INFORMATION SECURITY

DOI 10.20535/2411-1031.2023.11.1.279868
УДК 004.738.5

ВОЛОДИМИР АХРАМОВИЧ

МЕТОД РОЗРАХУНКУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ В ЗАЛЕЖНОСТІ ВІД КІЛЬКОСТІ СПІВТОВАРИСТВ

Розроблена математична модель (лінійна система дифенціальних рівнянь) та проведено дослідження моделі захисту персональних даних від кількості співтовариств та інтенсивності передачі даних в соціальних мережах. Розглянуто лінійна системи захисту інформації в соціальних мережах у математичному розумінні цього терміну. При описі лінійними моделями об'єкт, хоча б приблизно, має бути лінійним. Такий підхід дозволяє достатньо просто розглянути математичні моделі. Якщо таке явище не спостерігається, необхідне дослідження системи захисту на лінійність. Досліджено 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 безпеки інформації від кількості співтовариств, а також враховано: враховано: Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації; C_v – коефіцієнт, що відображає вплив швидкості витоку даних; C_k – коефіцієнт, що відображає вплив кількості даних на їх витік, C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність; C_{d1} – коефіцієнт, що відображає вплив захищеності на витік даних; m_k – кількість зв'язків у соціальних мережах; n_k – кількість вершин у соціальних мережах; α – параметр α може служити для налагодження алгоритму розбиття мережі. Отримано рішення – рівняння гармонічного осцилятора, яке розпадається на три випадки: дорезонансна зона, резонансна та зарезонансна. Таким чином, досліджено вплив параметрів кількості співтовариств на параметри системи захисту соціальної мережі. Таке дослідження корисне та важливе з точки зору захисту інформації в мережі, оскільки параметри кількості співтовариств значно впливають, до 100 %, на показник захисту. В результаті досліджень встановлено, що системи захисту соціальної мережі нелінійні.

Ключові слова: соціальна мережа, кількості співтовариств, система захисту, нелінійність, диференціальні рівняння.

Постановка проблеми. Перша причина розбиття мережі на підмережі полягає в тому, щоб не отримати величезний broadcast домен. Другою важливою причиною поділу мережі на підмережі є забезпечення певного рівня безпеки.

Графи, що представляють реальні соціальні та комунікаційні мережі, швидко змінюються, при цьому ефективним інструментом їх вивчення служать випадкові графи. Важливим завданням є виділити структуру спільнот в мережах. В умовах великої розмірності мереж особливо актуальні наближені методи, які дозволяють за обмежений час знаходити рішення, близьке до оптимального.

В [1] запропоновано метод виділення структури спільнот на основі методу максимальної правдоподібності, і на його основі описаний чисельний алгоритм випадкового пошуку з використанням розподілу Больцмана-Гіббса.

Розбиття П*, для якого функція П досягає максимуму за всіма можливими розбиття, названо оптимальним.

Вказано, що метод максимальної правдоподібності зводиться до задачі максимізації цільової функції. Для знаходження максимуму цільової функції застосовано підхід, заснований на методах статистичної термодинаміки, а саме моделювання випадкової конфігурації П з розподілом Больцмана (Гіббса).

У даній статті описана математична модель, в якій граф генерується випадковим чином із заданими параметрами для внутрішніх і зовнішніх зв'язків між вершинами, а спільноти покладаються непересічними.

Під ітерацією алгоритму будемо розуміти n оновлень вершин. Відомо, що випадкове блукання, описане імовірнісним розподілом, за тривалий час призведе систему в стійку конфігурацію.

Метод максимальної правдоподібності зведено до задачі максимізації цільової функції (1). Відзначимо, що ця функція є потенціал в гедонічній грі, пов'язаної з графом.

$$P(\Pi) = \sum_{k=1}^{K} m_k - \frac{1}{2}\sum_{k=1}^{K} n_k^2 \alpha\,, \tag{1}$$

де: m_k – кількість зв'язків між вершинами в соціальній мережі, n_k – кількість вершин в соціальній мережі, параметр α може служити для налагодження алгоритму розбиття мережі. Так, в [1] розглянуті два граничних випадки $\alpha \to 0$ і $\alpha \to 1$ і доведено, що в першому з них максимум цільової функції досягається на розбитті графа, в ігровій постановці відповідній гранд-коаліції ΠN = {N}, а в другому – розбитті графа на максимальні кліки.

Постало питання теоретичне та практичне, як дослідити вплив кількості співтовариств на систему захисту персональних даних в соціальній мережі.

Аналіз останніх досліджень і публікацій. В статті [1] досліджено утворення (розбиття) соціальної мережі на співтовариства на основі методу максимальної правдоподібності з максимізацією цільової функції. Застосовано підхід, заснований на методах статистичної термодинаміки, а саме моделювання випадкової конфігурації П з розподілом Больцмана (Гіббса).

В роботі [2] представлена математична теорія інфекційних хвороб та її застосування. В статтях [3], [9] досліджуються комп'ютерні віруси, в вигляді теорії та експериментів, а також безпека. Епідеміологічна модель поширення вірусу та очищення. В статті [4] розроблено концептуальний підхід до аналізу онлайн соціальних мереж. Розглянуті питання управління соціальними мережами.

