КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2(14), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.14.3649
УДК 004.738.5

Ахрамович Володимир Миколайович
Доктор технічних наук, старший науковий співробітник,
Державний університет телекомунікацій, м. Київ, Україна
ORCID ID: 0000-0002-6174-5300
12z@ukr.net

МЕТОД РОЗРАХУНКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД КОЕФІЦІЄНТА КЛАСТЕРИЗАЦІЇ МЕРЕЖІ

Анотація. Розроблено математичну модель і проведено дослідження моделі захисту персональних даних від коефіцієнта кластеризації мережі і інтенсивності передачі даних в соціальних мережах. Розглянуто залежності: величини потоку інформації в соціальній мережі від складових захисту інформації, персональних даних, і швидкості потоку даних; захищеності системи від розмірів системи (так і від кількості персональних даних); загроз безпеці інформації від коефіцієнта кластеризації мережі. Отримано система лінійних рівнянь, яка складається з рівняння: швидкості зміни потоку інформації від захищеності соціальної мережі і коефіцієнтів, які відображають вплив заходів захищеності, кількості персональних даних, швидкості витоку, зміни показника захисту інформації від коефіцієнта кластеризації мережі, її розмірів, захищеності персональних даних. В результаті рішення системи диференціальних рівнянь отримані математичні та графічні залежності показника захисту персональних даних в соціальній мережі від різних складових. Розглянувши три варіанти вирішення рівняння близько стаціонарного стану системи, можна прийти до висновку, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючо. амплітудою, або експоненціально згасаючим законом. Виконано більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь до дискретної і промоделювати деякий інтервал існування системи. Представлені математичні та графічні залежності частоти власних коливань системи, періоду коливань, коефіцієнта загасання. Проведено імітаційне моделювання для значень з відхиленням від стаціонарної позиції системи. В результаті імітаційного моделювання доведено, що система захисту соціальної мережі нелінійна.

Ключові слова: коефіцієнт кластеризації; соціальна мережа; потік; інформація; дані; витік; коефіцієнт; рівняння.

ВСТУП

Обчислення або оцінка коефіцієнта кластеризації може дати уявлення про вплив поширення несанкціонованої інформації зловмисними користувачами. Після того, як шкідливий вузол додається до списку контактів, він може отримати доступ до чутливих даних і розкривати їх без розбору, використовуючи засоби соціальної мережі, такі як розміщення дощок об’яв, публікація зображень тощо. Такий вплив можна виміряти, обчисливши середнє співвідношення друзів, яке може отримати конфіденційну інформацію, розкриту зловмисним Кластеризація – це локальна характеристика мережі. Вона характеризує степінь взаємодії між собою найближчих сусідів даного вузла. У більшості мереж, якщо вузол А з'єднаний з вузлом В, а вузол В – з вузлом С, то існує велика ймовірність, що вузол А з'єднаний з вузлом С (друзі наших друзів зазвичай також є і нашими друзями). Коефіцієнт кластеризації даного вузла є ймовірність того, що два найближчих сусіда цього вузла самі є найближчими сусідами.

Коефіцієнт С відповідає відношенню реального числа зв'язків між його сусідами і їх потенційно можливого числа.

ISSN 2663 - 4023

Постановка проблеми. Коефіцієнт кластеризації може бути усереднений для будь–якої частини мережі або для мережі в цілому, стаючи її інтегральною характеристикою:

$$C=1\frac{1}{n}\sum C_i. \quad (1)$$

де $\sum C_1$ – загальна кількість зв'язків в соціальній мережі; n – загальна кількість вершин в мережі.

Коефіцієнт кластеризації – це метрика, яка є більш ефективною, ніж щільність, і її все частіше використовують в суспільних науках. Коефіцієнт кластеризації – ступінь, що визначає наскільки вузли прагнуть до кластеризації. Наприклад, в мережі друзів це ймовірність того, що двоє моїх друзів є друзями між собою. Тобто це деяка оцінка фрагментованості мережі. При високій кластеризації можна очікувати, що вірус буде поширюватися лише в певній підгрупі (кластері). При низькій кластеризації висока ймовірність швидкого поширення вірусу по всій мережі

Локальний коефіцієнт кластеризації. Коефіцієнт локального об'єднання в кластери (коефіцієнт кластеризації) є мірою того, наскільки добре пов'язані між собою сусіди даного вузла. Локальний коефіцієнт кластеризації розраховується як число зв'язків між сусідами даного вузла / можливе число зв'язків між сусідами.

