



DOI 10.28925/2663-4023.2023.20.272282

УДК 004.6

Дмитрієнко Катерина Анатоліївна

аспірант кафедри інформаційної та кібернетичної

безпеки імені професора Володимира Бурячка

Київський університет імені Бориса Грінченка, м. Київ, Україна

ORCID 0000-0001-7984-7279

k.dmytriienko.asp@kubg.edu.ua

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ В ІНТЕРНЕТ-СЕРЕДОВИЩІ

Анотація. Дослідження процесу поширення інформації в мережі Інтернет викликає особливий інтерес, оскільки це середовище загалом, а особливо — соціальні медіа стають все більш популярним каналом спілкування і все частіше — основним джерелом отримання інформації, відтак вони можуть сприяти поширенню фейкових новин, ненависті та дезінформації. Це може мати серйозні наслідки для суспільства, підриваючи довіру і розпалюючи конфлікти. Соціальні мережі стають потужним інструментом для маніпуляції громадською думкою. Пропаганда країни-агресора активно використовує їх для поширення фейкових новин, що підриває довіру до офіційних джерел інформації та дезорієнтує суспільство. Швидкість поширення інформації в інтернет-середовищі дозволяє створювати ефект «лавини», коли фейкові новини поширюються з неймовірною швидкістю, що ускладнює їх спростування. Моделювання розповсюдження інформації в інтернет-середовищі дозволяє зрозуміти її вплив на поведінку людей в економічній, політичній та соціальній сферах. В статті здійснено порівняльний аналіз різних методів розповсюдження інформації, зокрема моделі шуму та впливу, моделі вірусного поширення, моделі залежних поширень, моделі поширення чуток, моделі впливових користувачів та моделі на основі клітинних автоматів, включаючи принципи, особливості та можливі обмеження. Даний аналіз спрямований на визначення ефективності кожної моделі у відтворенні реальних процесів розповсюдження інформації, а також на виявлення можливості їх застосування за різноманітних сценаріїв. Узагальнено характеристики та визначено обмеження на застосування даних моделей при дослідженні розповсюдження інформації в інтернеті.

Ключові слова: розповсюдження інформації; моделі розповсюдження інформації; вплив на користувачів; джерело розповсюдження інформації.

ВСТУП

Постановка проблеми. Одним з найсуттєвіших викликів сьогодення стає реагування на кіберзагрози, складність яких зростає. Кібератаки стають все більш складними, цільовими та руйнівними, а учасники кіберконфліктів — більш різноманітними. З'являються нові методи атак, які важко виявити та протистояти. Існуючі моделі безпеки часто не враховують нових загроз та тенденцій, а отже, можуть бути нездатними адекватно оцінювати ризики [9]. Крім того, сучасний світ характеризується безпрецедентним потоком інформації, який поширюється через різноманітні канали, в тому числі через соціальні мережі. Швидке поширення інформації може мати значний вплив на суспільство, формуючи громадську думку, впливаючи на політичні процеси та навіть провокуючи соціальні конфлікти. Розуміння механізмів цього поширення є критично важливим для ефективної боротьби з дезінформацією, розповсюдження якої є одним із актуальних інформаційних ризиків [6]. Розповсюдження

інформації в Інтернеті є складним процесом, який може бути описаний та досліджений за допомогою різних моделей. Врахування різноманітних факторів, які впливають на цей процес, є ключовим для кращого розуміння процесу поширення інформації та розробки ефективних стратегій впливу на нього.

На сьогодні актуальною є проблема визначення оптимальних методів моделювання розповсюдження інформації в онлайн середовищі, оскільки моделі відрізняються за своєю точністю, складністю та можливістю відтворення реальних сценаріїв. Також існує питання щодо обмежень та недоліків кожної з моделей, можливостей їх застосування в конкретних контекстах та спроможності передбачення поведінки інформаційних потоків в мережі.