В роботі [5] досліджено епідеміологічну модель комп'ютерних вірусів із спрямованим графом.

В статті [6] - [8] досліджується метод розрахунку показника захисту інформації в соціальних мережах від репутації, довіри, розповсюдження та взаємодії користувачів в соціальних мережах.

В статті [10] розглянута стохастична поведінка випадкових постійних скануючих черв'яків. В статтях [11], [12] представлено модель поширення чуток SICR у складних мережах, та аналіз стабільності моделі поширення чуток I2S2R у комплексній мережі. Дослідження нелінійних систем представлено в роботі [13].

Метою статті є дослідження впливу кількості співтовариств та власних специфічних складових параметрів соціальної мережі на параметри захисту персональних даних.

Виклад основного матеріалу дослідження.

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

$$T_i = \left[\Pi_i\right], \tag{2}$$

де T_i – множина загроз від кількості співтовариств, Π_i – кількість співтовариств в соціальній мережі.

Втрата такої якості, як співтовариства Π_i – процес, який має часовий інтервал [4], [7], [11]. 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:

$$dI = 0; \frac{dI}{dt} = 0 . \tag{3}$$

Від чого може залежати витік інформації? Перш за все від захищеності системи – вжитих заходів з нейтралізації загроз безпеки даних. Z – показник захищеності інформаційної системи. Складемо рівняння:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I , \tag{4}$$

де Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації; C_v – коефіцієнт, що відображає вплив швидкості витоку даних; C_k – коефіцієнт, що відображає вплив кількості даних на їх витік.

Інтерпретувати дане рівняння можна наступним чином. Витік інформації залежить:

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

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

– від розмірів системи (як і від кількості даних);
– загроз безпеки інформації від втрати зв'язків між користувачами.

Складемо рівняння:

$$\frac{dZ}{dt} = \sum_{k=1}^{K} m_k - \frac{1}{2} \sum_{k=1}^{K} n_k^2 \alpha - I(C_{d2} + C_{d1}) , \tag{5}$$

де C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність; C_{d1} – коефіцієнт, що відображає вплив захищеності на витік даних; m_k – кількість зв'язків в СМ; n_k – кількість вершин в соціальній мережі (СМ); α – параметр α може служити для налагодження алгоритму розбиття мережі.

Так, в [1] розглянуті два граничних випадки $\alpha \to 0$ і $\alpha \to 1$ і доведено, що в першому з них максимум цільової функції досягається на розбитті графа, в ігровій постановці відповідній гранд-коаліції $\Pi N = \{N\}$, а в другому – розбитті графа на максимальні кліки. Об'єднаємо рівняння (3) і (4) в систему.

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = \sum_{k=1}^{K} m_k - \frac{1}{2} \sum_{k=1}^{K} n_k^2 \alpha_i - I(C_{d2} + C_{d1}) \end{cases} . \tag{6}$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (6). Умови стаціонарності $dI = 0, \frac{dI}{dt} = 0$. Отже:

$$\begin{cases} Z_p \bar{Z} + (C_v + C_K) \bar{I} = 0 \\ \sum_{k=1}^{K} m_k - \frac{1}{2} \sum_{k=1}^{K} n_k^2 \alpha_i - I(C_{d2} + Cd_1) = 0 \end{cases} . \tag{7}$$

З другого рівняння системи слідує:

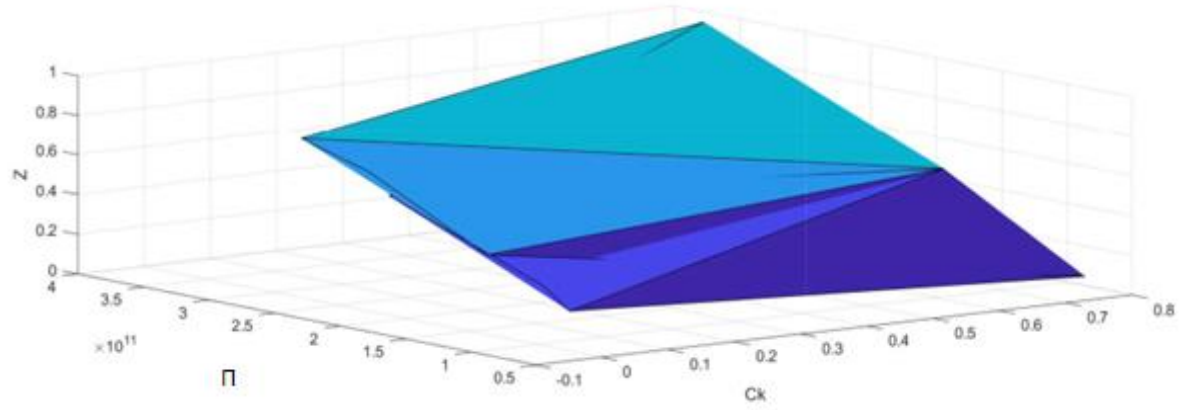
$$\bar{I} = \frac{\sum_{k=1}^{K} m_k - \frac{1}{2}\sum_{k=1}^{K} n_k^2 \alpha_i}{(C_{d2} + C_{d1})}. \quad (8)$$

Далі з першого рівняння системи рівнянь (7) знаходимо $\bar{Z}$ (рис. 1).

