INFORMATION SECURITY

DOI 10.20535/2411-1031.2022.10.2.270403
УДК 004(056.53::738.5)

ВОЛОДИМИР АХРАМОВИЧ

МЕТОД РОЗРАХУНКУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД СЕРЕДНЬОЇ ДОВЖИНИ ШЛЯХУ МІЖ КОРИСТУВАЧАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розроблена математична модель (лінійна система диференціальних рівнянь) та проведено дослідження моделі захисту персональних даних від середньої довжини шляху та інтенсивності передачі даних в соціальних мережах. За дослідженнями виконаними Мілградом найбільша середня довжина шляху між користувачами мережі не перевищує шести. Існує практичний інтерес дослідження поведінки системи захисту соціальних мереж від середньої довжини шляху між користувачами мережі. Теоретичне дослідження динамічної поведінки реального об'єкта вимагає створення його математичної моделі. Процедура розробки моделі полягає в складанні математичних рівнянь на основі фізичних законів. Вказані закони формалізовані диференціальними рівняннями. Розглянуто лінійну систему захисту інформації в соціальних мережах у математичному розумінні цього терміну. У цьому випадку об'єкт, хоча б наближено, повинен бути лінійним. Такий підхід дозволяє достатньо просто розглянути математичні моделі. Якщо таке явище не спостерігається, необхідне дослідження системи захисту на лінійність. Розглянуто залежності величини потоку інформації в соціальній мережі від складових захисту інформації, кількості персональних даних та швидкості потоку даних; захищеності системи від розмірів системи (як і від кількості персональних даних); загроз безпеці інформації від середньої довжини шляху. Отримано рішення – рівняння гармонічного осцилятора, яке розпадається на три випадки: дорезонансна зона, резонансна та зарезонансна. Таким чином, досліджено вплив параметрів середньої довжини шляху між користувачами на параметри системи захисту соціальної мережі. Таке дослідження корисне та важливе з точки зору захисту інформації в мережі, оскільки параметри середньої довжини шляху між користувачами значно впливають, до 100 %, на показник захисту. В результаті досліджень встановлено, що системи захисту соціальної мережі нелінійні.

Ключові слова: соціальна мережа, середня довжина шляху, система захисту, нелінійність, диференціальні рівняння.

Постановка проблеми. Середня довжина шляху в моделі Барабаш–Альберта (БА) збільшується в середньому як логарифм розміру мережі (рис. 1). Точна форма має подвійну логарифмічну поправку і виглядає як:

$$l \sim \frac{\ln N}{\ln \ln N}.$$

де l – довжина шляху між користувачами в соціальній мережі;

N – розмір соціальної мереж.

Модель БА має систематично коротший середній шлях, ніж випадковий граф. Тож постало питання теоретичне та практичне, як дослідити вплив середньої довжини шляху на систему захисту персональних даних в соціальній мережі.

Аналіз останніх досліджень і публікацій. Дослідженню соціальних мереж приділено увагу в [1] - [13]. У [1], [6], [8] досліджується метод розрахунку показника захисту інформації в соціальних мережах від репутації, довіри, та взаємодії користувачів в соціальних мережах.

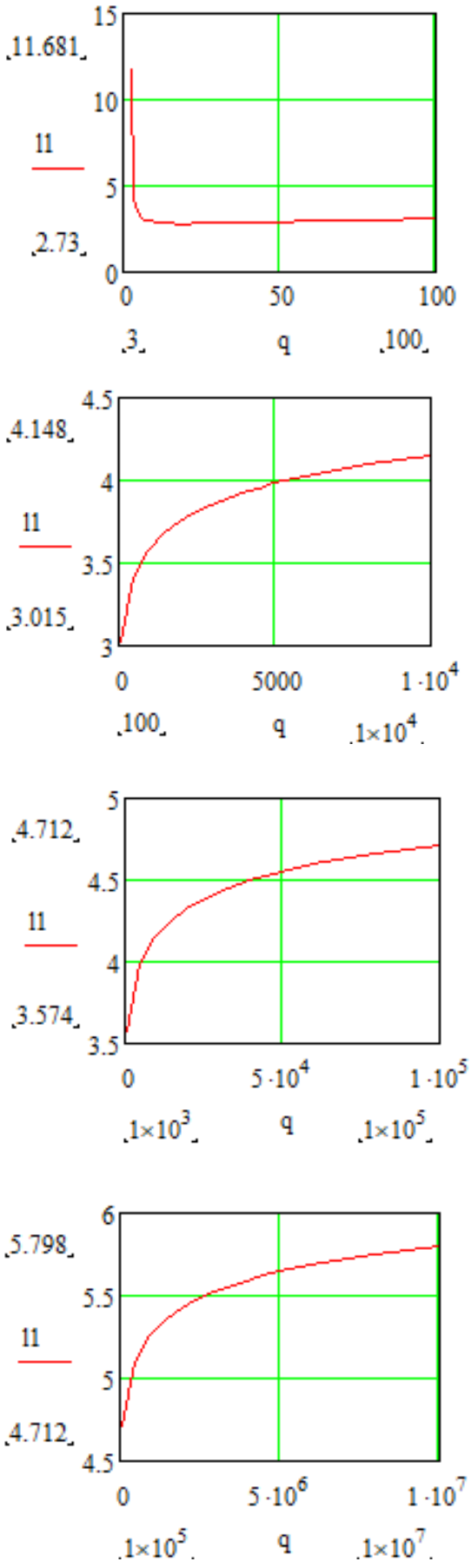

Рисунок 1 – Залежність середньої довжини шляху в моделі БА для степеневих мереж від кількості вузлів, де l_1 – середня довжина шляху, q – кількість вузлів в мережі