У непрямому графі коефіцієнт кластеризації c (v) вузла v з deg (v) ребрами визначається як кількість існуючих зв'язків між цими вузлами, позначені як , $e_{\deg(v)}$поділене на кількість усіх можливих посилань, які за умовою ($\frac{e_{\deg(v)}(e_{\deg(u)})-1}{2}$) (2). Тому у нас є: C(v)=$\frac{2e_{\deg(v)}}{e_{\deg(v)}(e_{\deg(u)})-1}$.

Коефіцієнт кластеризації загального графа, позначений як C (G), визначається як середній коефіцієнт кластеризації всіх вузлів графа, отже:

$$C(G)=\frac{\sum_{v\in V} c(v)}{\|V\|} \quad (2).$$

де: $\sum_{v\in Vc(v)}$ - загальна кількість зв'язків графа, ||V|| - загальна можлива кількість зв'язків графа.

Обчислення або оцінка коефіцієнта кластеризації (рис. 1,2) може дати уявлення про вплив поширення несанкціонованої інформації зловмисними користувачами на дружбу з вузлами. Після того, як шкідливий вузол η додається до списку контактів v, η може отримати доступ до чутливих даних v і розкривати їх без розбору, використовуючи засоби соціальної мережі, такі як розміщення дощок об'яв, публікація зображень тощо. Зокрема, якщо η клонує користувач, який користується професійним довірою, всі чутливі дані, як v ділиться з η,. Такий вплив можна виміряти, обчисливши середнє співвідношення Q_v друзів v, яке може отримати конфіденційну інформацію, розкриту зловмисним η таким чином: $Q_v = p_v c(v)$.

З цього рівняння робимо висновок, що ступінь поширення персональних даних пропорційна коефіцієнту кластеризації. Чим більший набір друзів, тим ширше розкриття персональних даних контактам користувача.

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

ISSN 2663 - 4023

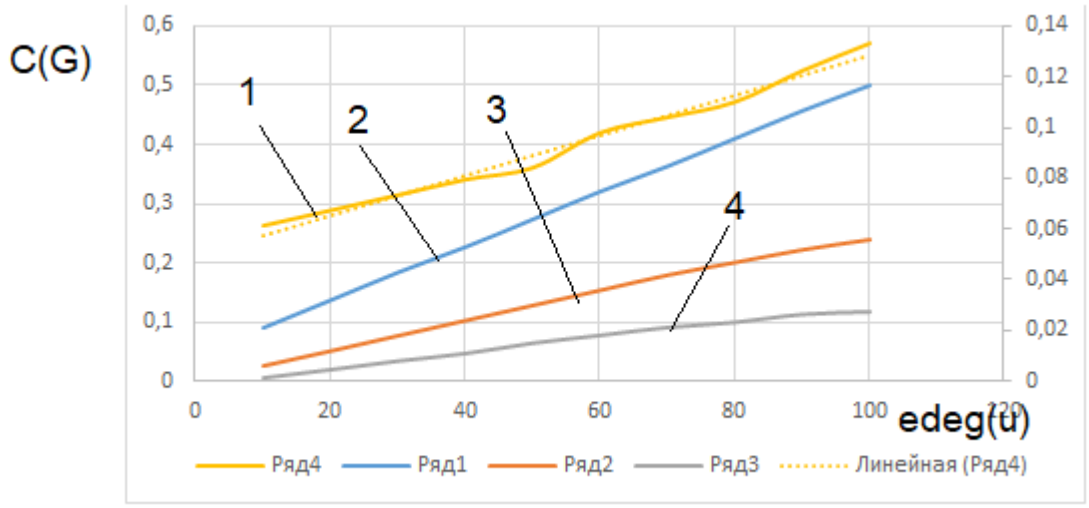

*Рис. 1 Коефіцієнт кластеризації: пряма 1 – при e*deg(v) *=(1, 1.1 2), шкала ординат зліва, рівняння C(G)=0,0034edeg(u)+0,2132; пряма 2 – при e*deg(v) *=(1, 1.5, 5) шкала ординат праворуч, рівняння (G)=0,0011edeg(u)+0,0106; пряма 3 – при e*deg(v) *=(1, 2, 10) шкала ординат праворуч, рівняння C(G)=0,0006edeg(u)+0,012; шкала ординат праворуч, пряма 4 – при e*deg(v) *=(1, 2, 20) шкала ординат праворуч, рівняння C(G)=0,0003edeg(u)–0,0006.*