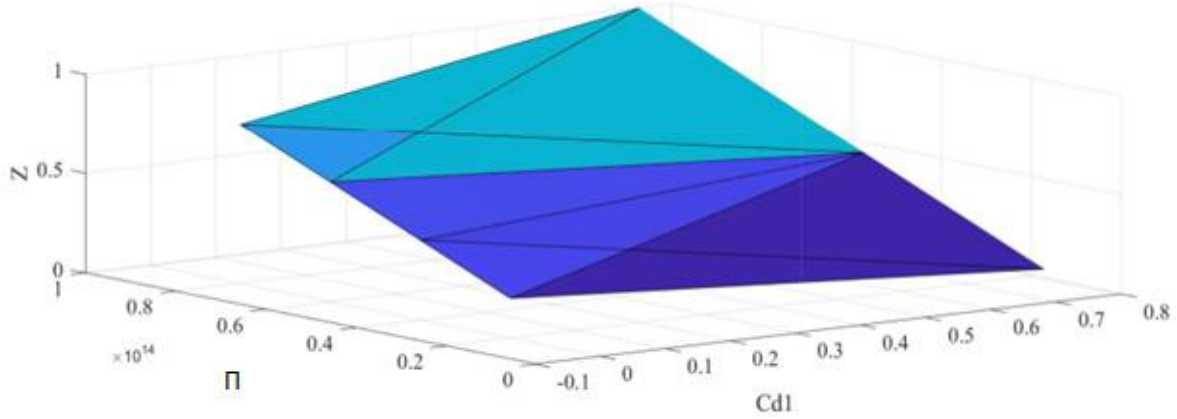
$$Z_p \bar{Z} - \frac{(C_v + C_K)(\sum_{k=1}^{K} m_k - \frac{1}{2}\sum_{k=1}^{K} n_k^2 \alpha)}{(C_{d2} + C_{d1})} = 0. \quad (9)$$

$$\bar{Z} = \frac{(C_v + C_K)(\sum_{k=1}^{K} m_k - \frac{1}{2}\sum_{k=1}^{K} n_k^2 \alpha)}{(C_{d2} + C_{d1}) Z_p}. \quad (10)$$

Введемо позначення $\sum_{k=1}^{K} m_k - \frac{1}{2}\sum_{k=1}^{K} n_k^2 \alpha = П$.



а)



б)

Рисунок 1 – Результати обрахунків за рівнянням (10):
а) – для $n = 100000, m = 500000$
б) – для $n = 1000000, m = 5000000$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \dfrac{\sum\limits_{k=1}^{K} m_k - \dfrac{1}{2}\sum\limits_{k=1}^{K} n_k^2 \alpha_i}{C_{d2} + Z_p} \\ \bar{Z} = \dfrac{(C_v + C_K)(\sum\limits_{k=1}^{K} m_k - \dfrac{1}{2}\sum\limits_{k=1}^{K} n_k^2 \alpha_i)}{(C_{d2} + C_{d1}) Z_p} \end{cases}. \quad (11)$$

Вирішимо систему рівнянь (6) методом «малих відхилень»: $I = \bar{I} + I; Z = \bar{Z} + Z$. Отже, система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p(\bar{Z} + Z) + (C_v + C_K)(\bar{I} + I) \\ \dfrac{dZ}{dt} = (\sum\limits_{k=1}^{K} m_k - \dfrac{1}{2}\sum\limits_{k=1}^{K} n_k^2 \alpha) - (\bar{I} + I)(C_{d2} + C_{d1}) \end{cases}. \quad (12)$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + (\sum\limits_{k=1}^{K} m_k - \dfrac{1}{2}\sum\limits_{k=1}^{K} n_k^2 \alpha_i) \end{cases}. \quad (13)$$

Диференціюючи перше рівняння системи (13) отримуємо (рис. 2):

$$\frac{d^2 I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha) - (C_v + C_K)\frac{dI}{dt}. \quad (14)$$

$$\frac{d^2 I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha)I = 0. \quad (15)$$

