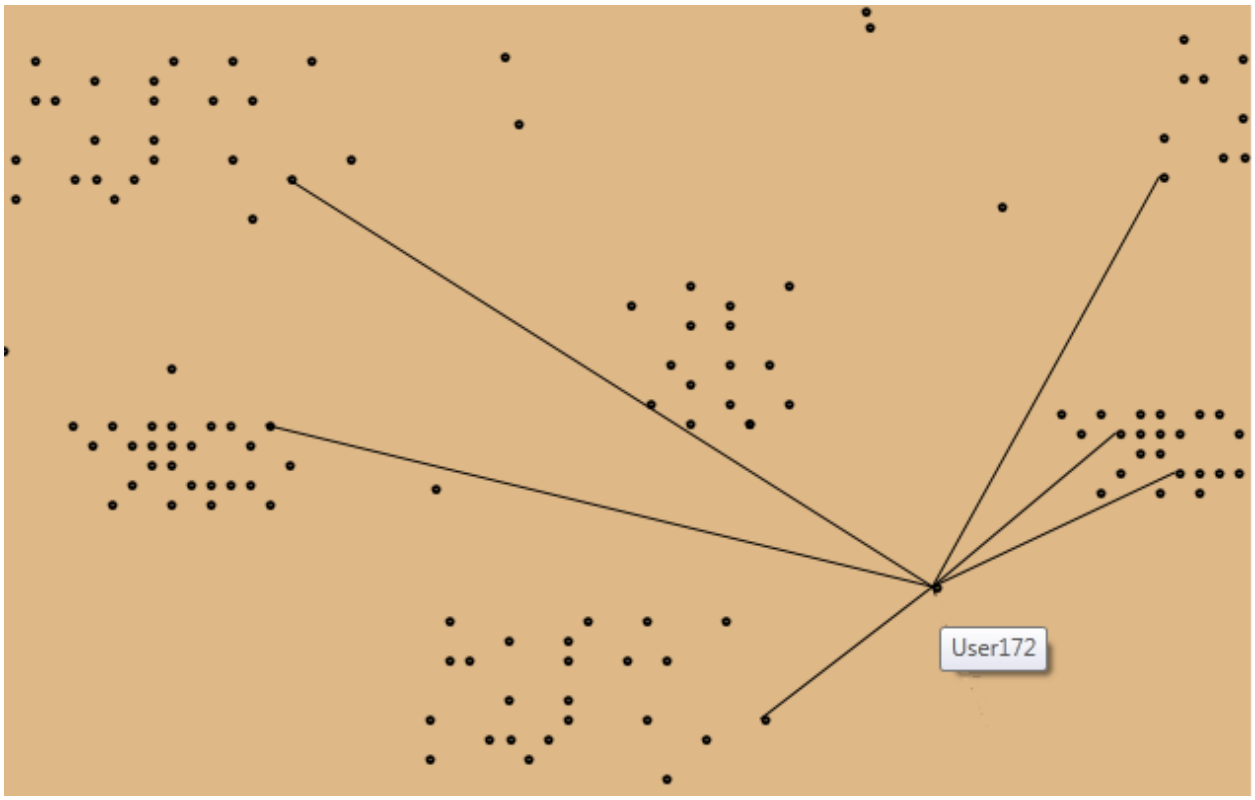


Рисунок В.5 – Відображення зв’язків вузла №172

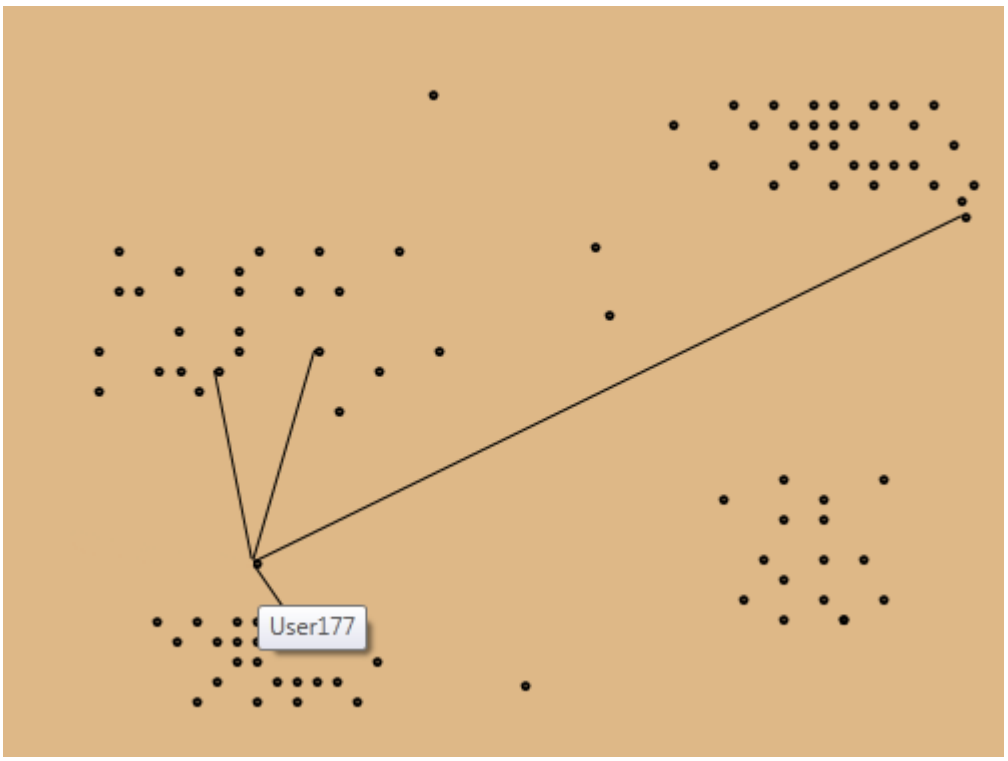


Рисунок В.6 – Відображення зв’язків вузла №177

Додаток Г. Приклад оцінки альтернативних вузлів за адаптованим методом аналізу ієрархій

Матриця ранжування критеріїв

	K1	K2	K3	K4	K5	K6	K7
K1	1	0,25	5	0,166667	3	2	0,142857
K2	4	1	6	0,333333	5	3	0,2
K3	0,2	0,166667	1	0,166667	0,5	0,2	0,125
K4	6	3	6	1	5	3	0,2
K5	0,333333	0,2	2	0,2	1	0,2	0,166667
K6	0,5	0,333333	5	0,333333	5	1	0,25
K7	7	5	8	5	6	4	1

K1	Кількість зв’язків.
K2	Активність
K3	Спротив
K4	Стр. положення
K5	Репутація
K6	R/O
K7	Act*Str

Вектори матриці:

u0= 0,0740842160924068

u1= 0,14920477711075

u2= 0,0241300326258813

u3= 0,216400859252458

u4= 0,0347320775397942

u5= 0,0814670884681576

u6= 0,419980948910552

Продовження додатку Г

Матриця парних порівнянь альтернатив відносно критерію :K1

	V168	V172	V177
V168	1	0,333333	1
V172	3	1	3
V177	1	0,333333	1

Вектори матриці
v0= 0,2
v1= 0,6
v2= 0,2

λ max:3

OC:2,46716227694479E-16

Матриця парних порівнянь альтернатив відносно критерію :K2

	V168	V172	V177
V168	1	2	0,5
V172	0,5	1	0,25
V177	2	4	1

Вектори матриці
v0= 0,285714285714286
v1= 0,142857142857143
v2= 0,571428571428571

λ max:3

OC:0

Матриця парних порівнянь альтернатив відносно критерію :K3

	V168	V172	V177
V168	1	4	3
V172	0,25	1	0,5
V177	0,3333333	2	1

Вектори матриці
v0= 0,625013074348293
v1= 0,136499802988861
v2= 0,238487122662845

λ max: 3,01829470728963

OC: 0,0101637262720174

Матриця парних порівнянь альтернатив відносно критерію :K4

