УДК 004.94 **doi: 10.26906/SUNZ.2024.3.153**

О. С. Ткаченко[1], Є. В. Мелешко[1], В. В. Міхав[2]

[1] Центральноукраїнський національний технічний університет, Кропивницький, Україна
[2] ПУ «Університет науки, підприємництва та технологій», Київ, Україна

КОМП'ЮТЕРНА МОДЕЛЬ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВІРУСІВ У СОЦІАЛЬНІЙ МЕРЕЖІ ПРИ РІЗНІЙ ПОВЕДІНЦІ КОРИСТУВАЧІВ

Анотація. У наш час моделювання процесів поширення інформаційних вірусів є важливою задачею кібербезпеки, адже треба чітко розрізняти де правда, а де фейк, вміти виявляти джерело поширення фейкових новин і протидіяти дезінформації, щоб доносити до людей істину. Метою даної роботи було створення та дослідження комп'ютерної моделі поширення інформаційних вірусів у соціальній мережі при різній поведінці користувачів. Для виконання поставленої мети було використано епідеміологічну модель SIRS та моделі генерації структури соціальної мережі Барабаши-Альберт та Воттса-Строгаца. Модель SIRS ідеально підходить для імітації поширення комп'ютерного вірусу, адже в цій моделі людина може приймати циклічно три стани: здоровий, хворий та з імунітетом, а потім знов здоровий, а в соціальній мережі користувач заражується фейком замість вірусу і також проходить через ці стани. Для моделювання структури соціальної мережі було використано алгоритми Барабаши-Альберт і Воттса-Строгаца, які доступні в бібліотеці Networkx мови програмування Python. Запропоновано декілька різних способів поведінки користувачів для захисту від інформаційних вірусів, зокрема, видалення зв'язків між користувачами, видалення користувачів з мережі та блокування користувачів при їх підозрілій активності. Здійснено емпіричне дослідження та порівняння запропонованих методів боротьби з інформаційним вірусом за різними критеріями. Було запропоновано початкові параметри мережі, а саме, кількість користувачів, кількість зв'язків між ними та коефіцієнти моделі SIRS. З використанням мови програмування Python та бібліотек Pygame і Networkx було реалізовано запропоновану модель поширення інформаційного вірусу в соціальній мережі та змодельовано такі методи боротьби з фейком як: видалення зв'язків між користувачами, створення нового зв'язку, видалення користувачів, блокування користувачів. Найкращий результат боротьби з інформаційним вірусом ми отримуємо при комбінуванні методів видалення зв'язків і користувачів, а також блокуванні користувачів. При запропонованій поведінці користувачів інформаційному вірусу вдалося вдало протидіяти й виявити поширювача фейку та видалити його, при цьому кількість зв'язків між користувачами соціальної мережі зменшилась не дуже суттєво.

Ключові слова: соціальна мережа, інформаційна безпека, фейкові новини, інформаційні віруси, модель SIRS, модель Барабаши-Альберт, модель Воттса-Строгаца.

Вступ

Швидкий розвиток інформаційних технологій в останні роки суттєво вплинув на трансформацію соціальних структур, що призвело до появи інформаційного суспільства та цифрової економіки. Становлення глобальних медіа, розвиток комп'ютерних технологій, зростання Інтернету та соціальних мереж – ці та інші аспекти докорінно змінили механізми виробництва та поширення інформації, значно розширивши можливості для маніпулювання індивідуальною та суспільною свідомістю.

З одного боку, соціальні мережі дуже корисний та зручний інструмент для спілкування та бізнесу, з іншого боку, вони можуть використовуватися для поширення фейкових новин, ведення інформаційних воєн та впливу на політичні процеси [1]. Також соціальні мережі використовують складні алгоритми для персоналізації контенту, зокрема, рекомендаційні системи [2], що може призводити до створення *камер відлуння* [3, 4] та *бульбашок фільтрів* [4, 5], де користувачі стикаються лише з інформацією, що відповідає їхнім переконанням. Це сприяє утворенню ілюзії, що їхні погляди є загальноприйнятими та правдивими. В соціальних мережах інформацію зручно подавати таким чином, щоб викликати сильні емоції та використовувати суб'єктивні судження для впливу на громадську думку [6].