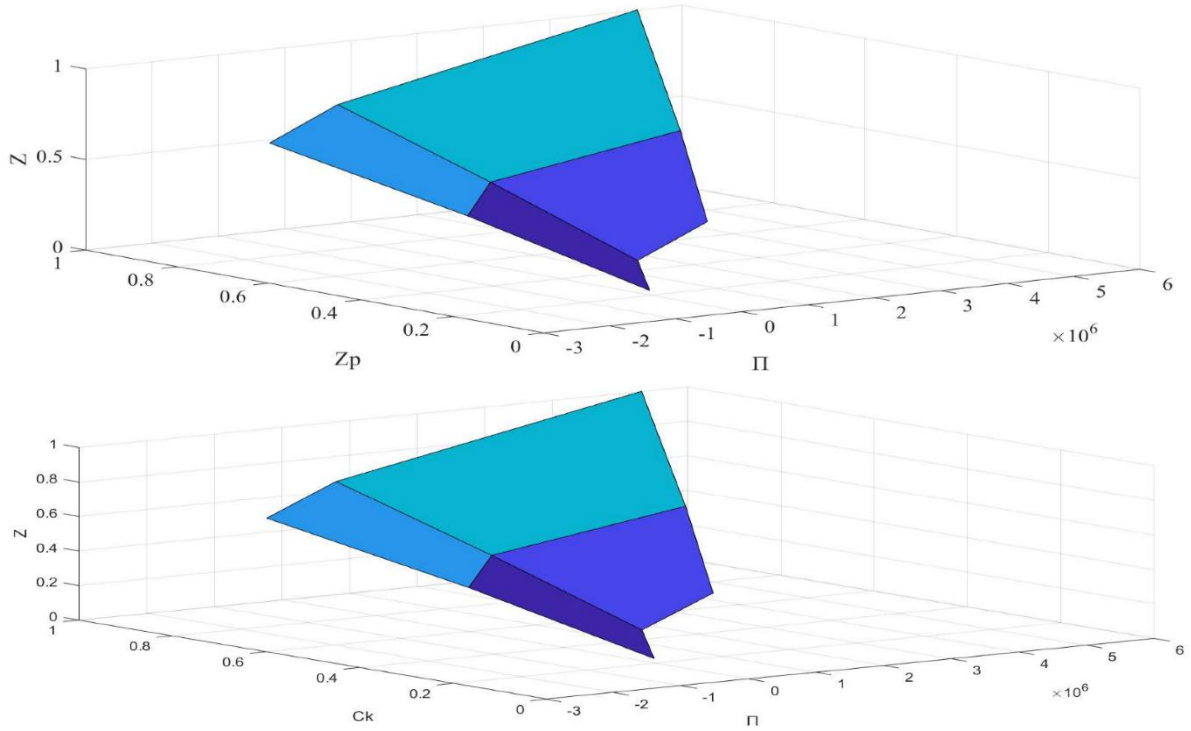


Рисунок 2 – Значення показника захисту від складових за (15) при $n = 100000, m = 500000$

Рівняння (15) є рівнянням гармонічного осцилятора з затухаючою амплітудою [3], де (рис. 3, 4)

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})(Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha)}\,. \tag{16}$$

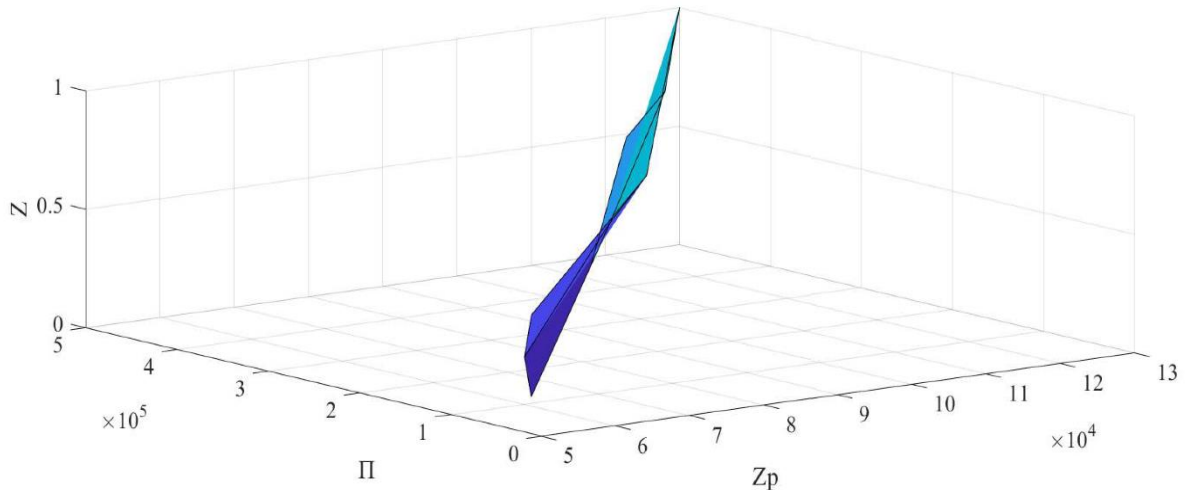


Рисунок 3 – Особиста частота системи захисту при $n = 100000, m = 500000$

$$\omega = \sqrt{(C_{d1} + C_{d2})(Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha) - \frac{(C_v + C_K)^2}{4}}\,. \tag{17}$$