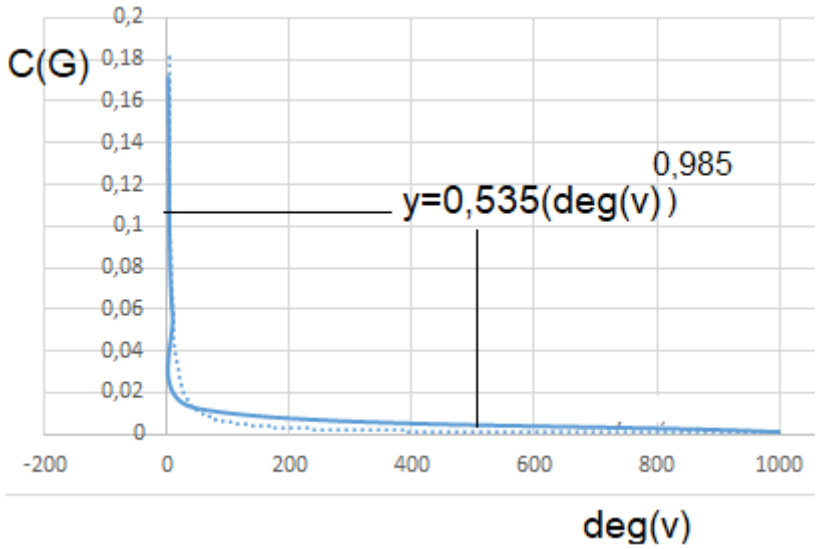

Рис. 2 Залежність коефіцієнта кластеризації від deg(v) при e_{deg} *= (1, 100, 1000)*

Аналіз останніх досліджень і публікацій. В статті [1], [15] досліджується метод розрахунку захисту інформації від репутації користувачів та взаємовпливу користувачів в соціальних мережах.

В статті [2] представлена математична теорія інфекційних хвороб та її застосування. В статті [3], [10] 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 статті [5] досліджено епідеміологічну модель комп'ютерних вірусів із спрямованим графіком. В статті [6] розглянуто нелінійну математичну модель залежності між довірою та показником захисту інформації в соціальній мережі. В роботі [7], [9] досліджуються основні параметри соціальних мереж з отриманням графічних залежностей. Математичні моделі параметрів соціальної мережі, в тому числі, коефіцієнта кластеризації представлені в статті з візуалізацією графічних залежностей. В статті [8] розглянута стохастична поведінка випадкових постійних скануючих черв'яків. В статті [11], [12] представлено модель поширення чуток SICR у складних мережах, та аналіз стабільності моделі поширення чуток I2S2R у комплексній мережі. В статті [13] розглянуто величину впливу розповсюдження інформації та інвестиційної поведінки про поширення інвестиційних продуктів в Інтернеті. В статті [14] розроблена модель сильних та слабких зв'язків користувачів в соціальних мережах з отриманням графічних залежностей. Дослідження нелінійних систем представлено в роботі [16].

Мета статті. Метою статті є дослідження впливу коефіцієнта кластеризації мережі та інших складових параметрів соціальної мережі на параметри захисту персональних даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ. У класичному підході до захисту персональних даних розрізняють коефіцієнт кластеризації:

$$\gamma = (\frac{\sum_{v \in V} C_{v1}}{N^2}) \tag{3}$$

де $\sum_{v \in V} C_{v1}$ – загальна кількість зв'язків в соціальній мережі; N – загальна кількість вершин в мережі.

Втрата такої якості, як кластеризація в мережі – 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:

$$dI = 0; \frac{dI}{dt} = 0 \tag{4}$$

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

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I \tag{5}$$

ISSN 2663 - 4023

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

- 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 безпеки інформації).

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

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

Складемо рівняння:

$$\frac{dZ}{dt} = \frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4} - I(C_{d2} + C_{d1}) \tag{6}$$

Об'єднаємо рівняння (5) і (6) в систему.

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \dfrac{dZ}{dt} = \dfrac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4} - I(C_{d2} + C_{d1}) \end{cases} \tag{7}$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (7). Умови стаціонарності $dI = 0; \dfrac{dI}{dt} = 0$. Отже:

$$\begin{cases} Z_p \bar{Z} + (C_v + C_K) \bar{I} = 0 \\ \dfrac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4} - I(C_{d2} + C_{d1}) = 0 \end{cases} \tag{8}$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{\dfrac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}}{(C_{d2} + C_{d1})} \tag{9}$$

ISSN 2663 - 4023

Далі з першого рівняння системи рівнянь (8) знаходимо $\bar{Z}$.

$$Z_p \bar{Z} - \frac{\frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}(C_v + C_k)}{(C_{d2} + C_{d1})} = 0 \quad (10)$$

$$\bar{Z} = \frac{\frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}(C_v + C_k)}{(C_{d2} + C_{d1})Z_p} \quad (11)$$

Графічні результати обчислення представлені на рис. 3,4.
Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \dfrac{\frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}}{(C_{d2} + C_{d1})} \\ \bar{Z} = \dfrac{\frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}(C_v + C_k)}{(C_{d2} + C_{d1})Z_p} \end{cases} \quad (12)$$