У [2] представлена математична теорія інфекційних хвороб та її застосування. У [3], [9] досліджуються комп'ютерні віруси за допомогою теорії та експериментів, а також безпека, епідеміологічна модель поширення вірусу та очищення. У [4] розроблено концептуальний підхід до аналізу онлайн соціальних мереж. Розглянуті питання управління соціальними мережами. В [5] досліджено епідеміологічну модель комп'ютерних вірусів із спрямованим графіком. У [7] досліджуються основні параметри соціальних мереж з отриманням графічних залежностей. Математичні моделі параметрів соціальної мережі представлені з візуалізацією графічних залежностей. У [10] розглянута стохастична поведінка випадкових постійних скануючих черв'яків. У [11], [12] представлено модель поширення чуток SICR (англ. Susceptible – Infective – Counterattack – Refractory) у складних мережах, та аналіз стабільності моделі поширення чуток I2S2R у комплексній мережі. Дослідження нелінійних систем представлено в [13].

Метою статті є дослідження впливу середньої довжини шляху та власних специфічних складових параметрів соціальної мережі на параметри захисту персональних даних.

Виклад основного матеріалу дослідження. Середня довжина шляху в степеневих соціальних мережах моделі БА збільшується в середньому як логарифм розміру мережі. Точна форма має подвійну логарифмічну поправку і виглядає, як: $l \sim \frac{\ln n}{\ln \ln n}$.

У класичному підході до захисту персональних даних розрізняють [4], [5], [11], [12]:

$$T_i = [L_i], \tag{1}$$

де T_i – множина загроз від довжини шляху між користувачами;

L_i – довжина шляху між користувачами.

Втрата такої якості, як довжина шляху між користувачами – процес, який має часовий інтервал. Позначимо кількість інформації в системі – I. Потік інформації за межі інформаційної системи через – dI, швидкість зміни цього потоку – $\frac{dI}{dt}$. Логічно, що якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає [1], [6], [8]:

$$dI = 0; \frac{dI}{dt} = 0. \tag{2}$$

Від чого може залежати витік інформації? Перш за все від захищеності системи – вжитих заходів з нейтралізації загроз безпеці персональних даних [2], [3], [5], [9], [10]. Z – показник захищеності інформаційної системи. Складемо рівняння:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I, \tag{3}$$

де Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації;

C_v – коефіцієнт, що відображає вплив швидкості витоку персональних даних;

C_k – коефіцієнт, що відображає вплив кількості персональних даних на їх витік.

Інтерпретувати дане рівняння можна наступним чином. Витік інформації залежить [1], [6], [8]:

- від розміру інформаційної системи (отже, в якійсь мірі і від кількості персональних даних);
- від швидкості витоку персональних даних;
- витік інформації купірується захищенністю системи (заходами щодо нейтралізації загроз безпеці інформації).

Далі розглянемо, від чого залежить захищеність системи – Z. Визначимо захищеність системи як її здатність протистояти несанкціонованому доступу до персональних даних. Отже, захищеність системи буде залежати:

- від розмірів системи (як і від кількості персональних даних);
- загроз безпеці інформації від приєднання між користувачами.

Складемо рівняння:

$$\frac{dZ}{dt} = \frac{\ln n}{\ln\ln n} + I(C_{d2} + C_{d1}), \tag{4}$$

де n – загальне число вершин графа в момент часу t;

C_{d1} – коефіцієнт, що відображає вплив захищеності на витік інформації;

C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність.

Об'єднаємо рівняння (3) і (4) в систему.

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_k)I, \\ \frac{dZ}{dt} = \frac{\ln n}{\ln\ln n} + I(C_{d1} + C_{d2}). \end{cases} \tag{5}$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (5). Умови стаціонарності $dI = 0; \frac{dI}{dt} = 0$. Отже:

$$\begin{cases} Z_p \overline{Z} + (C_v + C_k)\overline{I} = 0, \\ \frac{\ln n}{\ln\ln n} - I(C_{d1} + C_{d2}) = 0. \end{cases} \tag{6}$$

З другого рівняння системи слідує:

$$\overline{I} = \frac{\ln n}{\ln\ln n(C_{d1} + C_{d2})}. \tag{7}$$

Далі з першого рівняння системи рівнянь (6) знаходимо $\overline{Z}$.

$$Z_p \overline{Z} - \frac{\ln n(C_v + C_k)}{\ln\ln n(C_{d1} + C_{d2})} = 0. \tag{8}$$

$$\overline{Z} = \frac{\ln n(C_v + C_k)}{\ln\ln n(C_{d1} + C_{d2})Z_p} = 0. \tag{9}$$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \overline{I} = \frac{\ln n}{\ln\ln n(C_{d1} + C_{d2})}, \\ \overline{Z} = \frac{\ln n(C_v + C_k)}{\ln\ln n(C_{d1} + C_{d2})Z_p}. \end{cases} \tag{10}$$

Графічні залежності представлено на рис. 2 і 3.