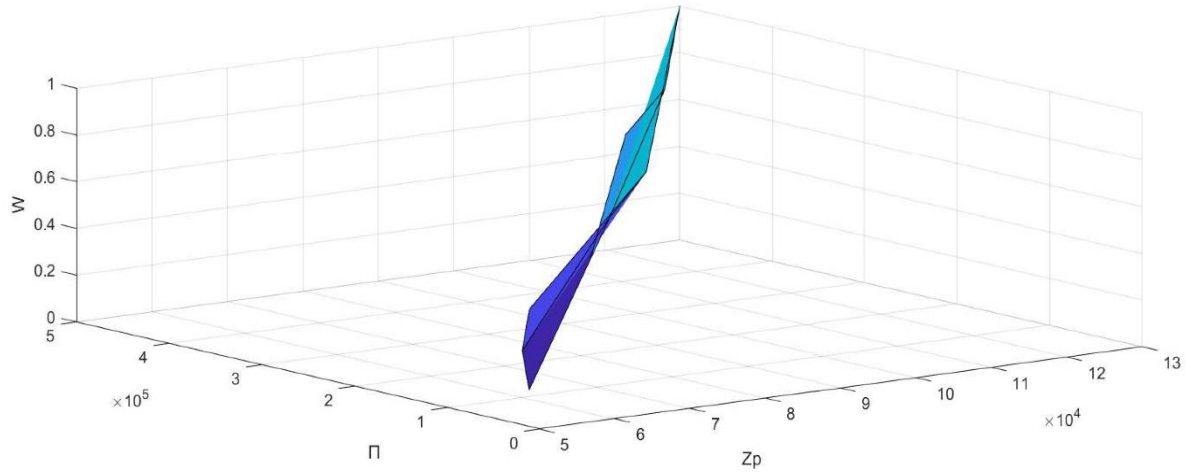


Рисунок 4 – Частота системи захисту при $n = 100000, m = 500000$

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2})(Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha) - \frac{(C_v + C_K)^2}{4}}}\,. \tag{18}$$

$$\beta = \frac{(C_v + C_K)}{2}\,. \tag{19}$$

Рішення рівняння гармонічного осцилятора розпадається на три випадки (рис. 5).

$$\beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2} \cos(\sqrt{(C_{d1} + C_{d2} + Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha) - \frac{(C_v + C_K)^2}{4}} t + \varphi_0)\,. \tag{20}$$

$$\beta = \omega_0 : I = (A_0 + B_0 t \exp(-\frac{(C_v + C_K}{2} t)\,. \tag{21}$$

$$\beta \succ \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t)$$

де .

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha)} \quad (22)$$

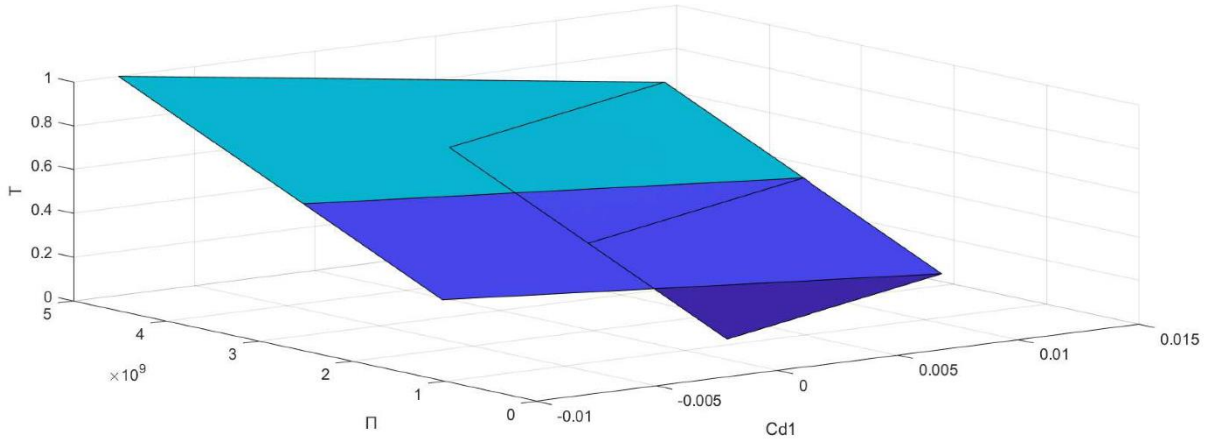


Рисунок 5 – Період коливань системи захисту при $n = 100000, m = 500000$

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], [3], [13]. Виконаємо більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь (5), (6) до дискретної і промоделювавши деякий інтервал існування системи. А саме:

$$\begin{cases} \frac{I_{n+1} - I_n}{\Delta t} = (C_{d1} + C_{d2}) Z_n - (C_v + C_K) I_n) \\ \frac{Z_{n+1} - Z_n}{\Delta t} = Z_p - (C_{d2} + C_{d1}) I_n - (Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha) I_n) \end{cases} . \quad (23)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1} + C_{d2}) Z_n - (C_v + C_K) I_n) \Delta t \\ Z_{n+1} = Z_n + (Z_n - I_n (C_{d2} + C_{d1} + Z_p + \sum_{k=1}^{K} m_k - \sum_{k=1}^{K} n_k \alpha)) \Delta t \end{cases} . \quad (24)$$

Спочатку приймемо коефіцієнти $C_{d1}, C_v, C_{d2}, Z_p, C_k, \Pi$ за одиницю. 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 таблиці 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 $\beta \prec \omega_o, \beta = \omega_o, \beta \succ \omega_o$ з відхиленням від стаціонарної позиції системи. Дані представимо в табл. 1 .

Таблиця 1 – Параметри моделювання

№ з/п	Z_p	I	Z	C_v	C_{d1}	n	C_{d2}	m	C_K	Параметри
1	1	0,5	1	0,5	1	100000	1	500000	0,5	$\beta \prec \omega_0$
2	1	0,5	1	2	1	100000	1	500000	2	$\beta = \omega_0$
3	1	0,5	1	4	1	100000	1	500000	5	$\beta \succ \omega_0$

Візуалізація результатів (рис. 6-8).