Аналіз останніх досліджень і публікацій. Дослідження різних моделей розповсюдження інформації в Інтернеті відкриває шлях для розуміння та вдосконалення стратегій контролю, управління і впливу на цей процес в цілому. На основі базової моделі розповсюдження інформації (рис. 1) були створені безліч різних моделей розповсюдження інформації, які мають велику кількість класифікацій [4], [5], [10], [14]. В роботі [16] запропоновано математичну вірусну модель для характеристики динаміки поширення інформації на платформах соціальних медіа та показано, що вона може застосовуватися для розуміння деяких надзвичайних явищ у соціальних мережах. В роботі [7] при дослідженні настроїв у соціальних мережах рекомендується використовувати аналіз на основі технологій штучного інтелекту, що видається ефективним, оскільки дозволяє ідентифікувати настрої споживачів, контекст та іронію на основі текстових даних та емоджі з високим рівнем ймовірності. В [8] досліджується феномен соціальної дифузії інформації за наявності в мережі суперечливої інформації на основі марківської ланцюгової моделі. В дослідженні [12] пропонується методологія відстеження швидкості, з якою інформація поширюється через структуру соціальної взаємодії, на основі дифузійних моделей.

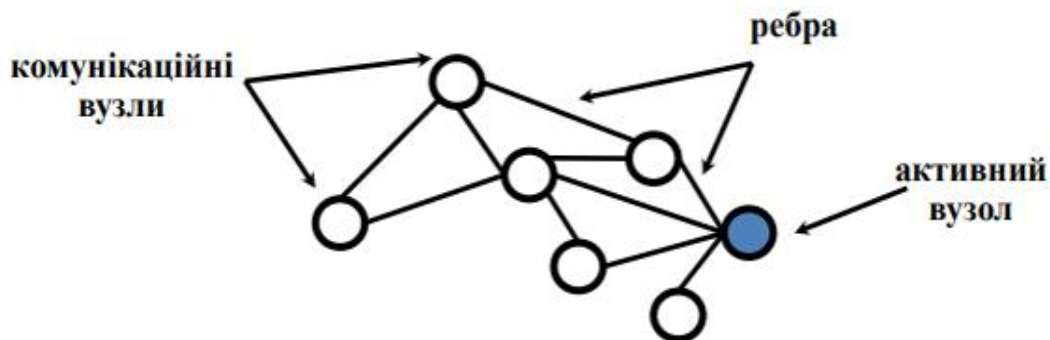


Рис. 1. Базова модель розповсюдження інформації [1]

Ці моделі допомагають розуміти, як вірусні пости, новини, інформаційні тенденції та ідеї поширюються через мережу Інтернет.

Метою статті є визначення властивостей, характеристик і недоліків досліджених моделей розповсюдження інформації.



РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Модель шуму та впливу (Threshold Model). Ця модель враховує психологічні аспекти впливу на прийняття рішень. Користувач приймає рішення на основі внутрішнього порогу чи «шуму», коли певна кількість його зв'язків або оточення вже прийняли певну інформацію.

Для аналізу соціальних мереж використовують адаптовану теорію динамічного соціального впливу Латане, яка дозволяє визначити кількість впливів на окремих користувачів (агентів) з боку їхнього оточення. Ця теорія виділяє три ключові атрибути взаємодії між джерелом впливу та агентом: відстань між агентом і джерелом, інтенсивність впливу джерела на агента та кількість джерел, що впливають на агента. Під відстанню мається на увазі швидкість передачі інформаційного повідомлення від джерела до агента впливу.