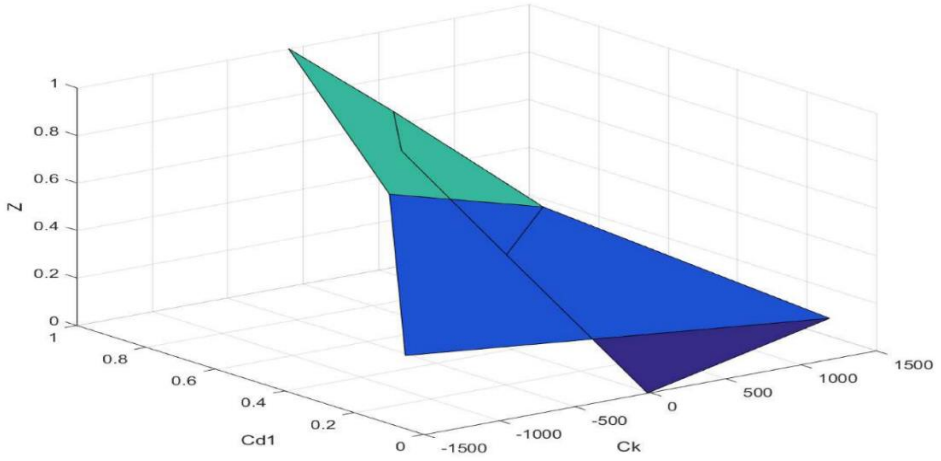

Рисунок 2 – Залежність захисту персональних даних від складових C_{d1} і C_k

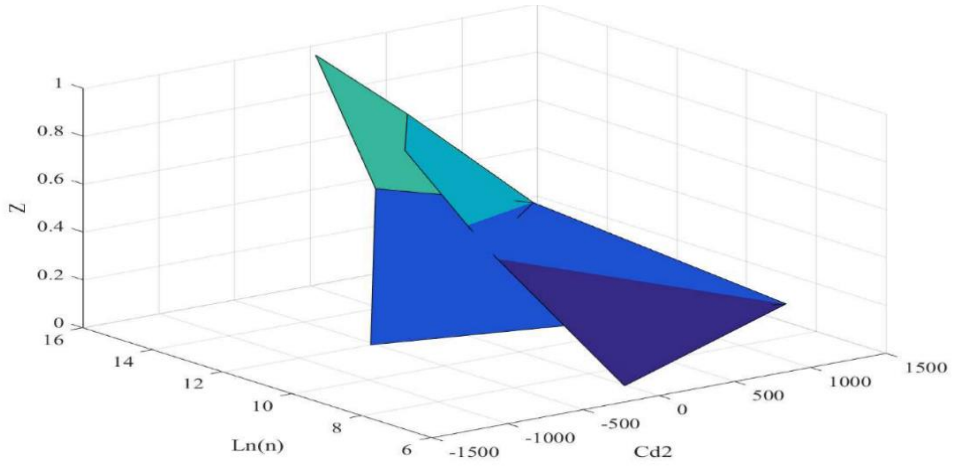

Рисунок 3 – Залежність захисту персональних даних від складових $L_n(n)$ і C_{d2}

Вирішимо систему рівнянь (10) методом “малих відхилень” $I = \bar{I} + I; Z = \bar{Z} + Z$, отже, система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p(\bar{Z} + Z) + (C_v + C_k)(\bar{I} + I), \\ \dfrac{dZ}{dt} = \dfrac{\ln n(C_v + C_k)}{\ln\ln n(C_{d1} + C_{d2})Z_p} - (\bar{I} + I)(C_{d1} + C_{d2}). \end{cases} \tag{11}$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_k)I, \\ \dfrac{dZ}{dt} = -I(C_{d1} + C_{d2}) + \dfrac{\ln n - n}{n(\ln\ln n)^2}(C_v + C_k)_i(C_v + C_k). \end{cases} . \tag{12}$$

Диференціюючи перше рівняння системи (12) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + \frac{\ln n - n}{n(\ln\ln n)^2}(C_v + C_k)) - (C_v + C_k)\frac{dI}{dt}. \tag{13}$$

$$\frac{d^2I}{dt^2} + (C_v + C_k)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + \frac{\ln n - n}{n(\ln\ln n)^2}(C_v + C_k))I = 0. \tag{14}$$

Рівняння (14) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де:

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})\left(Z_p + \frac{\ln n - n}{n(\ln\ln n)^2}\right)}. \tag{15}$$

Графічна залежність представлена на рис. 4.

$$\omega = \sqrt{(C_{d1} + C_{d2})\left(Z_p + \frac{\ln n - n}{n(\ln\ln n)^2} - \frac{(C_v + C_k)^2}{4}\right)}. \tag{16}$$

Графічна залежність представлена на рис. 5.

$$T\frac{2\pi}{\sqrt{(C_{d1} + C_{d2})\left(Z_p + \dfrac{\ln n - n}{n(\ln\ln n)^2}(C_v + C_k) - \dfrac{(C_v + C_k)^2}{4}\right)}}. \tag{17}$$

Графічна залежність представлена на рис. 6.

$$\beta = \frac{C_v + C_k}{2}. \tag{18}$$

Графічна залежність представлена на рис. 7.