Вирішимо систему рівнянь (7) методом «малих відхилень» $I = \bar{I} + I; Z = \bar{Z} + Z$:, отже, система рівнянь прийме вигляд:

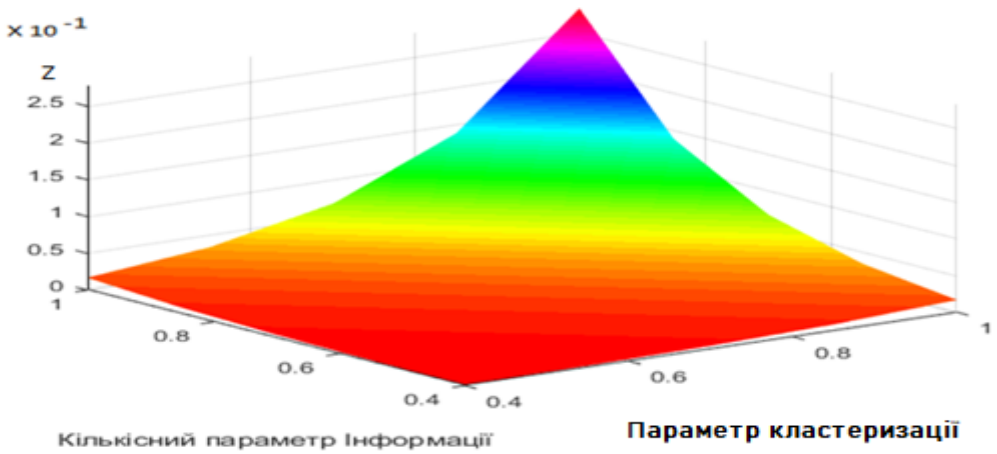

Рис. 3 Залежність захисту персональних даних від складових

ISSN 2663 - 4023

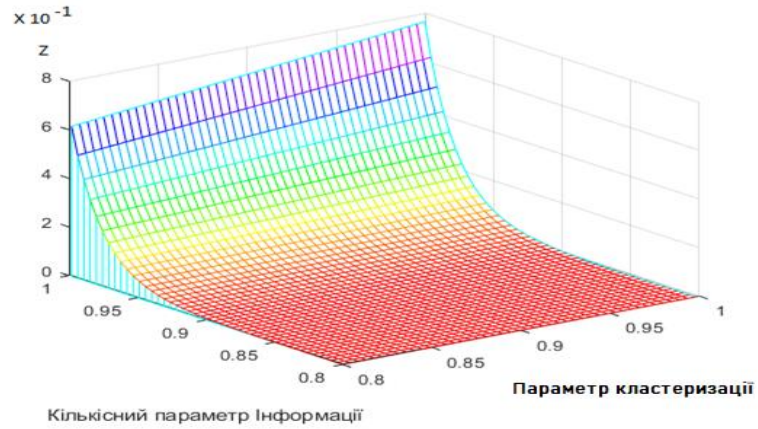

Рис. 4 Залежність захисту персональних даних від складових

$$\begin{cases} \dfrac{dI}{dt} = Z_p(\bar{Z}+Z) + (C_v + C_K)(\bar{I}+I) \\ \dfrac{dZ}{dt} = \dfrac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4}(C_v + C_k)(C_v + C_k) - (\bar{I}+I)(C_{d2} + C_{d1}) \end{cases} \quad (13)$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + \dfrac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4}(C_v + C_k)_i(C_v + C_k) \end{cases} \quad (14)$$

Диференціюючи перше рівняння системи (14) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + \frac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4}(C_v + C_k)) - (C_v + C_K)\frac{dI}{dt} \quad (15)$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + \frac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4}(C_v + C_k))I = 0 \quad (16)$$

Рівняння (16) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де:

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})(Z_p + \frac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4})} \quad (17)$$

$$\omega = \sqrt{(C_{d1} + C_{d2})(Z_p + \frac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4} - \frac{(C_v + C_K)^2}{4})} \quad (18)$$

$$T = \frac{2\pi}{\sqrt{(C_{d1}+C_{d2})(Z_p + \frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}(C_v + C_k) - \frac{(C_v + C_K)^2}{4}}}) \quad (19)$$

$$\beta = \frac{(C_v + C_K)}{2} \quad (20)$$

Рішення рівняння гармонічного осцилятора розпадається на три випадки.

1. $$\beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2}\cos(\sqrt{(C_{d1}+C_{d2}) + Z_p + \frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4}} \quad (21)$$
$$(C_v + C_k) - \frac{(C_v + C_K)^2}{4} t + \varphi_0)$$

Графічні результати обчислення представлені на рис. 5.