Рівень впливу на агента обчислюється за формулою:

$$I_i = -S_i \beta - \sum_{j=1, j \neq i}^N \frac{S_j O_j O_i}{d_{ij}^\alpha}, \quad (1)$$

де I_i — кількість соціального тиску на агента i ; O_i — думка i -го агента (+/-1) відносно даного запитання; (значення +1 відповідає підтримці, значення -1 — спротиву щодо пропозиції); S_i — сила соціального впливу ($S_i \geq 0$); β — спротив агента щодо змін ($\beta > 0$); α — ступінь ослаблення відстані ($\alpha \geq 0$); N — загальна кількість агентів, які взаємодіють; d_{ij} — відстань між агентами i та j ($d_{ij} \geq 1$). Відповідно, $\beta = 2$, ґрунтуючись на дослідженнях Латане. Більше значень β означає, що для зміни думки агента потрібно більший тиск і навпаки. Нехай $\alpha = 2$. Відповідно, більше α означає, що збільшуючи відстань між джерелом та агентом потрібна більша величина тиску. У випадку щодо використання соціальних мереж доцільно інтегрувати різні підходи, наприклад, нехтуючи відстанню [2].

Модель шуму та впливу має кілька недоліків. Вона може надмірно спрощувати реальні умови, не враховувати динамічні зміни загроз та технологій захисту, і недооцінювати роль людського фактора, зокрема поведінкові аспекти користувачів. Для дуже складних систем модель може бути недостатньо точною або занадто складною для практичного застосування. Також їй може бракувати емпіричних даних для підтвердження теоретичних передумов, механізмів адаптації до нових типів загроз, і налаштування може вимагати значних ресурсів і спеціалізованих знань.

2. Модель вірусного поширення (Viral Spread Model). Ця модель аналізує поширення інформації як вірусу. Інформаційний «вірус» поширюється в мережі через дії користувачів, які діляться контентом з іншими користувачами.

Розвиток зазначеного напрямку дослідження проводиться на основі сучасних наукових методів теорії соціальних досліджень та теорії інформаційних операцій з метою виявлення часових показників, які характеризують розповсюдження матеріалів інформаційних впливів до кожної цільової аудиторії. Крім цього доцільно застосовувати методи дослідження, які засновані на подібності процесів розповсюдження інформації та процесів поширення епіdemій. Процес розповсюдження інформації і вірусної хвороби можна аналітично формалізувати за допомогою однакової системи диференціальних рівнянь (2):

$$\begin{cases} \frac{dA}{dt} = -A(t)\mu + B(t)\varepsilon + C(t)\lambda; \\ \frac{dB}{dt} = -B(t)\mu - B(t)\varepsilon + C(t)\lambda(1 - \varepsilon); \\ \frac{dC}{dt} = (A(t) + B(t)\mu - C(t)\lambda). \end{cases} \quad (2)$$

з початковими умовами в момент часу $t = 0$:

$$A(t) = A_0, B(0) = B_0, C(0) = C_0.$$

Рішення цієї системи рівнянь може бути подане у наступному вигляді:

$$\begin{aligned} A(t) &= C_1g + C_2ve^{t(-\mu-\lambda)} - C_3e^{t(-\mu-\varepsilon)}, \\ B(t) &= -C_1r - C_2ue^{t(-\mu-\lambda)} + C_3e^{t(-\mu-\varepsilon)}, \\ C(t) &= C_1 + C_2e^{t(-\mu-\lambda)}, \end{aligned}$$

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

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

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

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

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

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

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

Логіка функціонування моделі, що розглядається, базується на поданні цільової аудиторії інформаційного каналу як суми трьох груп людей: A — кількість активних користувачів новинного каналу, тобто тих, хто прочитав інформаційну новину; B — кількість неактивних користувачів каналу, тобто тих, хто не прочитав новину, але є користувачем; C — кількість не підписників, які відповідно і не читали новину. Крім того, до моделі входять наступні параметри: λ — інтенсивність підписування на новинного агента; μ — інтенсивність відписування від новинного агента; ξ — інтенсивність прочитування новини. Дані щодо кількісних значень перших двох параметрів можна отримати за допомогою моніторингу за новинним агентом та кількістю його користувачів. Параметр ξ враховує такі властивості новини як актуальність і час опублікування, а також активність взаємодії користувачів у внутрішніх мережах новинного агента.

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

$$\varphi = \frac{m}{M}, \quad (3)$$

m — кількість новинних джерел, які описують вибрану новину;

M — загальна кількість джерел.