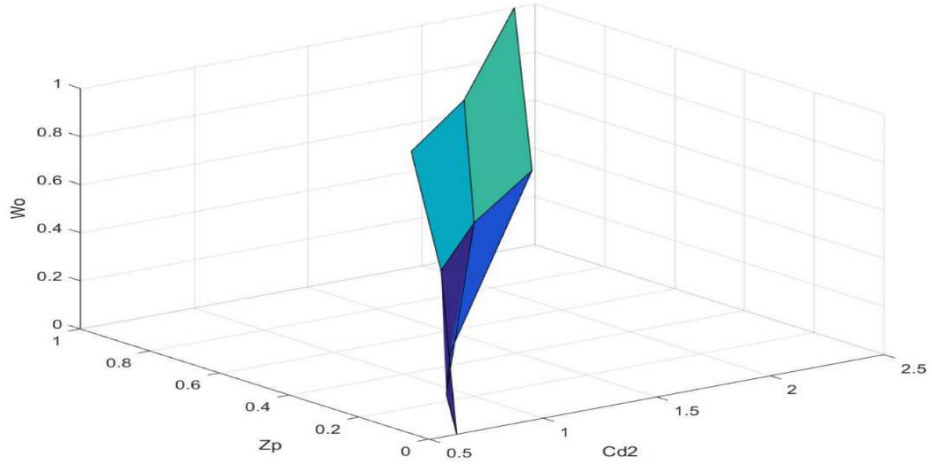

Рисунок 4 – Залежність особистої частоти системи захисту за (15)

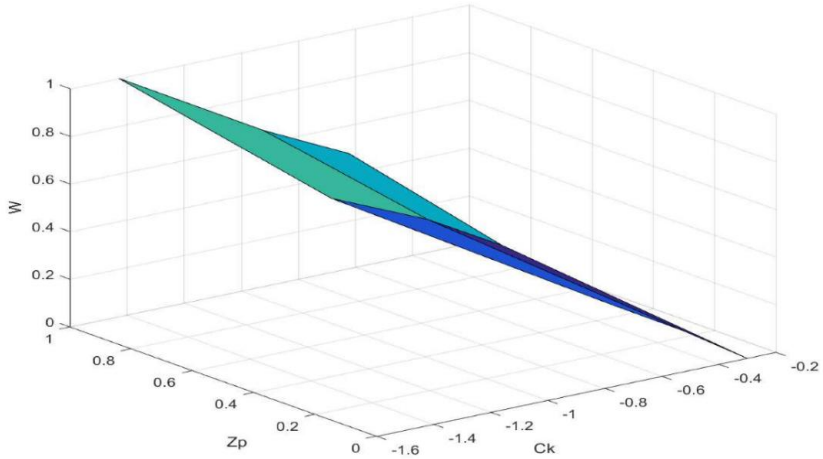

Рисунок 5 – Залежність частоти системи захисту за (16)

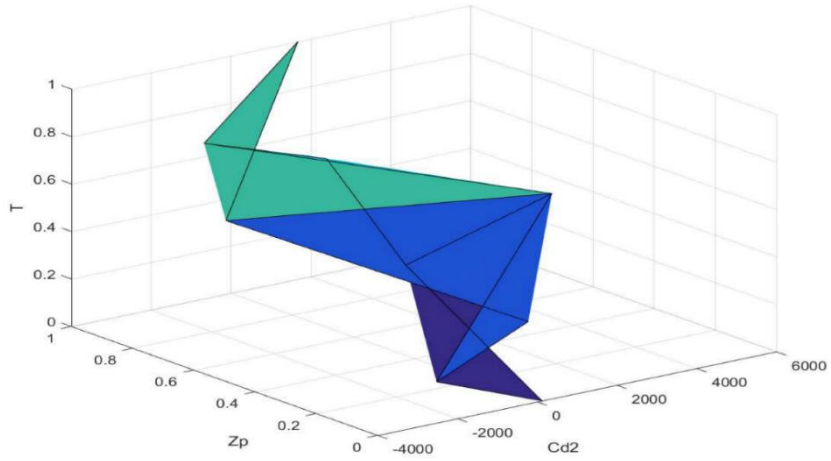

Рисунок 6 – Залежність періоду коливань за (17)

Рішення рівняння гармонічного осцилятора розпадається на три випадки.

1. $$\beta \prec \omega_0 : I = A_0 \exp(-\frac{C_v + C_k}{2} \times \\ \times \cos\left(\sqrt{(C_{d1} + C_{d_2}) + Z_p + \frac{\ln\ln n - n}{n(\ln\ln n)^2}(C_v + C_k) - \frac{(C_v + C_k)^2}{4}} \cdot t + \varphi_0\right). \quad (19)$$

2. $$\beta = \omega_0 : I = A_0 + B_0 t \exp\left(-\frac{C_v + C_k}{2} t\right). \quad (20)$$

3. $$\beta \succ \omega_0 : I = A_0 \exp(-yt) + B_0 \exp\left(-\frac{C_v + C_k}{2} t\right), \quad (21)$$

де $$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_k)^2}{4} - (C_{d1} + C_{d_2} + Z_p + \frac{\ln\ln n - n}{n(\ln\ln n)^2}(C_v + C_k))}.$$