2. $$\beta = \omega_0 : I = (A_0 + B_0 t \exp(-\frac{(C_v + C_K}{2} t) \quad (22)$$

Графічні результати обчислення представлені на рис. 6.

3. $$\beta \succ \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t)$$
$$де$$
$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + Z_p + \frac{Nd\sum_{v\in V} C_{v1} - \sum_{v\in V} C_{v1} dN}{N^4})(C_v + C_k)} \quad (23)$$

Графічні результати обчислення представлені на рис. 7.

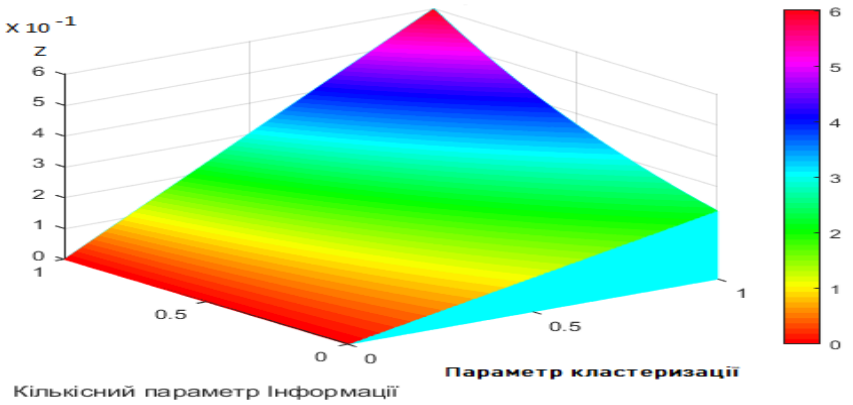

Рис. 5 Залежність захисту персональних при умові (21)

ISSN 2663 - 4023

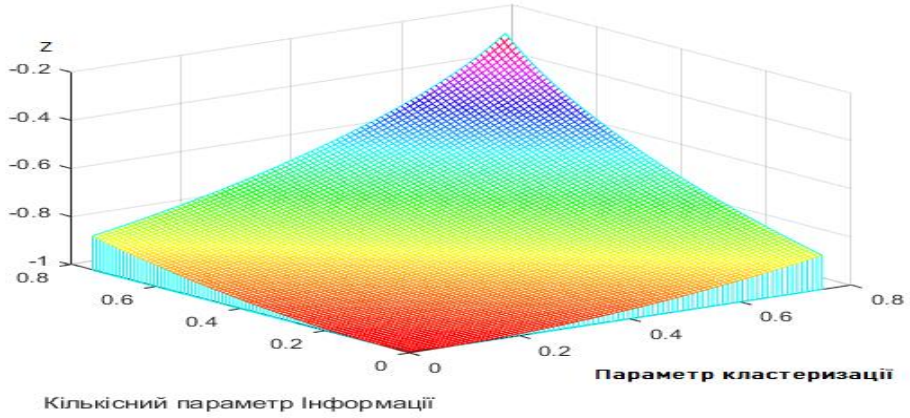

Рис.6 Залежність захисту персональних при умові (22)

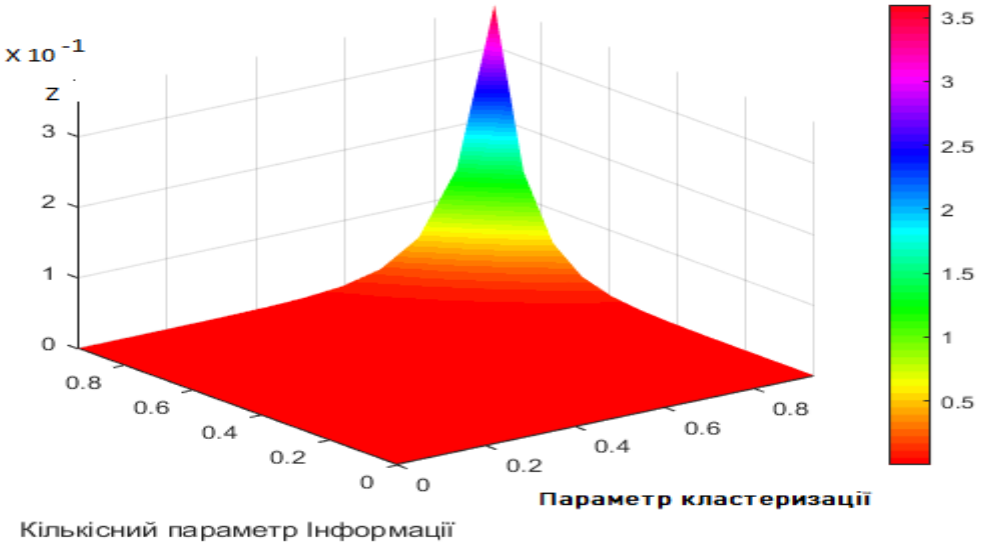

Рис. 7 Залежність захисту персональних при умові (23)