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

$$\delta = \frac{e}{E}, \quad (4)$$

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

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

Наступний параметр — ω — характеризує імовірність користувачів впливати на процес зростання прочитуваності новини. Будемо вважати, що

$$\omega = \frac{s}{(A_0 + B_0)}, \quad (5)$$

де s — кількість користувачів, що здійснили одну з дій: лайк або репост; (A_0+B_0) — кількість користувачів новинного агента.

Таким чином імовірність прочитання новини можна подати наступним виразом:

$$\varepsilon = \varphi \delta \omega. \quad (6)$$

Таким чином, якщо відомі всі розглянуті параметри моделі, то можуть бути розраховані значення функції $A(t)$ в потрібний момент часу і побудований графік зростання кількості користувачів за зазначений час дослідження [2]. Модель вірусного поширення також має свої недоліки. Вона може не враховувати складність сучасних мереж і систем, де віруси поширюються не тільки через прямі контакти, але і через складні мережеві взаємодії. Модель може спрощувати різноманітність векторів атак і методів захисту, що існують в реальному світі. Вона часто недооцінює вплив поведінки користувачів та соціальних інженерних атак. Крім того, ефективність моделі залежить від точності введених даних і параметрів, що може бути проблематичним через брак достовірної інформації. Налаштування і моделювання можуть потребувати значних обчислювальних ресурсів і спеціалізованих знань.

3. Модель залежних поширень (Dependent Cascade Model). Ця модель передбачає, що кожен користувач може поширювати інформацію тільки залежно від своїх сусідів.

Модель Ізінга в основному використовується для опису фазового переходу речовини. Завдяки фазовій зміні матеріал створює нові структури та фізичні властивості. Система фазової зміни, як правило, є сильною взаємодією між молекулами, яка також відома як кооперативні системи.

Рівняння (7) є детальним описом цієї моделі для обліку внесків користувачів. Наприклад, коли користувач бере участь у дослідженні певного проекту, стан встановлюється на «+1». В іншому випадку, коли користувач вирішує залишити цей проект, стан встановлюється на «-1». Імовірність того, що індивід змінить поточний стан, визначається у рівняннях (7), (8) наступним чином:

$$p_i(t) = \frac{1}{1 + \exp\left(\frac{\Delta\mu_i(t)}{T}\right)}, \quad (7)$$

$$\mu_i(t) = -m_i(t-1) \sum_{j=1}^n m_j(t-1), \quad (8)$$

де $\sum_{j=1}^n m_j$ — де стан сусіда i в момент часу t , а T — зовнішня температура [11].

4. Модель поширення чуток (Rumor Spreading Model). Ця модель аналізує, як чутки та нечітка інформація поширюються в мережі через міжособистісні зв'язки та комунікацію.

В своїй роботі О.С. Улічев зазначає, що «...взявши за основу модель SIR в 1965 році була запропонована модель Далей-Кендалла (ДК-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 чуток (новини); V — група, що сприймає чуток і продовжує її розповсюдження; W — група, що не сприймає інформації і не розповсюджує її далі. В

«моделі розповсюдження чуток» виділено всі ті ж три групи, але їх інтерпретація адаптована саме до процесу інформаційного обміну. В ДК-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 [15, ст. 148]:

$$\gamma V(V + W)/N». \quad (9)$$

Модель недооцінює складність і динаміку реальних соціальних мереж, через що моделювання стає менш точним. Ця модель часто припускає однорідність поведінки користувачів, не враховуючи різноманітні індивідуальні характеристики, мотивації та рівень впливу. Це може призвести до неточностей у прогнозах поширення інформації. Крім того, модель може не враховувати зовнішні фактори, такі як зміни в суспільних настроях або вплив медіа, що також знижує її ефективність. Вона може бути менш застосовною до інформації, яка потребує спеціальних знань для розуміння, оскільки припускає просту передачу чуток без перевірки фактів.