У наші часи розуміння унікальної епідеміології фейкових новин може мати таку ж вагу, як і вміння критичного мислення та фактчекінгу [7]. Постачальники дезінформації шукають найбільш вразливих та цінних «жертв» – тих, хто найбільше поширить їх інформаційні віруси. Вже не секрет, що для реклами продукту формується група людей або залучається популярна людина, щоб коментувати чи поширювати інформацію про цей об'єкт з найкращої сторони, рекомендуючи його через Twitter, Facebook або інші соціальні мережі. Схожий принцип використовується для поширення фейків та впливу на свідомість людей.

Таким чином середовище соцмереж схильне до епідемій фейкових новин [7]. Протидія фейкам вже стала питанням національної безпеки, як і протидія епідеміям біологічних вірусів. Бізнес підроблених новин приносить видавцям значні доходи від реклами та політичний вплив. Фейкові новини здатні впливати на соціальну реальність та змінювати її. Соцмережі стали ідеальною платформою для обміну контентом й поширення фейків. Тому питання захисту від інформаційних вірусів є дуже важливим для кібербезпеки у наш часі.

Метою роботи є розробка комп'ютерної моделі поширення інформаційних вірусів у соціальній мережі при різній поведінці користувачів. Для досягнення поставленої мети було використано теорію складних мереж [8–10] та моделі поширення вірусів [11].

Дослідження моделей соціальних мереж та моделей поширення вірусів

У якості моделей для генерації структури соціальної мережі були взяті моделі Барабаши-Альберт та Воттса-Строгаца, а для поширення вірусу – епі-

деміологічна модель SIRS. Розглянемо ці моделі та модель SIR, на якій заснована SIRS.

Модель Барабаши-Альберт є однією з ключових моделей для пояснення виникнення та еволюції складних мереж. Ця модель базується на двох основних концепціях: «прив'язка» та «безшкальне структурування» [9]. Концепція прив'язки вказує на те, що нові вузли у мережі більш схильні приєднуватися до вузлів, які вже мають багато зв'язків, ніж до менш зв'язаних вузлів. Це призводить до того, що деякі вузли набувають значно більше зв'язків, ніж інші, що створює безшкальну структуру мережі.

Алгоритм побудови моделі Барабаши-Альберт наступний:

Крок 1. Створюється початковий граф з декількох вузлів.

Крок 2. Додається новий вузол до графа.

Крок 3. Вибирається випадковий існуючий вузол у графі з ймовірністю, яка залежить від кількості зв'язків цього вузла.

Крок 4. Новий вузол з'єднується з обраним вузлом.

Крок 5. Повторюються кроки 2-4, доки не буде створено достатньо вузлів у графі.

Модель Воттса-Строгаца є ще однією важливою моделлю для вивчення складних мереж. Ця модель базується на концепції «малого світу» та «згрупованості» [10]. Концепція «малого світу» вказує на те, що в багатьох реальних мережах відстань між будь-якими двома вузлами виявляється дуже короткою, незважаючи на велику кількість вузлів у мережі. Концепція «згрупованості» показує, що в реальних мережах часто спостерігається явище, коли вузли мають тенденцію групуватися разом у підграфи.

Алгоритм побудови моделі Воттса-Строгаца наступний:

Крок 1. Створюємо граф у вигляді початкової решітки з N вузлів, де кожен вузол початково з'єднаний з k найближчими сусідами.