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

$$\begin{cases} \dfrac{I_{n+1}-I_n}{\Delta t} = (C_{d1}+C_{d2})Z_n - (C_v+C_K)I_n) \\ \dfrac{Z_{n+1}-Z_n}{\Delta t} = Z_p - (C_{d2}+C_{d1})I_n - (Z_p + + \dfrac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4}(C_v+C_k)(C_v+C_k)I_n) \end{cases} \quad (24)$$

ISSN 2663 - 4023

$$\begin{cases} I_{n+1} = I_n + (C_{d1} + C_{d2})Z_n - (C_v + C_K)I_n)\Delta t \\ Z_{n+1} = Z_n + (Z_n - I_n(C_{d2} + C_{d1} + Z_p + + \dfrac{Nd\sum\limits_{v\in V} C_{v1} - \sum\limits_{v\in V} C_{v1}dN}{N^4}(C_v + C_k)(C_v + C_k))\Delta t \end{cases} \quad (25)$$

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 $\beta \prec \omega_0, \beta = \omega_0, \beta \succ \omega_0$ 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}	C_{d2}	C_K	D	R	Параметри
1	1	0,5	1	1	1	0,5	1	1	1	$\beta \prec \omega_0$
2	1	0,5	1	6	1	1	6	1	1	$\beta = \omega_0$
3	1	0,5	1	6	1	1	6	0,5	1	$\beta \succ \omega_0$

Графічні результати ітераційного обчислення представлені на рис. 8-10.

Візуалізація результатів.

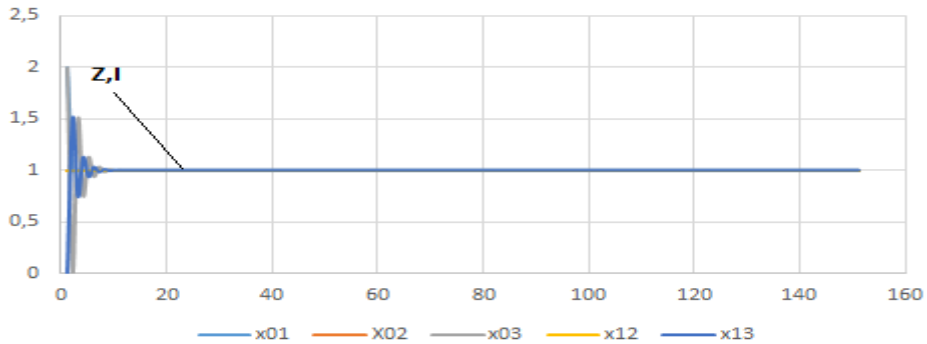

Рис. 8 Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140). Дані складових взяті з табл. 1. $\beta \prec \omega_0$, через і позначено кількість ітерацій.

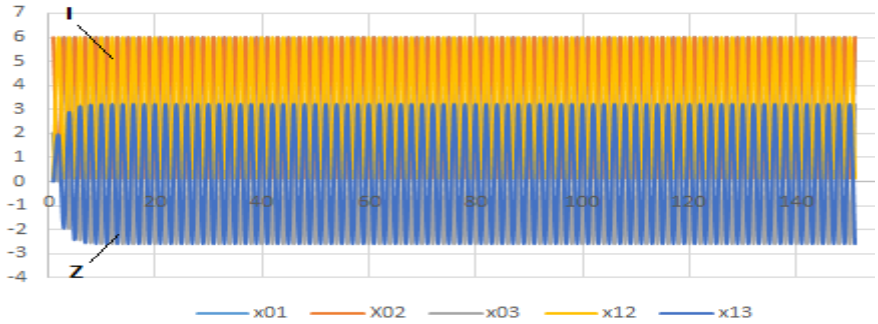

Рис. 9 Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140). $\beta = \omega_0$, Di=0,5