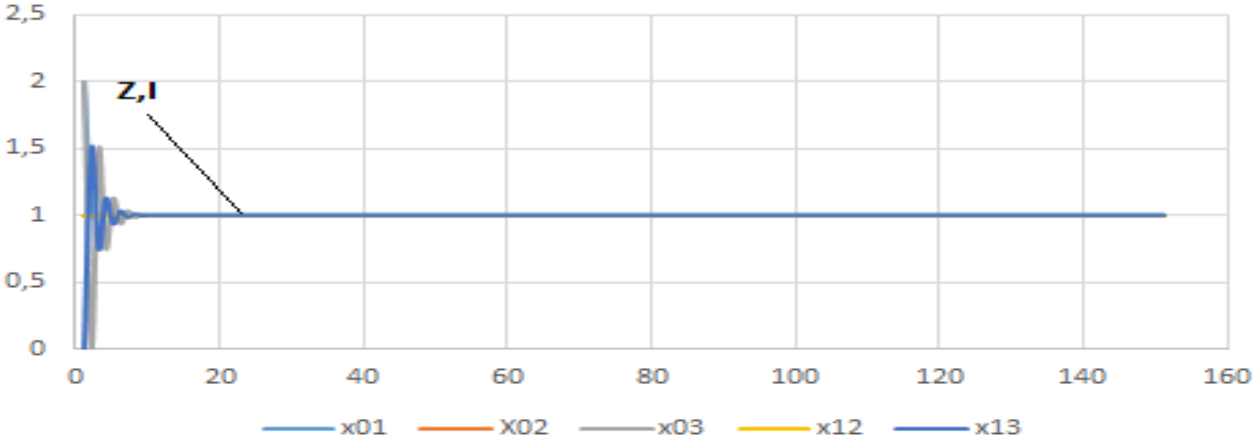


Рисунок 6 – Залежність інтенсивності та захисту даних від кількості ітерацій (140).
Дані складових взяті з табл. 1. $\beta \prec \omega_o$, через *i* позначено кількість ітерацій.

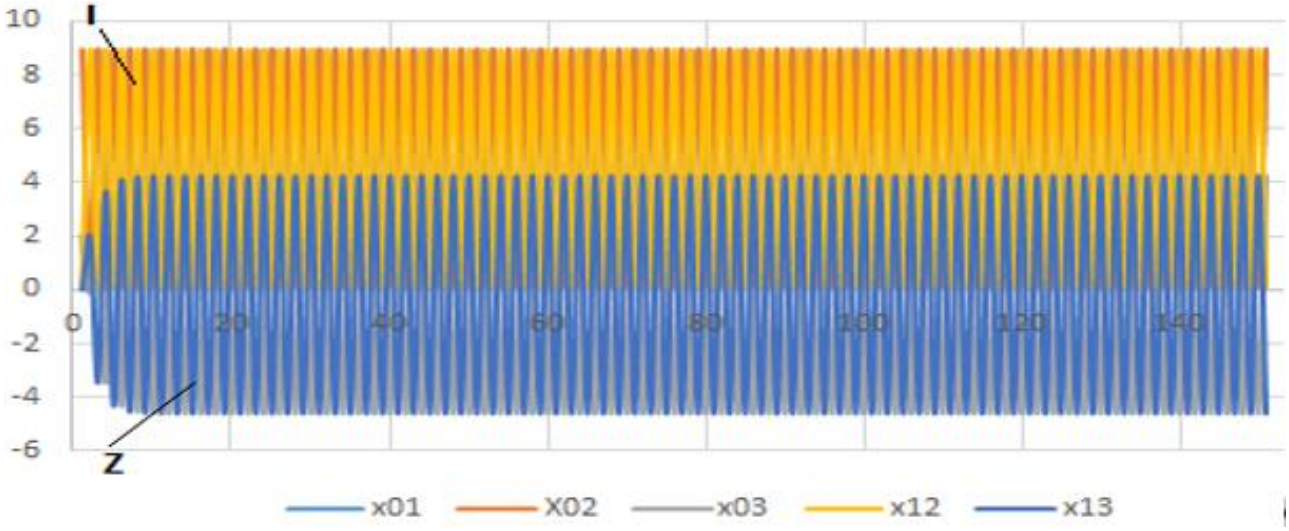


Рисунок 7 – Залежність інтенсивності та захищеності даних від кількості ітерацій (140).
$\beta = \omega_o$,