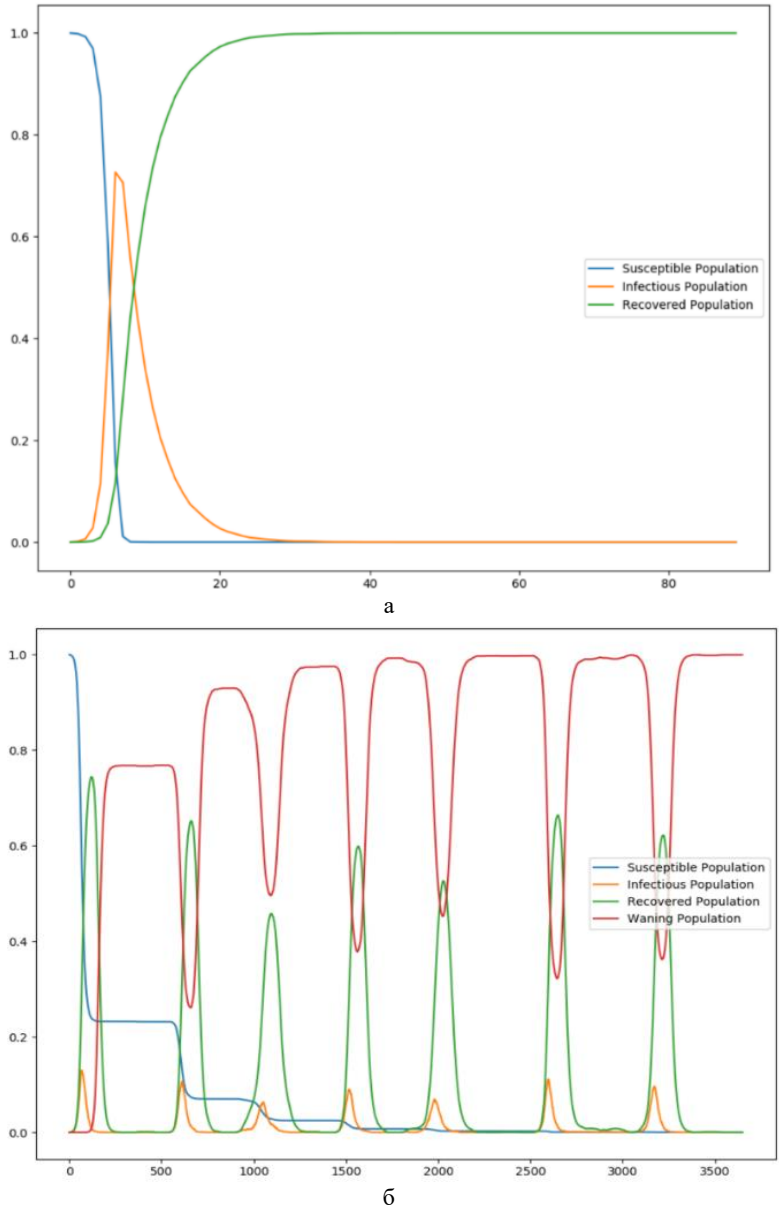
Крок 2. Для кожного вузла i, розглядаємо кожне з його з'єднання (i, j) і видаляємо з ймовірністю p.

Крок 3. З ймовірністю p, для кожного вузла i, замість видаленого зв'язку (i, j), додаємо новий зв'язок (i, m), де m обирається випадково з усіх інших вузлів, за винятком себе і своїх поточних сусідів, щоб уникнути повторень. Повторюємо цей крок доки не буде створено достатньо зв'язків у мережі.

Модель SIR – загальна епідеміологічна модель, яка забезпечує спрощений спосіб опису передачі інфекційного захворювання через людей, де вони можуть проходити через наступні 3 стани: сприйнятливі – S, заразні – I та одужали – R [11]. Загальна популяція: $N = S + I + R$. У замкнутій популяції без життєвої динаміки епідемія в кінцевому підсумку згасне через недостатню кількість сприйнятливих осіб для підтримки захворювання. Інфіковані особи, додані пізніше, не почнуть нової епідемії через довічний імунітет наявної популяції. На рис. 1, а представлено графік зростання інфекції та її виснаження під час спалаху за моделлю SIR.

Модель SIRS. Попередня модель SIR припускає, що люди мають довічний імунітет до хвороби після одужання і це стосується різноманітних захворювань. Але для іншого класу повітряно-крапельних захворювань, наприклад сезонного грипу, імунітет людини може з часом ослабнути. У цьому випадку використовується модель SIRS [11], яка дозволяє моделювати той факт, що люди, які одужали від вірусу, можуть повернутися до сприйнятливого стану.

На рис. 1, б показано коливання через те, що люди втрачають імунітет і знову стають сприйнят-



а

б

Рис. 1. Графіки SIR (а) та SIRS з "Waning Population" (б) [11]

ливими (особи, сприйнятливі через ослаблений імунітет, не класифікуються як сприйнятливі на графіку, а позначені як “Waning Population”, а ось після повної втрати імунітету особи знову стають “Susceptible”).