	V168	V172	V177
V168	1	5	2
V172	0,2	1	0,33333
V177	0,5	3	1

Вектори матриці
v0= 0,581552066851616
v1= 0,10945228951552
v2= 0,308995643632864

λ max: 3,00369459806364

OC: 0,00205255447979989

Продовження додатку Г

Матриця парних порівнянь альтернатив відносно критерію :K5

	V168	V172	V177
V168	1	7	5
V172	0,1428573	1	0,33333
V177	0,2	3	1

Вектори матриці
v0= 0,73064467136113
v1= 0,0809612319997507
v2= 0,18839409663912

λ max: 3,06488757987282

ОС: 0,0360486554848993

Матриця парних порівнянь альтернатив відносно критерію :K6

	V168	V172	V177
V168	1	7	5
V172	0,1428543	1	0,5
V177	0,2	2	1

Вектори матриці
v0= 0,73959409328298
v1= 0,0938126507273069
v2= 0,166593255989713

λ max: 3,01415188218621

ОС: 0,00786215677011488

Матриця парних порівнянь альтернатив відносно критерію :K7

	V168	V172	V177
V168	1	5	1
V172	0,2	1	0,25
V177	1	4	1

Вектори матриці
v0= 0,466469858366229
v1= 0,100497884471846
v2= 0,433032257161925

λ max: 3,0055351117385

ОС: 0,00307506207694338

Продовження додатку Г

Матриця порівняння альтернатив

	K1	K2	K3	K4	K5	K6	K7
	0,074084	**0,149205**	**0,02413**	**0,216401**	**0,034732**	**0,081467**	**0,419981**
V168	0,2	0,285714	0,625013	0,581552	0,730645	0,739594	0,46647
V172	0,6	0,142857	0,1365	0,109452	0,080961	0,093813	0,100498
V177	0,2	0,571429	0,238487	0,308996	0,188394	0,166593	0,433032

Узагальнені пріоритети

$\lambda 0 = 0{,}479914570940781$

$\lambda 1 = 0{,}145406604199733$

$\lambda 2 = 0{,}374678824859486$

Альтернатива, що вибрана на основі методу аналізу ієрархій: **V168**