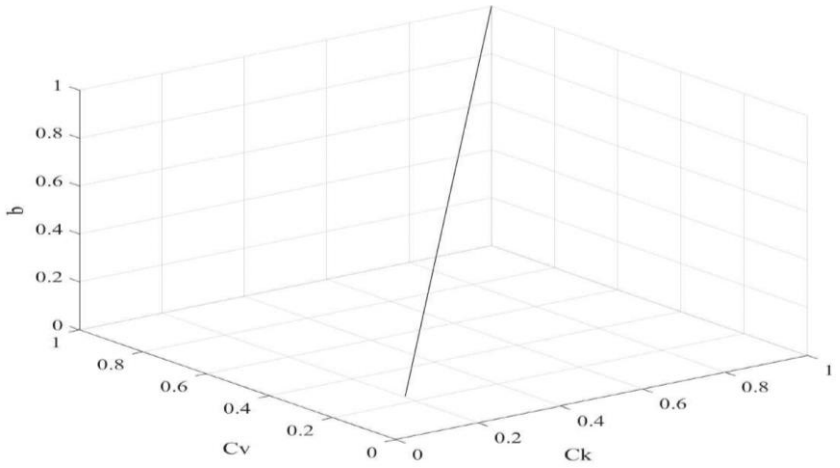

Рисунок 7 – Залежність коефіцієнта затухання за (18)

Розглянувши три варіанти вирішення рівняння близько стаціонарного стану системи, можна прийти до висновку, що, виходячи з умов співвідношення диссипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненціально загасаючим законом [1], [7]. Виконаємо більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь (5), (6) до дискретної і промоделювавши деякий інтервал існування системи, а саме:

$$\begin{cases} \frac{I_{n+1} - I_n}{\Delta t} = (C_{d1} + C_{d2}) Z_n - (C_v + C_k) I_n, \\ \frac{Z_{n+1} - Z_n}{\Delta t} = Z_p - (C_{d1} + C_{d2}) I_n - (Z_p + \frac{\ln\ln n - n}{n(\ln\ln n)^2}(C_v + C_k)(C_v + C_k) I_n). \end{cases} \quad (22)$$

$$\begin{cases} I_{n+1} = I_n + \left(C_{d1} + C_{d2}\right) Z_n - (C_v + C_k) I_n \Delta t, \\ Z_{n+1} = Z_n + \left(Z_n - I_n (C_{d1} + C_{d2} + Z_p + \frac{\ln\ln n - n}{n(\ln\ln n)^2}(C_v + C_k)(C_v + C_k) I_n) \right) \Delta t. \end{cases} \quad (23)$$

Слідуючи з умови стаціонарної позиції системи, I і Z будуть рівні 0,5 і 0,5. Крок моделювання приймемо за 0,1 для всіх ітерацій моделювання, тому в табл. 1 відображати його не будемо. Величини I_{sp}, Z_{sp} відображають стаціонарні значення параметрів, якщо такі були досягнуті за кінцеве число ітерацій. Далі проведемо імітаційне моделювання для значень $\beta \prec \omega_0$, $\beta = \omega_0$, $\beta \succ \omega_0$ з відхиленням від стаціонарної позиції системи (табл. 1).

Візуалізація результатів представлена на рис. 8 - 10. Залежність (1) показує класичний підхід до захисту персональних даних. Отримано систему лінійних диференційних рівнянь (5), яка описувала систему захисту соціальної мережі. Знайдено стаціонарну позицію системи, що відображається системами рівнянь (6), (10). Розв'язок системи рівнянь (5) знайдено методом "малих відхилень" (12). Рівняння гармонічного осцилятора отримано завдяки диференціюванню першого рівняння системи (12). Розв'язок рівняння гармонічного осцилятора (13), (14) розпалося на три випадки, в залежності від співвідношення частоти

системи та коефіцієнта затухання (19) - (21). Було встановлено, що система захисту інформації є нелінійною. Це пояснюється тим, що за межами резонансної області (рис. 10) [13] виявлені незатухаючі коливання системи захисту.

Таблиця 1 – Параметри моделювання

№ з/п	Z_p	I	Z	C_v	C_{d1}	C_{d2}	C_K	n	Параметри
1	0,5	0,5	1	1	1	0,5	1	100000	$\beta \prec \omega_0$
2	0,5	0,5	1	3	1,5	1,5	3	100000	$\beta = \omega_0$
3	0,5	0,5	1	4	1	1	4	100000	$\beta \succ \omega_0$

Особливості запропонованого методу і отриманих результатів полягають в одержанні кількісних показників захисту інформації від специфічних параметрів соціальної мережі, в тому числі, від параметрів середньої довжини шляху між користувачами. Існуючі методи дослідження не дають можливості отримати такі показники. На відміну від попередніх досліджень, отримані результати вказують на нелінійність системи захисту соціальних мереж.