Наведена нижче схема SIR/SIRS моделей (рис. 2) показує, як люди змінюють свої стани під час поширення вірусу.

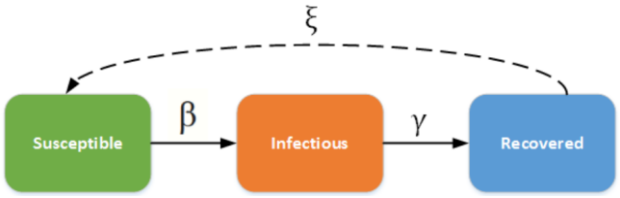


Рис. 2. Моделі SIR та SIRS [11]

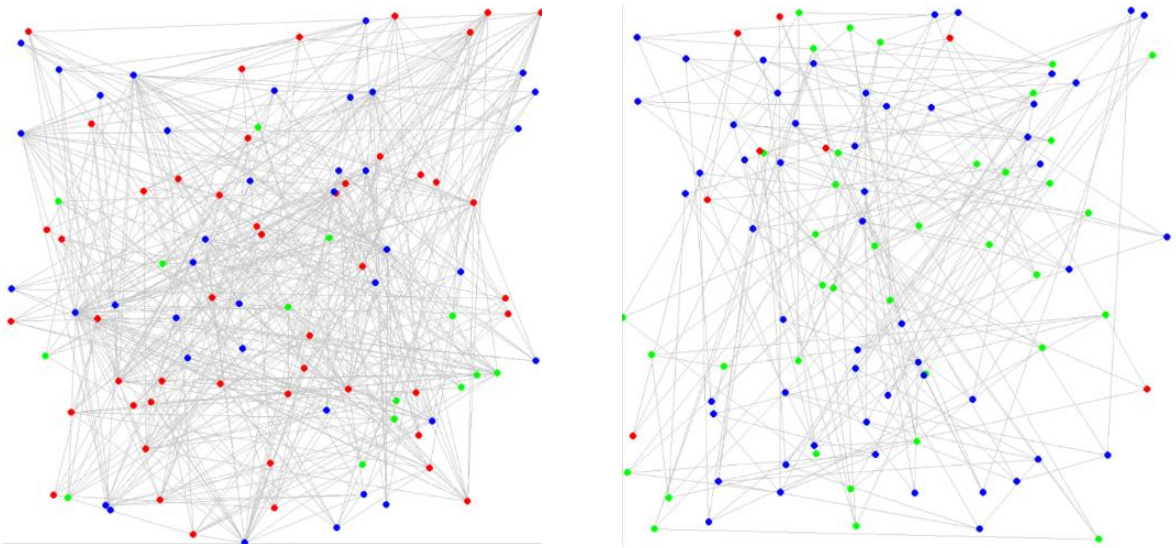
Пунктирна лінія показує, як модель SIR стає моделлю SIRS (Susceptible – Infectious – Recovered – Susceptible), де одужання не надає довічного імунітету, і люди можуть знову стати сприйнятливими.

Рівень зараження, β, контролює швидкість поширення, яка представляє ймовірність передачі захворювання між сприйнятливою та інфікованою особиною. Швидкість одужання, $\gamma = 1/D$, визначається середньою тривалістю інфекції D. У моделі SIRS ξ – швидкість, з якою особи, що одужали, повертаються до чутливого стану з втратою імунітету.

Запропонована модель поширення інформаційних вірусів у соціальній мережі та її емпіричне дослідження

На основі вище наведеного дослідження було розроблено модель соціальної мережі, в якій поширюється інформаційний вірус у вигляді фейку.

Засобами мови програмування Python та бібліотеки Networkx було реалізовано розробку та візуалізацію розробленої моделі (рис. 3).



а б

Рис. 3. Візуалізація запропонованої моделі поширення інформаційних вірусів у соціальній мережі: а) на основі моделей Барабаши-Альберт та SIRS, б) на основі моделей Воттса-Строгаца та SIRS

У моделі SIRS є такі показники: β – це показник того, на скільки користувач мережі сприятливий для прийняття фейку як правдивої інформації; γ – цей показник означає, наскільки швидко користувач перестає вірити цьому фейку; ξ – це швидкість, з якою користувачі, які перестали вірити фейку, знову починають вірити цій інформації під впливом інших користувачів.