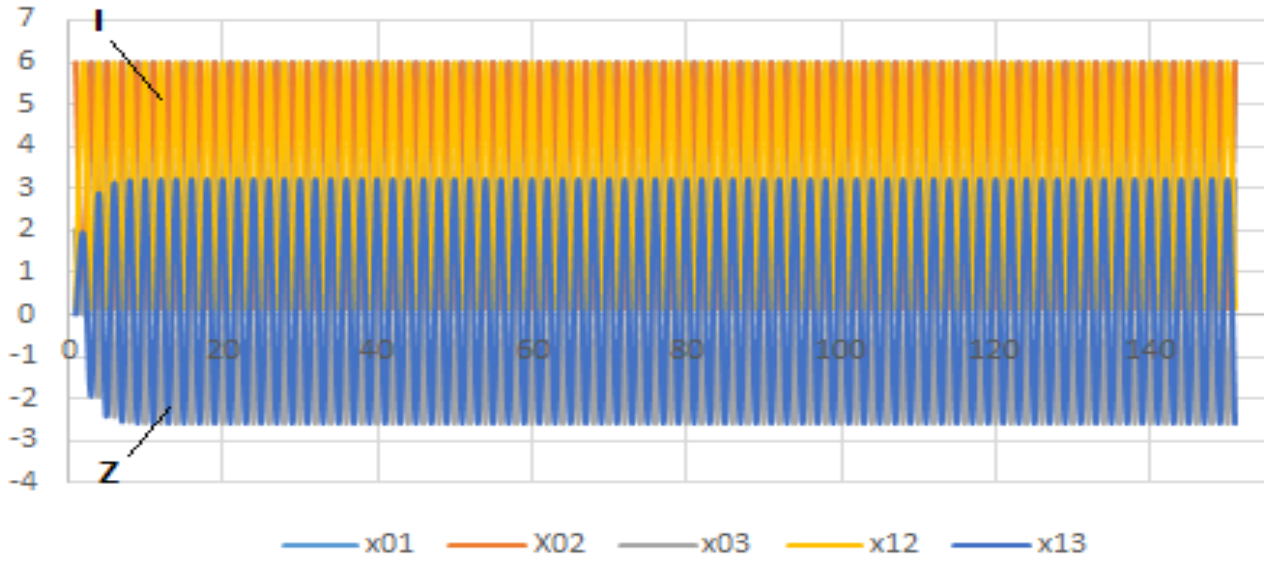


Рисунок 8 – Залежність інтенсивності та захисту даних від кількості ітерацій (140). $\beta \succ \omega_o$,

Обговорення результатів дослідження рівня захищеності інформаційного простору соціальних мереж з врахуванням кількості співтовариств. Залежність (2) показує класичний підхід до захисту персональних даних. Отримано систему лінійних диференційних рівнянь (6), яка описувала систему захисту соціальної мережі. Знайдено стаціонарну позицію системи, що описується системами рівнянь (7), (11). Розв'язок системи рівнянь (6) отримано методом «малих відхилень» (13). Рівняння гармонічного осцилятора отримано завдяки диференціюванню першого рівняння системи (13). Розв'язок рівняння гармонічного осцилятора (14), (15) розпалося на три випадки, в залежності від співвідношення частоти системи та коефіцієнта затухання (20)-(22).

Було встановлено, що система захисту інформації є нелінійною. Це пояснюється тим, що за межами резонансної області (рис. 8) [13] виявлені незатухаючі коливання системи захисту. Завдяки цьому проведені подальші дослідження нелінійної системи захисту.

Особливості запропонованого методу і отриманих результатів полягають в одержанні кількісних показників захисту інформації від специфічних параметрів соціальної мережі, в тому числі, від кількості співтовариств. Існуючі методи дослідження не дають можливості отримати такі показники. На відміну від попередніх досліджень, отримані результати вказують на нелінійність системи захисту СМ. Запропановано математичну модель впливу комплексу специфічних параметрів мережі на систему захисту.

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.

Висновки та перспективи подальших досліджень.

1. Дослідження лінійної моделі впливу середньої відстані між користувачами в СМ на систему захисту дозволило перейти від класичного підходу до систем диференціальних рівнянь, що дозволило отримати математичні залежності між специфічними параметрами соціальної мережі, в тому числі кількості співтовариств та показником захисту. В результаті дослідження отримані рівняння гармонічного осцилятора з затухаючою амплітудою. Це дозволило визначити 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.

2. Перевірка на лінійність системи захисту інформації вказала на її нелінійність. Це доведено шляхом розгляду трьох варіантів розв’язку рівняння осцилятора близько стаціонарного стану системи. Це дозволило зауважити, 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 деякого інтервалу існування системи. В результаті аналізу ітерації коливань системи захисту виявлено її нелінійність. Це дозволить перейти до дослідження нелінійної системи захисту. Необхідне подальше дослідження нелінійної системи захисту персональних даних соціальної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. Ахрамович, С. Лазаренко, Г. Мартинюк, та Ю. Баланюк, “Модель пошуку співтовариств в соціальній мережі”, *Безпека інформації*. К. НАУ. том 26, №1, с. 35-41, 2020, doi: https://doi.org/10.18372/2225-5036.26.14668.