5. Модель впливових користувачів (Influential User Model). Ця модель враховує вплив важливих та впливових користувачів в мережі на поширення інформації. Існує декілька моделей визначення впливових користувачів, але центральність Каца вимірює відносну важливість вузла мережі і шляхом обчислення кількості інших вузлів — сусідів першого ступеня, які підключаються до вузла, подається як:

$$CKatz(i) = \sum_{k=1}^{\infty} \sum_{j=1}^n \alpha^k (A^k)_{ji}. \quad (10)$$

Це рівняння показує, що значення на місці (i,j) матриці суміжності A , піднесеної до степеня k , такий як A_k , представляє загальну кількість k -ступеневі зв'язки між вузлом i та вузлом j .

Коефіцієнт ослаблення α регулюється таким чином, що його значення є меншим, ніж зворотне абсолютне значення найвищого власного значення матриці A . У цьому сценарії наступне рівняння можна використовувати для обчислення центральності Каца, заданої як:

$$\overrightarrow{C_{Katz}} = \{(I - \alpha A^T)^{-1} - I\} \vec{I}, \quad (11)$$

де I та \vec{I} представляють матрицю ідентичності та вектор ідентичності (розмірністю, що дорівнює кількості вузлів мережі) відповідно. Так само A^T транспонування матриці суміжності A і $(I - \alpha A^T)^{-1}$ є матрицею, оберненою до члена $(I - \alpha A^T)$. Однак, якщо високопідключений вузол з'єднується з багатьма іншими мережевими вузлами, тоді ці інші вузли отримують високі оцінки центральності. Центральність, яка досягається за допомогою посилення із важливих вузлів, повинна бути розведена або зменшена, якщо важливі вузли великодушно підтримують підтримку [13].

Як і всі інші моделі, модель впливових користувачів також має свої недоліки. Вона може переоцінювати роль впливових користувачів, припускаючи, що вони завжди відіграють ключову роль у поширенні інформації, що не завжди відповідає дійсності. Інформація може поширюватися й через менш впливових, але більш численних користувачів. Крім того, ідентифікація впливових користувачів може бути складною та неточною, оскільки рівень впливу може змінюватися залежно від контексту та часу. Модель також може недооцінювати важливість контенту та його відповідність аудиторії, зосереджуючись виключно на характеристиках користувачів. Це може призвести до спрощення складних процесів інформаційного впливу та знижувати точність прогнозів.

6. Модель на основі клітинних автоматів (Cellular automaton-based model). У дослідженні моделей поширення інформації та інформаційних впливів у соціальних

мережах описано модель на основі клітинних автоматів. В основі таких моделей лежить дискретна динамічна система, що складається з однорідних клітин. Кожна клітина може перебувати в певних станах та переходити між ними за визначеними правилами. На перехід клітини до іншого стану впливають оточуючі її клітини. Моделі відрізняються наборами можливих станів та правилами переходів між ними. Ці моделі враховують динаміку та структуру мережі, включаючи околиці кожної клітини та стани оточуючих її клітин. У деяких джерелах такі моделі називають моделями дифузії інновацій.

Формально клітинний автомат може бути описаний співвідношенням:

$$y_j(t+1) = F(y_j(t), O(j), T), \quad (12)$$

де t — крок ітерації, F — формальне представлене правило переходу до іншого стану; $y_j(t)$ — стан на попередніх ітераціях; $O(j)$ — множина сусідніх клітин (окіл кінцевого клітинного автомату). У 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. Також пропонується враховувати параметр старіння новини та використовувати систему порогів [15].

Недоліки моделей на основі клітинних автоматів включають обмежену точність передбачення, складність визначення початкових умов та обмежену придатність до моделювання динамічних систем.

Клітинні автомати можуть мати складності у відтворенні реальних процесів через спрощену модель взаємодії між клітинами та обмежену рівномірність інформаційного обміну. Крім того, вони можуть виявляти складнощі у врахуванні глобальних впливів на систему і невідповідність динаміки реального світу. Ці недоліки можуть ускладнювати точне моделювання та аналіз систем, особливо в контексті складних та динамічних процесів, які характеризуються високою ступенем нелінійності та непередбачуваністю.