В дослідженні розглянуті наступні можливі значення показників моделі SIRS: β – від 0.3 до 0.7, так як цілком захищених від фейків користувачів немає, але і всій інформації повністю користувач не довіряє. Вирішено обрати середнє значення $\beta = 0.5$. Показник γ – від 0.1 до 0.5, адже зазвичай, якщо людина в щось вірить, її важко переконати у іншому. Для моделювання було обрано середнє: $\gamma = 0.3$. Показник ξ – від 0.01 до 0.05, він найменший, тому що, якщо людина перестала вірити фейку, то ймовірність того, що вона знову у нього повірить дуже мала. Обрано середнє – $\xi = 0.03$.

Було проведено серію експериментів з розробленою моделлю та різним комбінаціями її параметрів, результати представлені у табл. 1-2.

Ймовірність p для моделі Воттса-Строгаца обрана стала – 0.1.

Генерувалися мережі зі 100 користувачів, один з яких поширює фейки. Програма виконується певний час, на вибір користувача (обрано 10 секунд).

За допомогою запропонованої моделі ми порівнювали такі критерії: кількість сприятливих до фейку користувачів; кількість заражених (інфікованих) фейком; кількість користувачів, які перестали вірити фейку (одужали); кількість зв’язків між користувачами в мережі, які залишились, після боротьби з фейковими новинами такими способами як: видалення зв’язків між користувачами, створення нового зв’язку, якщо у користувача жодного не залишилось; видалення користувачів з мережі; блокування користувачів; поєднання різних комбінацій із запропонованих способів.

Таблиця 1 – **Результати експериментів для розробленої моделі на основі моделей Барабаши-Альберт та SIRS, початкові параметри: кількість вузлів графа – 100, кількість ребер – 475, β = 0.5, γ = 0.3, ξ = 0.03**

	Сприятливі	**Інфіковані**	**Одужали**	**К-ть зв'язків**	**Сприятливі**	**Інфіковані**	**Одужали**	**К-ть зв'язків**
Вид	*Режим №1. Базовий режим моделювання*				*Режим №4. Наявні додаткові дії: видалення зв'язків і створення нового, якщо зв'язків не залишилось*			
1	17	3	80	475	49	1	50	426
2	16	7	77	475	98	1	1	464
3	12	11	77	475	96	1	3	459
Сер.	15	7	78	475	81	1	18	449.67
Вид	*Режим №2. Наявні додаткові дії: видалення зв'язків і вузлів (користувачів)*				*Режим №5. Наявні додаткові дії: блокування вузлів (користувачів)*			
1	87	0	12	439	11	10	79	475
2	32	7	61	427	16	11	73	475
3	99	0	0	467	20	7	73	475
Сер.	72.67	2.33	24.33	444.33	15.67	9.33	75	475
Вид	*Режим №3. Наявні додаткові дії: видалення зв'язків і вузлів, блокування вузлів (користувачів)*				*Режим №6. Наявні додаткові дії: видалення зв'язків, створення нового, якщо зв'язків не залишилось, і блокування*			
1	92	0	7	423	70	1	29	421
2	98	1	1	470	22	8	70	421
3	99	0	0	461	84	1	15	436
Сер.	96.33	0.33	2.67	451.33	58.67	3.33	38	426

Таблиця 2 – **Результати експериментів для розробленої моделі на основі моделей Воттса-Строгаца та SIRS, початкові параметри: кількість вузлів графа – 100, кількість ребер – 200, β = 0.5, γ = 0.3, ξ = 0.03**