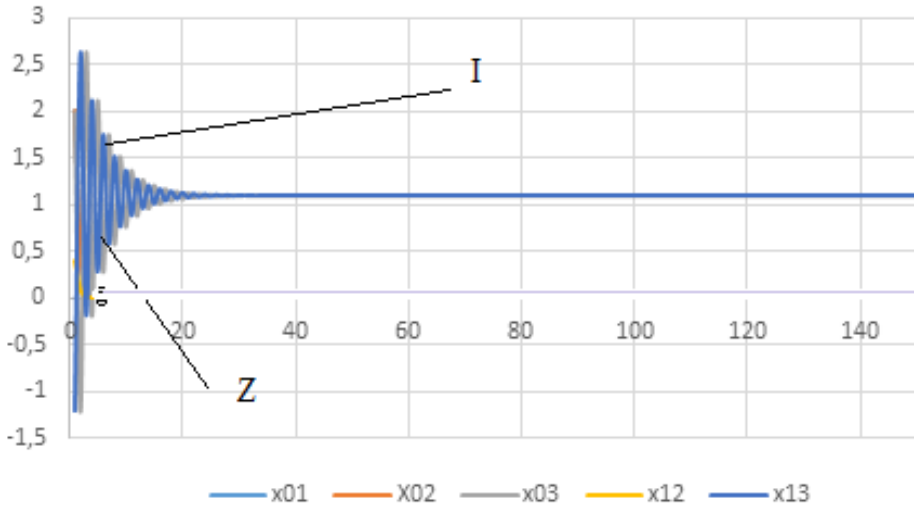

Рисунок 8 – Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140). Дані складових взяті з табл. 1. $\beta \prec \omega_0$, через i позначено кількість ітерацій

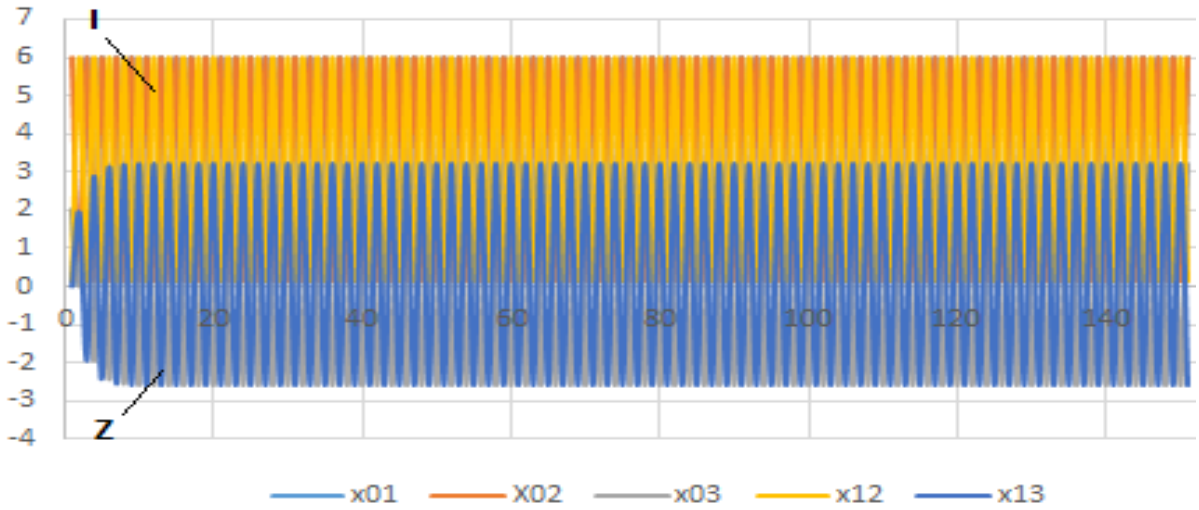

Рисунок 8 – Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140). $\beta = \omega_0$, $D_i = 0.5$

Подальший розвиток даного дослідження полягає у використані відомих специфічних параметрів соціальних мереж (взаємовпливу, розширення мереж, коефіцієнта кластеризації, поширення інформації, центральності мережі тощо), виявленні нових факторів та параметрів.

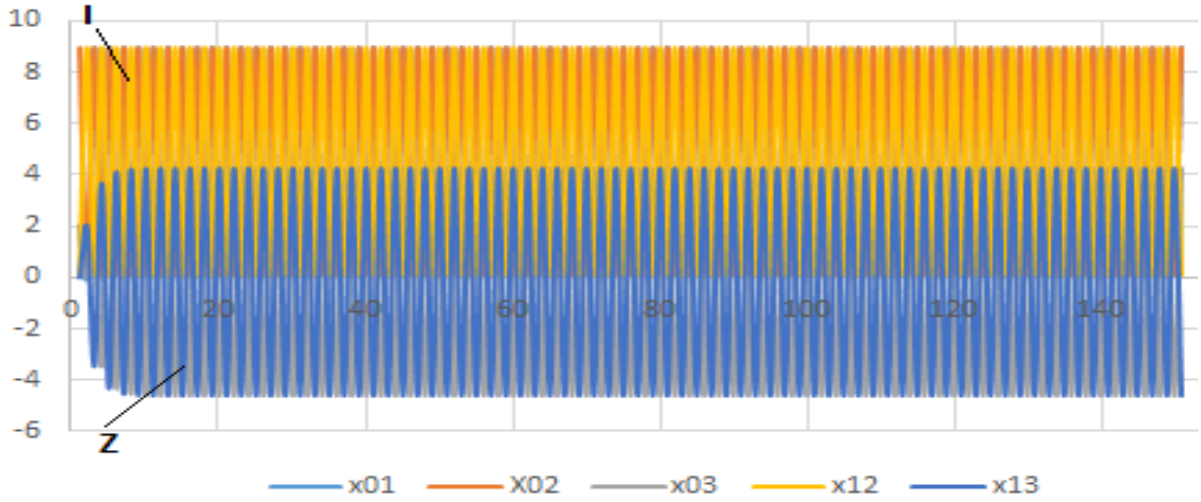

Рисунок 10 – Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140). $\beta \succ \omega_0$, $D_i = 0.1$