Ці моделі допомагають аналізувати та передбачати способи та швидкість поширення інформації в Інтернеті. Вони є важливими для розуміння соціальних явищ та впливу в Інтернеті, а також для ефективного управління та розробки стратегій поширення контенту та інформації.

Згідно з проаналізованими даними можна визначити властивості моделей і їх основні характеристики, які наведені в табл. 1.

Таблиця 1

Властивості та основні характеристики розглянутих моделей

Властивості / Модель	1	2	3	4	5	6	7	8	9	10	11
Модель шуму та впливу	+	-	+	-	-	+	+	+/-	-	-	+
Модель вірусного поширення	-	+	-	-	+	-	+	-	+	-	+/-
Модель залежних поширень	+/-	+	-	-	+	-	+	-	+/-	+/-	-
Модель поширення чуток	+/-	+	+/-	-	-	+/-	+	-	-	-	-
Модель впливових користувачів	+	+	+	-	-	-	-	+	+	+	+
Моделі на основі клітинних автоматів	+	-	+	+	+/-	+	-	-	-	+/-	+



Стовпці таблиці:

- 1 — Вплив оточуючих на зміну думки користувачів;
- 2 — Наявність ймовірнісних параметрів;
- 3 — Різний ступінь схильності агентів до інформаційного впливу;
- 4 — Оптимізація інформаційного впливу;
- 5 — Оцінка ймовірності результату та розподілу користувачів у певний момент часу;
- 6 — Кількість джерел інформації;
- 7 — Ігнорування відстані між користувачами;
- 8 — Визначення початку розповсюдження інформації;
- 9 — Часовий масштаб моделі;
- 10 — Адаптація моделі до змін;
- 11 — Рівень деталізації моделі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розглянуті моделі допомагають аналізувати та передбачати способи та швидкість поширення інформації в Інтернеті. Вони є важливими для розуміння соціальних явищ та впливу в Інтернеті, а також для ефективного управління та розробки стратегій поширення контенту та інформації. Дослідження показує, що кожна з них має свої переваги і обмеження. Наприклад, модель шуму та впливу може бути корисною для аналізу динаміки поширення інформації в мережі, але вона може недостатньо враховувати особливості соціальних взаємодій. Модель вірусного поширення, у свою чергу, може бути ефективною для вивчення масштабів розповсюдження інформації через мережі, але вона може не враховувати динаміку соціальних зв'язків та впливу внутрішніх факторів на процес поширення. Моделі залежних поширень, поширення чуток та впливових користувачів можуть застосовуватися для аналізу взаємодії між учасниками мережі та виявлення ключових впливових факторів, але можуть бути обмеженими у своїй спроможності передбачити складні динамічні зміни у поведінці користувачів та поширенні інформації.

Отже, для подальшого вдосконалення моделей розповсюдження інформації необхідно проводити додаткові дослідження та розробляти нові підходи, які б враховували широкий спектр факторів, що впливають на динаміку поширення інформації в мережі. Особливо важливо також розвивати методи об'єднання різних моделей для створення більш комплексних та адаптивних підходів до аналізу розповсюдження інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Voitko, O. (2021). Model of dissemination of information in the implementation of the strategic narrative of the state. *Modern Information Technologies in the Sphere of Security and Defence*, 41(2), 47–52. <https://doi.org/10.33099/2311-7249/2021-41-2-47-52>
2. Войтко, О., Солонніков, В., & Полякова, О. (2022). SIR-модель розповсюдження та врахування результатів негативного впливу інформаційних каналів на громадську думку населення. *Сучасні інформаційні технології у сфері безпеки та оборони*, 43(1), 115–120. <https://doi.org/10.33099/2311-7249/2022-43-1-115-120>
3. Гриб'юк, О. (2017). *Феномен соціальних мереж: парадокс залежності та варіативності моделювання*. Digital Library NAES of Ukraine.