	Сприятливі	**Інфіковані**	**Одужали**	**К-ть зв'язків**	**Сприятливі**	**Інфіковані**	**Одужали**	**К-ть зв'язків**
Вид	*Режим №1. Базовий режим моделювання*				*Режим №4. Наявні додаткові дії: видалення зв'язків і створення нового, якщо зв'язків не залишилось*			
1	30	3	67	200	95	1	4	195
2	46	1	53	200	40	1	59	188
3	39	1	60	200	71	1	28	174
Сер.	38.33	1.67	60	200	68.67	1	30.33	185.67
Вид	*Режим №2. Наявні додаткові дії: видалення зв'язків і вузлів (користувачів)*				*Режим №5. Наявні додаткові дії: блокування вузлів (користувачів)*			
1	99	0	0	196	45	4	51	200
2	99	0	0	196	37	3	60	200
3	99	0	0	194	64	16	20	200
Сер.	99	0	0	195.33	48.67	7.67	43.67	200
Вид	*Режим №3. Наявні додаткові дії: видалення зв'язків і вузлів, блокування вузлів (користувачів)*				*Режим №6. Наявні додаткові дії: видалення зв'язків, створення нового, якщо зв'язків не залишилось, і блокування*			
1	99	0	0	196	96	1	3	194
2	99	0	0	196	98	1	1	194
3	99	0	0	196	98	1	1	197
Сер.	99	0	0	196	97.33	1	1.67	195

Під час *базового режиму* моделювання фейк поширюється мережею без будь-яких обмежень.

Видалення зв'язків – кожен вузол (користувач) в графі (мережі) має декількох сусідів, з якими утворює зв'язок, а так як фейк поширюється від одного користувача до іншого, то видалення між ними зв'язку означає, що користувач перестав вірити своєму сусіду, від якого часто отримував фейки. У дослідженні ми видаляли зв'язок, коли користувач тричі отримав фейк від сусіда.

Створення нового зв'язку – якщо користувач розірвав зв'язки з усіма своїми сусідами, то щоб не видаляти його з мережі, було вирішено додати можливість створення нового зв'язку для нього, за умови, що цей користувач зараз не має ніяких зв'язків.

Видалення вузлів – якщо зв'язків не залишилось, то користувач видаляється (можна обрати лише або цей варіант, або попередній), тобто він повністю втратив довіру до своїх сусідів, або сусіди до нього.

Блокування вузлів – користувач, який повірив фейку деяку кількість разів (в дослідженні – 3 рази), блокується на певний час (в дослідженні – 0.0001 с) для того, щоб його сусіди на деякий час перестали з ним взаємодіяти, через те, що він часто «хворіє».

Висновки

Було розроблено та реалізовано комп'ютерну модель поширення інформаційних вірусів у соціальній мережі з використанням моделей Барабаши-Альберт та Воттса-Строгаца для генерації структури мережі та епідеміологічної моделі SIRS для моделювання поширення вірусної інформації. Запропоновано різні способи моделювання поведінки користувачів у соціальній мережі при поширенні інфор-

маційного вірусу, та різні способи боротьби з ним. Було проведено експерименти з використанням різних запропонованих способів моделювання поведінки користувачів у соціальній мережі. За результатами дослідження можна зробити такі висновки:

– чим більша кількість зв'язків у соціальній мережі, тим легше інформаційному вірусу поширюватися нею;

– ынформаційний вірус поширюється хвилями у соціальній мережі;

– найкращий результат боротьби з інформаційним вірусом у розробленій моделі отримано при комбінуванні таких стратегій захисту користувачів, як видалення зв'язків і вузлів та блокування вузлів при їх підозрілій активності, адже за час роботи моделі у такому режимі вдалось виявити поширювача фейку та видалити його, при цьому кількість зв'язків між користувачами зменшилась не дуже сильно;

– при запропонованій поведінці користувачів (комбінація видалення зв'язків і вузлів та блокування вузлів при їх підозрілій активності) інформаційному вірусу вдається успішно протидіяти;

Запропоновані способи боротьби проти поширенням інформаційного вірусу працюють, і їх можна застосовувати і в реальних соціальних мережах, якщо в них є необхідні умови та механізми.