Висновки. Дослідження лінійної моделі впливу середньої відстані між користувачами в соціальних мережах на систему захисту сприяло переходу від класичного підходу до систем диференціальних рівнянь, що дозволило отримати математичні залежності між специфічними параметрами соціальної мережі, в тому числі середньої відстані між користувачами та показником захисту. В результаті дослідження отримані рівняння гармонічного осцилятора з затухаючою амплітудою. Завдяки цьому визначено частоти коливань, період, коефіцієнт затухання системи захисту. Отримано математичні залежності поведінки системи захисту в дорезонансній, резонансній та післярезонансних областях. Такий підхід дозволив перейти до дослідження лінійності системи захисту.

Перевірка на лінійність системи захисту інформації вказала на її нелінійність. Це доведено шляхом розгляду трьох варіантів розв'язку рівняння осцилятора близько стаціонарного стану системи. Зауважено, що виходячи з умов співвідношення дисипації і власної частоти коливань величини, затухання останньої, до певного значення, здійснюється періодично. Амплітуда коливань є затухаючою амплітудою за експоненціально загасаючим законом. Виконано більш наочний аналіз поведінки системи шляхом переходу від диференціальної форми рівнянь до дискретної і моделювання інтервалу існування системи. В результаті аналізу ітерації коливань системи захисту виявлено її нелінійність. Це дозволить перейти до дослідження нелінійної системи захист персональних даних соціальної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] V. Akhramovich, A. Hrebennikov, B. Tsarenko, and O. Stefurak, "Method of calculating the protection of personal data from the reputation of users", *Sciences of Europe*, vol. 1, no. 80, pp. 23-31, 2021.

[2] N. Bailey, *The mathematical theory of infectious diseases and its applications*. New York : Hafner Press, 1975.

[3] F. Cohen, "Computer viruses, theory and experiments", *Computers & Security*. vol. 6, iss. 1, pp. 22-35, 1987, doi: https://doi.org/10.1016/0167-4048(87)90122-2.

[4] D. Gubanov, and A. Chkhartishvili, “A conceptual approach to the analysis of online social networks”, *Automation and Remote Control*, vol. 76, iss. 8, pp. 1455-1462, 2015, doi: https://doi.org/10.1134/S000511791508010X.
[5] J. Kephart, and S. White, “Directed-graph epidemiological model of computer viruses”, in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1991, pp. 343.
[6] O. Laptiev, V. Savchenko, A. Kotenko, V. Akhramovych, V. Samosyuk, G. Shuklin, and A. Biehun, “Method of determining trust and protection of personal data in social networks”, *International Journal of Communication Networks and Information Security* (*IJCNIS*), vol. 13, no. 1, pp. 15-21, 2021, doi: https://doi.org/10.17762/ijcnis.v13i1.4882.
[7] P. Shchypanskyi, V. Savchenko, V. Akhramovych, T. Muzshanova, S. Lehominova, and V. Chegrenets, “The model of secure social networks activity based on graph theory”, *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), vol. 9, iss. 4, pp. 1803-1810, 2020, doi: https://doi.org/10.35940/ijitee.D1768.029420.
[8] V. Akhramovych, G. Shuklin, Y. Pepa, T. Muzhanova, and S. Zozuli, “Devising a procedure to determine the level of informational space security in social networks considering interrelations among users”, *Eastern European Journal of Advanced Technologies*, vol. 1, no. 9 (115), pp. 63-74, 2022, doi: https://doi.org/10.15587/1729-4061.2022.252135.
[9] M. M. Williamson, and L. Jasmin, “An epidemiological model of virus spread and cleanup”, Hewlett-Packard Laboratories, 2003. [Online]. Available: https://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf. Accessed on: May 29, 2022.
[10] Y. Zan, J. Wu, P. Li, and Q. Yu, “SICR rumor spreading model in complex networks: counterattack and self-resistance”, *Physica A: Statistical Mechanics and its Applications*, vol. 405, pp. 159-170, 2014, doi: https://doi.org/10.1016/j.physa.2014.03.021.
[11] Y. Zhang, and J. Zhu, “Stability analysis of I2S2R rumor spreading model in complex networks”, *Physica A: Statistical Mechanics and its Applications*, vol. 503, pp. 862-881, 2018.
[12] N. Zhao, and X. Cheng, “Impact of information spread and investment behavior on the diffusion of internet investment products”, *Physica A: Statistical Mechanics and its Application*s, vol. 512, pp. 427-436, 2018, doi: https://doi.org/10.1016/j.physa.2018.08.075.
[13] Д. И. Трубецков, *Введение в синергетику. Хаос и структуры*. Москва: Едиториал УРСС, 2004.

Стаття надійшла до редакції 20.09.2022.

