УДК 004.056.5:004.77:316.472.4
DOI: 10.31673/2409-7292.2023.030303

**Ахрамович В. М., Чупрун С. Г.,
Стефурак О. Р., Придибайло Р. В.**

ВИЗНАЧЕННЯ СТУПЕНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ В ЗАЛЕЖНОСТІ ВІД ПРОФІЛЮ ЗВ'ЯЗКІВ МІЖ АБОНЕНТАМИ

Ще до виникнення соціальних мереж було з'ясовано який вплив дають особі оточуючі її люди. При цьому було визначено, що дуже часто найбільш корисним для особи є не близьке оточення суб'єкта (сильні зв'язки), а люди, з якими суб'єкт спілкується «поверхово» (слабкі зв'язки). На основі цих висновків виникає питання про роль малознайомих людей в житті окремо взятої особистості. Люди, які не входять у вузький кластер близьких друзів і знайомих, відкривають перед особистістю корисну інформацію – ту інформацію, якої особистість не володіє, в силу того, що зі слабкими зв'язками у суб'єкта комунікації менше загальних контактів. При цьому виникає інша проблема – проблема захищеності інформації, до якої можуть отримати доступ зовсім невідомі люди, які не входять до близького оточення суб'єкта. Для розробки методики оцінки захищеності інформації в соціальних мережах було відшукано рішення системи захисту в соціальних мережах з урахуванням дії специфічного параметру – сили зв'язків між абонентами, провести наочний аналіз поведінки системи. На відміну від класичного підходу, створена лінійна математична модель, знайдено стаціонарну позицію системи, отримано рівняння гармонічного осцилятора з затухаючою амплітудою. Визначено власну частоту коливань, період та коефіцієнт демпфування системи захисту. Зроблено висновок, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненціально загасаючим законом. В результаті досліджень лінійної моделі захисту на основі диференціальних рівнянь встановлено, що системи захисту соціальної мережі нелінійні. Визначено необхідність подальшого дослідження нелінійної моделі системи захисту інформації в соціальних мережах з метою розрахунку захищеності інформації з врахуванням типу зв'язків в між абонентами.

Ключові слова: соціальна мережа, зв'язки абонентів, система захисту, диференційні рівняння.

Вступ

За десятиліття до виникнення соціальної мережі Facebook Марк Грановеттер [1], провів перше своє знамените дослідження соціальних мереж, маючи на меті з'ясувати, який вплив вони надають на соціальну мобільність, а також які сприятливі можливості дають людині оточуючі його люди. Провівши опитування серед жителів передмістя Бостона, які недавно змінили роботу, соціолог визначив, що найбільш корисним з точки зору пошуку роботи є не близьке оточення суб'єкта (сильні зв'язки), а люди, з якими брали інтерв'ю спілкувалися «поверхово» (слабкі зв'язки). На основі цих висновків Грановеттера створив свою новаторську статтю «Сила слабких зв'язків», де розглянув найважливішу роль малознайомих людей в житті окремо взятої особистості.

Відповідно до теорії Грановеттера, люди, які не входять у вузький кластер близьких друзів і знайомих, відкривають перед особистістю корисну інформацію – ту інформацію, якої особистість не володіє, в силу того, що зі слабкими зв'язками у суб'єкта комунікації менше загальних контактів.

Постановка проблеми

Якщо слабкі зв'язки між абонентами утворюються як в спільнотах так і в соціальних мережах, то сильні зв'язки створюються переважно в спільнотах. Безумовно, більшість ваших близьких друзів (з якими у вас сильні зв'язки) є людьми, з якими ви перебували в одних і тих же співтовариствах в той чи інший момент свого життя. Ці спільноти можуть бути двором, де ви виросли, школою, яку відвідували, лабораторією, в якій працювали, або будь–якої групою за інтересом, наприклад фотогуртки або секцією з бадмінтону. І хоча ви часто перетинаєтеся з новими друзями своїх друзів (через вашу соціальну мережу), без спільноти, здатного розвинути ваші поверхневі відносини, ваша «дружба» з ними так і залишиться всього лише знайомством.