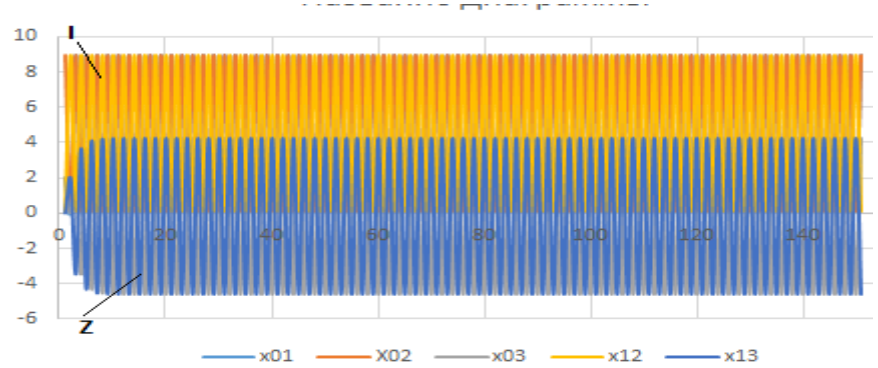

Рис. 10 Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140). $\beta \succ \omega_0$, Di=0,1

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ. Таким чином розроблена математична модель та проведено дослідження моделі захисту персональних даних від коефіцієнта кластеризації мережі та інтенсивності передачі даних в соціальних мережах.

В результаті математичного моделювання доказано, що система захисту соціальної мережі нелінійна [15] на що вказують результати імітаційного моделювання (рис. 10).

Необхідне подальше дослідження нелінійної системи захисту персональних даних соціальної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Akhramovich, V., Hrebennikov, A., Tsarenko, B., Stefurak, O. (2021). Method of calculating the protection of personal data from the reputation of users. *Sciences of Europe*, *1*(80), 23-31.
2. Bailey, N. (2014) The Mathematical Theory of Infectious Diseases and Its Applications. *Hafner Press*, 1(405), 159–170.
3. Cohen, F. (1987). Computer viruses, theory and experiments. *Computers & Security*, 6, 22-35.
4. Gubanov, D., Chkhartishvili, A. (2013). A conceptual approach to the analysis of online social networks. *Upravlenie bol'shimi sistemami – Large-Scale Systems Control*, 45, 222−236 (In Russian).
5. Kephart, J. O., & White, S. R. (б. д.). Directed-graph epidemiological models of computer viruses. У *1991 IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE Comput. Soc. Press. https://doi.org/10.1109/risp.1991.130801
6. Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security*, 1, 15-21.

7. The Model of Secure Social Networks Activity Based on Graph Theory. (2020). *International Journal of Innovative Technology and Exploring Engineering*, *9*(4), 1803–1810. https://doi.org/10.35940/ijitee.d1768.029420
8. Rohloff, K. R., & Basar, T. (2005). Stochastic behavior of random constant scanning worms. У *14th International Conference on Computer Communications and Networks, 2005. ICCCN 2005*. IEEE. https://doi.org/10.1109/icccn.2005.1523881
9. Savchenko, V. (2020). Analysis of Social Network Parameters and the Likelihood of its Construction. *International Journal of Emerging Trends in Engineering Research*, *8*(2), 271–276. https://doi.org/10.30534/ijeter/2020/05822020
10. Williamson, Matthew M.; Laeveillae, J. (2003). Epidemiological model of virus spread and cleanup. *Hewlett-Packard Laboratories Bristol*. http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf
11. Zan, Y., Wu, J., Li, P., & Yu, Q. (2014). SICR rumor spreading model in complex networks: Counterattack and self-resistance. *Physica A: Statistical Mechanics and its Applications*, *405*, 159–170. https://doi.org/10.1016/j.physa.2014.03.021
12. Zhang, Y., & Zhu, J. (2018). Stability analysis of I2S2R rumor spreading model in complex networks. *Physica A: Statistical Mechanics and its Applications*, *503*, 862–881. https://doi.org/10.1016/j.physa.2018.02.087
13. Zhao, N., Cheng, X., & Guo, X. (2018). Impact of information spread and investment behavior on the diffusion of internet investment products. *Physica A: Statistical Mechanics and its Applications*, *512*, 427–436. https://doi.org/10.1016/j.physa.2018.08.075
14. Ахрамович, В.М. (2019). Модель сильних та слабких зв'язків користувачів в соціальних мережах. *Зв'язок*, 3, 8–12.
15. Савченко, В. А., Ахрамович, В. М., Дзюба, Т. М., Лаптєв, С. О., Матвієнко, М. В. (2021). Метод розрахунку захисту інформації від взаємовпливу користувачів в соціальних мережах. *Сучасний захист інформації*, 1, 6-13.
16. Трубецков, Д.И. (2004). *Введение в синергетику. Хаос и структуры.* Изд. 2–е испр. И доп.– М. Едиториал. УРСС.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Akhramovich M. Volodymyr
Doctor of Technical Sciences, Senior Research Fellow,
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-6174-5300
12z@ukr.net