REFERENCE

[1] V. Akhramovich, A. Hrebennikov, B. Tsarenko, and O. Stefurak, “Method of calculating the protection of personal data from the reputation of users”, *Sciences of Europe*, vol. 1, no. 80, pp. 23-31, 2021.
[2] N. Bailey, *The mathematical theory of infectious diseases and its applications*. New York : Hafner Press, 1975.
[3] F. Cohen, “Computer viruses, theory and experiments”, *Computers & Security*. vol. 6, iss. 1, pp. 22-35, 1987, doi: https://doi.org/10.1016/0167-4048(87)90122-2.
[4] D. Gubanov, and A. Chkhartishvili, “A conceptual approach to the analysis of online social networks”, *Automation and Remote Control*, vol. 76, iss. 8, pp. 1455-1462, 2015, doi: https://doi.org/10.1134/S000511791508010X.
[5] J. Kephart, and S. White, “Directed-graph epidemiological model of computer viruses”, in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1991, pp. 343.
[6] O. Laptiev, V. Savchenko, A. Kotenko, V. Akhramovych, V. Samosyuk, G. Shuklin, and A. Biehun, “Method of determining trust and protection of personal data in social networks”,

International Journal of Communication Networks and Information Security (*IJCNIS*), vol. 13, no. 1, pp. 15-21, 2021, doi: https://doi.org/10.17762/ijcnis.v13i1.4882.

[7] P. Shchypanskyi, V. Savchenko, V. Akhramovych, T. Muzshanova, S. Lehominova, and V. Chegrenets, "The model of secure social networks activity based on graph theory", *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), vol. 9, iss. 4, pp. 1803-1810, 2020, doi: https://doi.org/10.35940/ijitee.D1768.029420.

[8] V. Akhramovych, G. Shuklin, Y. Pepa, T. Muzhanova, and S. Zozuli, "Devising a procedure to determine the level of informational space security in social networks considering interrelations among users", *Eastern European Journal of Advanced Technologies*, vol. 1, no. 9 (115), pp. 63-74, 2022, doi: https://doi.org/10.15587/1729-4061.2022.252135.

[9] M. M. Williamson, and L. Jasmin, "An epidemiological model of virus spread and cleanup", Hewlett-Packard Laboratories, 2003. [Online]. Available: https://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf. Accessed on: May 29, 2022.

[10] Y. Zan, J. Wu, P. Li, and Q. Yu, "SICR rumor spreading model in complex networks: counterattack and self-resistance", *Physica A: Statistical Mechanics and its Applications*, vol. 405, pp. 159-170, 2014, doi: https://doi.org/10.1016/j.physa.2014.03.021.

[11] Y. Zhang, and J. Zhu, "Stability analysis of I2S2R rumor spreading model in complex networks", *Physica A: Statistical Mechanics and its Applications*, vol. 503, pp. 862-881, 2018.

[12] N. Zhao, and X. Cheng, "Impact of information spread and investment behavior on the diffusion of internet investment products", *Physica A: Statistical Mechanics and its Application*s, vol. 512, pp. 427-436, 2018, doi: https://doi.org/10.1016/j.physa.2018.08.075.

[13] D. Trubetskov, *Introduction to synergetics. Chaos and Structures*. Moscow: Editorial URSS, 2004.

VOLODYMYR AKHRAMOVYCH

METHOD OF CALCULATION OF PROTECTION OF INFORMATION FROM THE AVERAGE LENGTH OF THE ROAD BETWEEN USERS IN SOCIAL NETWORKS

A mathematical model (linear system of differential equations) was developed and a study of the model of personal data protection from the average path length and intensity of data transmission in social networks was conducted. According to research conducted by Milgrad, the maximum average path length between network users does not exceed six. There is a practical interest in studying the behavior of the system of protection of social networks from the average path length between network users. Theoretical study of the dynamic behavior of a real object requires the creation of its mathematical model. The procedure for developing a model is to compile mathematical equations based on physical laws. These laws are formulated in the language of differential equations. The linear system of information protection in social networks in the mathematical sense of this term is considered. When describing linear models, the object must be at least approximately linear. This approach allows you to easily consider mathematical models. If such a phenomenon is not observed, it is necessary to study the protection system for linearity. Dependencies are considered: the amount of information flow in the social network from the components of information protection, the amount of personal data, and the speed of data flow; security of the system from the size of the system (as well as from the amount of personal data); information security threats from medium path length. A solution is obtained – the equation of a harmonic oscillator, which is divided into three cases: preresonance zone, resonance and afterresonance. Thus, the influence of the parameters of the average path length between users on the parameters of the social network protection system is investigated. Such research is

useful and important from the point of view of information protection in the network, as the parameters of the average path length between users significantly affect, up to 100%, the protection rate. As a result of research it is established that social network protection systems are nonlinear.

Key words: social network, average path length, protection system, nonlinearity, differential equations.

Ахрамович Володимир Миколайович, доктор технічних наук, старший науковий співробітник, професор кафедри систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, Київ, Україна, ORCID 0000-0002-6174-5300, 12z@ukr.net.

Akhramovych Volodymyr, doctor of technical sciences, senior research fellow, professor at the department of information and cyber defense systems academic department, State university of telecommunications, Kyiv, Ukraine.