З появою соціальних мереж можливостей прикладного втілення даної концепції стало незрівнянно більше. Так, автори дослідження, проведеного Facebook Data Team, виявили, що незважаючи на те що абонементи соціальних мереж частіше споживають і поширюють

інформацію, якою з ними діляться близькі знайомі, вони також отримують величезний обсяг інформації від слабких зв'язків, і найчастіше саме подібні віддалені контакти служать каналом поширення нової та корисної інформації. Даний факт ще раз підтверджує, що соціальні мережі служать впливовим медіа–каналом для поширення корисної інформації (просування нових продуктів, обговорення актуальних подій і т. д.), А також є вагомим аргументом на користь теорії Грановеттера.

Аналіз публікацій та підходів

Метод аналізу впливів, ґрунтується на наступних припущеннях [2–8]:

1. Сила впливу одного фактора на інший по даному шляху залежить від довжини цього шляху (тобто числа ребер в ньому).

2. Чим більше паралельних впливів (за різними шляхами) існує між факторами, тим сильніше вплив між ними.

Нехай P_{ij}^m та N_{ij}^m – число позитивних і негативних шляхів довжини m, що йдуть від фактора x_i до фактору x_j, відповідно. Тоді сумарні позитивний і негативний вплив фактора x_i на фактор x_j визначаються наступним чином (рис. 1): $\bar{P}_{ij} = \sum_{m=1}^{\infty} f(m) P_{ij}^m$ – позитивний вплив, $\bar{N}_{ij} = \sum_{m=1}^{\infty} f(m) N_{ij}^m$ – негативний вплив, де $f(m)$ – монотонна функція, яка не спадає від довжини шляху m, та визначає ступінь ослаблення впливу на шляху від x_i до x_j – число позитивних і негативних шляхів довжини m, що йдуть від фактора x_i до фактору x_j, відповідно.

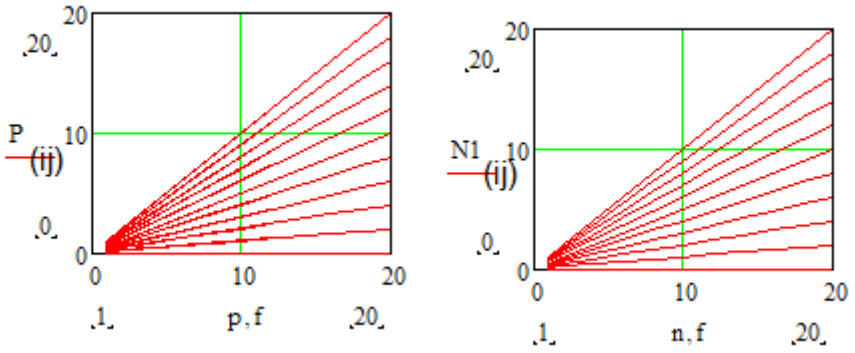
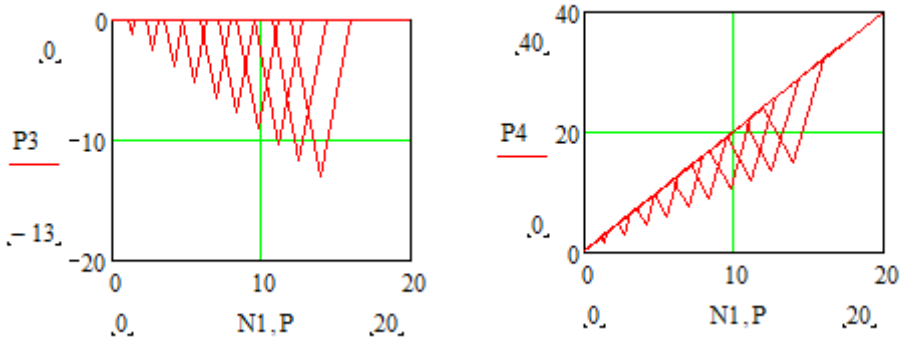


Рис. 1. Можливий вплив абонента: а) – позитивний вплив f (0, 0.1, 1), p (1, 2, 20), б) негативний вплив f (0, 0.1, 1), n (1, 2, 20).