[2] N. Bailey, “The mathematical theory of infectious diseases and its applications”, New York, USA: Hafner Press, 1975.
[3] F. Cohen, “Computer viruses, theory and experiments”, *Computers & Security*. vol. 6, pp. 22-35, 1987.
[4] D. Gubanov, and A. Chkhartishvili, “A conceptual approach to the analysis of online social networks”, *Upravlenie bol'shimi sistemami – Large-Scale Systems Control*, No. 45, pp. 222−23, 2013.
[5] J. Kephart, and S. White, “Directed-graph D. Gubanov, and A. Chkhartishvili, “A conceptual approach to the analysis of online social networks”, Automation and Remote Control, vol. 76(8), pp. 1455-1462, 2015, doi: https://doi.org/10.1134/S000511791508010X.
[6] V. Savchenko, V. Akhramovych, T. Dzyuba, S. Laptiev, N. Lukova-Chuiko, and T. Laptieva, “Methodology for calculating information protection from parameters of its distribution in social networks”. in *Proc. IEEE 3rd International Conference on Advanced Trends in Information Theory* (*ATIT*), Kyiv, 2021, pp. 99-105, doi: https://doi.org/10.1109/ATIT54053.2021.9678599.
[7] 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*), № 1, pp. 15-21, 2021, doi: https://doi.org/10.17762/ijcnis.v13i1.4882.
[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”, *Східно-Європейський журнал передових технологій*, № 1/9 (115). pp. 63-74, 2022, doi: https://doi.org/10.15587/1729-4061.2022.252135.
[9] M. M. Williamson, and J. Léveillé, “An epidemiological model of virus spread and cleanup”, *Hewlett-Packard Laboratories*, February 27th, 2003. [Online]. Available: https://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf. Accessed on: Apr. 21, 2023.
[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.
[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.
[13] Д.И. Трубецков, *Введение в синергетику. Хаос и структуры*, Изд. 2-е испр. и доп. Москва: Едиториал УРСС, 2004.

Стаття надійшла до редакції 02.02.2023.

REFERENCES

[1] V. Akhramovych, S. Lazarenko, H. Martynyuk, and Yu. Balanyuk, “Social network communities’ search model”, *Ukrainian scientific journal of information security*, vol. 26, no. 1, pp. 35-41, 2020, doi: https://doi.org/10.18372/2225-5036.26.14668.
[2] N. Bailey, “The mathematical theory of infectious diseases and its applications”, New York, USA: Hafner Press, 1975.

[3] F. Cohen, “Computer viruses, theory and experiments”, *Computers & Security*. vol. 6, pp. 22-35, 1987.

[4] D. Gubanov, and A. Chkhartishvili, “A conceptual approach to the analysis of online social networks”, *Upravlenie bol'shimi sistemami – Large-Scale Systems Control*, No. 45, pp. 222−23, 2013.

[5] J. Kephart, and S. White, “Directed-graph D. Gubanov, and A. Chkhartishvili, “A conceptual approach to the analysis of online social networks”, Automation and Remote Control, vol. 76(8), pp. 1455-1462, 2015, doi: https://doi.org/10.1134/S000511791508010X.

[6] V. Savchenko, V. Akhramovych, T. Dzyuba, S. Laptiev, N. Lukova-Chuiko, and T. Laptieva, “Methodology for calculating information protection from parameters of its distribution in social networks”. in *Proc. IEEE 3rd International Conference on Advanced Trends in Information Theory* (*ATIT*), Kyiv, 2021, pp. 99-105, doi: https://doi.org/10.1109/ATIT54053.2021.9678599.

[7] 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*), № 1, pp. 15-21, 2021, doi: https://doi.org/10.17762/ijcnis.v13i1.4882.

[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*, no. 1/9 (115). pp. 63-74, 2022, doi: https://doi.org/10.15587/1729-4061.2022.252135.

[9] M. M. Williamson, and J. Léveillé, “An epidemiological model of virus spread and cleanup”, *Hewlett-Packard Laboratories*, February 27th, 2003. [Online]. Available: https://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf. Accessed on: Apr. 21, 2023.

[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.

[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.

[13] D. Trubetskov, *Introduction to synergetics. Chaos and Structures*, 2nd ed. rev. and add., Moscow: Editorial URSS, 2004.

VOLODYMYR AKHRAMOVYCH

METHOD OF CALCULATING OF THE INFORMATION IN SOCIAL NETWORKS PROTECTION DEPENDING ON THE NUMBER OF COMMUNITIES

A mathematical model (linear system of differential equations) was developed and a research of the model of personal data protection against the number of communities and the intensity of data transfer in social networks was conducted. The linear system of information protection in social networks in the mathematical sense of this term is considered. When described by linear models, the object should be linear, at least approximately. This approach makes it quite simple to consider mathematical models. If such a thing is not noticed, it is necessary to examine the security system for linearity. Such dependecies has been studied: the dependence of the amount of information flow in

the social network on the components of information protection, the amount of personal data, and the speed of the data flow; the security of the system on the size of the system (as well as on the amount of personal data); information security threats on the number of communities, and also calculated: Z_p – coefficient representing the impact of information protection measures; C_v – coefficient representing the impact of data leakage rate; C_k – the coefficient representing the influence of the amount of data on its leakage; C_{d2} – the coefficient representing the influence of the system size on system security; C_{d1} – coefficient representing the impact of system security on data leakage; m_k – the number of connections in the social networks; n_k – number of vertices in the social networks; α – the α parameter can be used to configure the network partitioning algorithm. The solution has been obtained - the harmonic oscillator equation, which breaks down into three cases: pre-resonance zone, resonance zone and post-resonance zone. So, the impact of the parameters of the number of communities on the parameters of the social network security system was investigated. Such a study is useful and important from the point of view of information protection in the network, since the parameters of the number of communities has significant influence, up to 100%, per protection indicator. As the result of research, it was established that social network security systems are non-linear.

Keywords: social network, number of communities, security system, non-linearity, differential equations.

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

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