METHOD OF CALCULATING THE PROTECTION OF PERSONAL DATA FROM THE NETWORK CLUSTERING FACTOR

Annotation. A mathematical model has been developed and a study of the model of personal data protection from network clustering coefficient and data transfer intensity in social networks has been carried out.
Dependencies of protection of the system from the size of the system (and from the amount of personal data); information security threats from the network clustering factor.
A system of linear equations is obtained, which consists of the equation: rate of change of information flow from social network security and coefficients that reflect the impact of security measures, amount of personal data, leakage rate, change of information protection from network clustering factor, its size, personal data protection.
As a result of solving the system of differential equations, mathematical and graphical dependences of the indicator of personal data protection in the social network from different components are obtained.
Considering three options for solving the equation near the steady state of the system, we can conclude that, based on the conditions of the ratio of dissipation and natural frequency, the attenuation of the latter to a certain value is carried out periodically, with decaying amplitude, or by exponentially decaying law. A more visual analysis of the system behavior is performed, moving from the differential form of equations to the discrete one and modeling some interval of the system existence.
Mathematical and graphical dependences of the system natural frequency, oscillation period, attenuation coefficient are presented.
Simulation modeling for values with deviation from the stationary position of the system is carried out. As a result of simulation, it is proved that the social network protection system is nonlinear.

Keywords: clustering coefficient; social network; flow; information; data; leakage; coefficient; equation

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Akhramovich, V., Hrebennikov, A., Tsarenko, B., Stefurak, O. (2021). Method of calculating the protection of personal data from the reputation of users. *Sciences of Europe*, *1*(80), 23-31.
2 Bailey, N. (2014) The Mathematical Theory of Infectious Diseases and Its Applications. *Hafner Press*, 1(405), 159–170.
3 Cohen, F. (1987). Computer viruses, theory and experiments. *Computers & Security*, 6, 22-35.
4 Gubanov, D., Chkhartishvili, A. (2013). A conceptual approach to the analysis of online social networks. *Upravlenie bol'shimi sistemami – Large-Scale Systems Control*, 45, 222−236 (In Russian).
5 Kephart, J. O., & White, S. R. (б. д.). Directed-graph epidemiological models of computer viruses. У *1991 IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE Comput. Soc. Press. https://doi.org/10.1109/risp.1991.130801
6 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security*, 1, 15-21.
7 The Model of Secure Social Networks Activity Based on Graph Theory. (2020). *International Journal of Innovative Technology and Exploring Engineering*, *9*(4), 1803–1810. https://doi.org/10.35940/ijitee.d1768.029420
8 Rohloff, K. R., & Basar, T. (2005). Stochastic behavior of random constant scanning worms. У *14th International Conference on Computer Communications and Networks, 2005. ICCCN 2005*. IEEE. https://doi.org/10.1109/icccn.2005.1523881

9 Savchenko, V. (2020). Analysis of Social Network Parameters and the Likelihood of its Construction. *International Journal of Emerging Trends in Engineering Research*, *8*(2), 271–276. https://doi.org/10.30534/ijeter/2020/05822020

10 Williamson, Matthew M.; Laeveillae, J. (2003). Epidemiological model of virus spread and cleanup. *Hewlett-Packard Laboratories Bristol*. http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf

11 Zan, Y., Wu, J., Li, P., & Yu, Q. (2014). SICR rumor spreading model in complex networks: Counterattack and self-resistance. *Physica A: Statistical Mechanics and its Applications*, *405*, 159–170. https://doi.org/10.1016/j.physa.2014.03.021

12 Zhang, Y., & Zhu, J. (2018). Stability analysis of I2S2R rumor spreading model in complex networks. *Physica A: Statistical Mechanics and its Applications*, *503*, 862–881. https://doi.org/10.1016/j.physa.2018.02.087

13 Zhao, N., Cheng, X., & Guo, X. (2018). Impact of information spread and investment behavior on the diffusion of internet investment products. *Physica A: Statistical Mechanics and its Applications*, *512*, 427–436. https://doi.org/10.1016/j.physa.2018.08.075

14 Akhramovych, V.M. (2019). Model sylnykh ta slabkykh zviazkiv korystuvachiv v sotsialnykh merezhakh. Zviazok, 3, 8–12.

15 Savchenko, V. A., Akhramovych, V. M., Dziuba, T. M., Laptiev, S. O., Matviienko, M. V. (2021). Metod rozrakhunku zakhystu informatsii vid vzaiemovplyvu korystuvachiv v sotsialnykh merezhakh. Suchasnyi zakhyst informatsii, 1, 6-13.

16 Trubetskov, D.Y. (2004). Vvedenye v synerhetyku. Khaos y strukturы. Yzd. 2–e yspr. Y dop.– M. Edytoryal. URSS.