4. Рахімов, В. (2021). Розповсюдження інформації в соціальних мережах – головний інструмент реалізації державного нарративу. *Гібридна агресія Російської Федерації: досвід протидії України, наслідки для Європи: збірник матеріалів міжнародної науково-практичної конференції*, 192–197.
5. Черній, П. Д. (2017). Моделі поширення повідомлень в онлайн соціальних мережах: властивості, структура, особливості застосування. *Вісник Харківського національного університету імені В.Н. Каразіна*, 127–134.
6. Berestov, D., Kurchenko, O., Shechblanin, Y., Korshun, N., & Opryshko, T. (2021). Analysis of features and prospects of application of dynamic iterative assessment of information security risks. In: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 2923, 329–335.
7. Shevchuk, D., Harasymchuk, O., Partyka, A., & Korshun, N. (2023). Designing Secured Services for Authentication, Authorization, and Accounting of Users. In: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3550, 217–225.
8. Dennis, L. A., Fu, Y., & Slavkovik, M. (2022). Markov chain model representation of information diffusion in social networks. *Journal of Logic and Computation*. <https://doi.org/10.1093/logcom/exac018>
9. Grechaninov, V., Hulak, H., Sokolov, V., Skladannyi, P., & Korshun, N. (2021). Formation of dependability and cyber protection model in information systems of situational center. In: *Emerging Technology Trends on the Smart Industry and the Internet of Things*, vol. 3149, 107–117.
10. Guille, A., Hacid, H., Favre, C., & Zighed, D. A. (2013). Information diffusion in online social networks. *ACM SIGMOD Record*, 42(2), 17–28. <https://doi.org/10.1145/2503792.2503797>
11. Ishfaq, U., Khan, H. U., & Iqbal, S. (2022). Identifying the influential nodes in complex social networks using centrality-based approach. *Journal of King Saud University - Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2022.09.016>
12. Kumar, P., & Sinha, A. (2021). Information diffusion modeling and analysis for socially interacting networks. *Social Network Analysis and Mining*, 11(1). <https://doi.org/10.1007/s13278-020-00719-7>
13. Razaque, A., Rizvi, S., Khan, M. J., Almiani, M., & Rahayfeh, A. A. (2019). State-of-art review of information diffusion models and their impact on social network vulnerabilities. *Journal of King Saud University - Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2019.08.008>
14. Li, M., Wang, X., Gao, K., & Zhang, S. (2017). A survey on information diffusion in online social networks: models and methods. *Information*, 8(4), 118. <https://doi.org/10.3390/info8040118>
15. Ulichev, O. S. (2018). Research of information dissemination models and information influences in social networks. *Control, navigation and communication systems. Collection of scientific papers*, 4(50), 147–151. <https://doi.org/10.26906/sunz.2018.4.147>
16. A virus dynamics model for information diffusion in online social networks. (2021). *Communications in Mathematical Biology and Neuroscience*. <https://doi.org/10.28919/cmbn/6569>

**Kateryna Dmytriienko**

Graduate student of the Department of Information and Cyber Security

named after Professor Volodymyr Buryachok

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID 0000-0001-7984-7279

k.dmytriienko.asp@kubg.edu.ua**COMPARATIVE ANALYSIS OF INFORMATION DISSEMINATION
MODELS IN THE ONLINE ENVIRONMENT**

Abstract. The study of the process of information dissemination on the Internet is of particular interest today, since this environment in general, and social media in particular, are becoming an increasingly popular channel of communication and, increasingly, the main source of obtaining information, so they can contribute to the spread of fake news, hatred and misinformation. This can have serious consequences for society, undermining trust and fueling conflicts. Social networks are becoming a powerful tool for manipulating public opinion. Propaganda of the aggressor country actively uses them to spread fake news, which undermines trust in official sources of information and disorients society. The speed of information dissemination in the Internet environment allows creating an “avalanche” effect, when fake news spreads at an incredible speed, which makes it difficult to refute them. Modeling the spread of information in the Internet environment allows you to understand its impact on people’s behavior in the economic, political and social spheres. The article provides a comparative analysis of various information dissemination methods, including noise and impact models, viral propagation models, dependent propagation models, rumor propagation models, influencer models, and models based on cellular automata, including principles, features, and possible limitations. This analysis is aimed at determining the effectiveness of each model in reproducing real processes of information dissemination, as well as at identifying the possibility of their application in various scenarios. The characteristics are summarized and limitations on the application of these models for the study of information dissemination on the Internet are defined.