СПИСОК ЛІТЕРАТУРИ

1. Курбан О. В. Сучасні інформаційні війни в соціальних онлайн-мережах. *Інформаційне суспільство*. 2016. Вип. 23. С. 85-90. URL: http://nbuv.gov.ua/UJRN/is_2016_23_15
2. Мелешко Є. В. Проблеми сучасних рекомендаційних систем та методи їх рішення. *Системи управління, навігації та зв'язку*. 2018. Вип. 4. С. 120-124. URL: http://nbuv.gov.ua/UJRN/suntz_2018_4_25
3. Cinelli M., De Francisci Morales G., Galeazzi A., Quattrociocchi W., Starnini M. The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*. 2021. Vol. 118, No. 9, e2023301118. DOI: https://doi.org/10.1073/pnas.2023301118
4. Rhodes S. C. Filter bubbles, echo chambers, and fake news: how social media conditions individuals to be less critical of political misinformation. *Political communication*. 2022. Vol. 39, No. 1. P. 1-22. DOI: https://doi.org/10.1080/10584609.2021.1910887
5. Chitra U., Musco C. Analyzing the Impact of Filter Bubbles on Social Network Polarization. *In Proceedings of the 13th International Conference on Web Search and Data Mining (WSDM '20), Association for Computing Machinery, New York, NY, USA*. 2020. P.115-123. URL: https://doi.org/10.1145/3336191.3371825
6. Yerlikaya T., Aslan,S. T. Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process. *Insight Turkey*. 2020. Vol. 22, No. 2. P. 177-96. URL: https://www.jstor.org/stable/26918129
7. Динаміка поширення фейків в соціальному просторі. *Портал Медіаосвіти і Медіаграмотності*. 2020. URL: https://medialiteracy.org.ua/dynamika-poshyrennya-fejkiv-v-sotsialnomu-prostori/
8. Newman M. E. J. Networks: An Introduction (1st edn). *Oxford University Press*. 2010. DOI: https://doi.org/10.1093/acprof:oso/9780199206650.001.0001
9. Barabási A.-L., Albert R. Emergence of scaling in random networks. *Science*. 1999. Vol. 286(5439), P. 509-512. DOI: https://doi.org/10.1126/science.286.5439.509
10. Watts D. J., Strogatz S. H. Collective dynamics of 'small-world' networks. *Nature*. 1998. Vol. 393(6684), P. 440-442. DOI: https://doi.org/10.1038/30918
11. SIR and SIRS models. *IDM documentation*. URL: https://docs.idmod.org/projects/emod-generic/en/2.20_a/model-sir.html#sirs-model\

Received (Надійшла) 29.05.2024
Accepted for publication (Прийнята до друку) 31.07.2024

A computer model of information virus propagation in a social network with different user behavior

O. Tkachenko, Ye. Meleshko, V. Mikhav

Abstract. Nowadays, modeling the processes of the spread of information viruses is an important task of cybersecurity, because it is necessary to clearly distinguish where the truth is from where it is fake, to be able to identify the source of the spread of fake news and to counter disinformation in order to convey the truth to people. The purpose of this work was to create and research a computer model of information virus propagation in a social network with different user behavior. The SIRS epidemiological model and the Barabási-Albert and Watts-Strogatz social network structure generation models were used to achieve this goal. The SIRS model is ideal for simulating the spread of a computer virus, because in this model a person can cycle through three states: susceptible, infected, and recovered with immunity, analogous to how a user in a social network can be "infected" to and be "cured" of a fake. Barabási-Albert and Watts-Strogatz algorithms, which are available in the Networkx library of the Python programming language, were used to model the structure of the social network. Several different ways of user behavior have been proposed to protect against information viruses, including removing connections between users, removing users from the network, and blocking users for suspicious activity. An empirical research and comparison of the proposed methods of combating the information virus was carried out according to various criteria. The initial parameters of the network were proposed, namely, the number of users, the number of connections between them, and the coefficients of the SIRS model. Using the Python programming language and the Pygame and Networkx libraries, the proposed model of the spread of an information virus in a social network was implemented and such methods of combating fakes as: deleting connections between users, creating a new connection, deleting users, and blocking users – were simulated. We get the best result in the fight against the information virus when we combine the methods of deleting connections and users, as well as blocking users. With the proposed user behavior, the information virus managed to successfully counteract and detect the spreader of the fake and remove it, while the number of connections between users of the social network decreased not very significantly.

Keywords: social network, information security, fake news, information viruses, SIRS model, Barabási-Albert model, Watts-Strogatz model.