Keywords: information spread; information diffusion models; impact on users; information source.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Voitko, O. (2021). Model of information diffusion in the implementation of a state’s strategic narrative. *Modern information technologies in the field of security and defense*, 41(2), 47–52. <https://doi.org/10.33099/2311-7249/2021-41-2-47-52>
2. Voitko, O., Solonnikov, V., & Poliakova, O. (2022). SIR model for disseminating information and accounting for the negative effects of information channels on public opinion. *Modern information technologies in the field of security and defense*, 43(1), 115–120. <https://doi.org/10.33099/2311-7249/2022-43-1-115-120>
3. Hrybiuk, O. (2017). *The phenomenon of social networks: the paradox of dependence and modeling variability*. Digital Library NAES of Ukraine.
4. Rakhimov, V. (2021). Dissemination of information in social networks as the main tool for implementing the state narrative. *Hybrid aggression of the Russian Federation: the experience of countering Ukraine, consequences for Europe: collection of materials of the international scientific and practical conference*, 192–197.
5. Chernii, P. (2017). Models of message distribution in online social networks: properties, structure, features of application. *Bulletin of Kharkiv National University named after V.N. Karazin*, 127–134.
6. Berestov, D., Kurchenko, O., Shcheblanin, Y., Korshun, N., & Opryshko, T. (2021). Analysis of features and prospects of application of dynamic iterative assessment of information security risks. In: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 2923, 329–335.
7. Shevchuk, D., Harasymchuk, O., Partyka, A., & Korshun, N. (2023). Designing Secured Services for Authentication, Authorization, and Accounting of Users. In: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3550, 217–225.



8. Dennis, L. A., Fu, Y., & Slavkovik, M. (2022). Markov chain model representation of information diffusion in social networks. *Journal of Logic and Computation*. <https://doi.org/10.1093/logcom/exac018>
9. Grechaninov, V., Hulak, H., Sokolov, V., Skladannyi, P., & Korshun, N. (2021). Formation of dependability and cyber protection model in information systems of situational center. In: *Emerging Technology Trends on the Smart Industry and the Internet of Things*, vol. 3149, 107–117.
10. Guille, A., Hacid, H., Favre, C., & Zighed, D. A. (2013). Information diffusion in online social networks. *ACM SIGMOD Record*, 42(2), 17–28. <https://doi.org/10.1145/2503792.2503797>
11. Ishfaq, U., Khan, H. U., & Iqbal, S. (2022). Identifying the influential nodes in complex social networks using centrality-based approach. *Journal of King Saud University - Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2022.09.016>
12. Kumar, P., & Sinha, A. (2021). Information diffusion modeling and analysis for socially interacting networks. *Social Network Analysis and Mining*, 11(1). <https://doi.org/10.1007/s13278-020-00719-7>
13. Razaque, A., Rizvi, S., Khan, M. J., Almiani, M., & Rahayfeh, A. A. (2019). State-of-art review of information diffusion models and their impact on social network vulnerabilities. *Journal of King Saud University - Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2019.08.008>
14. A survey on information diffusion in online social networks: models and methods. (2017). *Information*, 8(4), 118. <https://doi.org/10.3390/info8040118>
15. Ulichev, O. S. (2018). Research of information dissemination models and information influences in social networks. *Control, navigation and communication systems. Collection of scientific papers*, 4(50), 147–151. <https://doi.org/10.26906/sunz.2018.4.147>
16. A virus dynamics model for information diffusion in online social networks. (2021). *Communications in Mathematical Biology and Neuroscience*. <https://doi.org/10.28919/cmbn/6569>