Для порівняння різних стратегій розглядаються різні варіанти оціночної функції V (s_{ij}, c_{ij}), де s_{ij} – сумарний вплив фактора i на фактор j та c_{ij} – консонанс впливу фактора і на фактор j, які визначаються з наступних співвідношень:

$$s_{ij} = \bar{P}_{ij} + \bar{N}_{ij}\ ,\ c_{ij} = (\bar{P}_{ij} - \bar{N}_{ij}) / (\bar{P}_{ij} + \bar{N}_{ij}) \qquad (1)$$

Консонанс [5] c_{ij} – це міра відмінності між позитивним і негативним впливом (рис. 2). Чим він більший, тим чіткіше характер впливу. Більш детальні характеристики взаємодії факторів можна виявити при використанні нечітких когнітивних карт. Найбільш поширений підхід до обчислення нечітких впливів, полягає в наступному. Нехай між f_i і f_j є m шляхів і $Ir(f_i, f_j)$ позначає вплив f_i на f_j по r–му шляху, а $T(f_i, f_j)$ – сумарний вплив f_i на f_j за всіма m шляхах. тоді, $I_r(f_i, f_j) = \min_P w_{p,p+1}$ $T(f_i, f_j) = \max_{1 \le r \le m} I_r(f_i, f_j)$, де: $w_{p,p+1}$ – вага орієнтованого ребра від f_p до $f_p + 1$ на r–му шляху.



а) б)

Рис. 2 Складові консонансу: а) $C(ij)= P(ij) – N(ij)$, б) $C(ij)= P(ij) + N(ij)$

Таким чином, операція $I_r(f_i, f_j)$ виділяє найбільш слабкий зв'язок в r–му шляху, а операція $T(f_i, f_j)$ виділяє найбільш сильний зі зв'язків $I_r(f_i, f_j)$. Проілюструємо ці визначення прикладом з [1] (рис. 3):

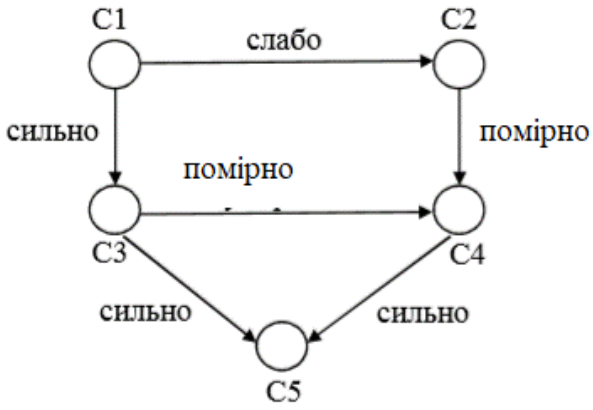


Рис.3. Нечіткий когнітивний граф впливів

Тут ваги ребер приймають значення з лінгвістичної шкали {слабо, помірно, сильно}. Розглянемо вплив фактора С1 на фактор С5. У графі три каузальних шляхи від С1 до С5 (r = 1, 2, 3): r = 1 відповідає шлях (С1, С3, С5), r = 2 – шлях (С1, С3, С4, С5), r = 3 – шлях (С1, С2, С4, С5). Три непрямих впливів С1 на С5 такі:

I_1 (С1, С5) = min {w13, w35) = min {сильно, сильно) = сильно;

I_2 (С1, С5) = min {w13, w34, w45) = min {сильно , помірно, сильно) = помірно;

I_3(С1, С5) = min {w12, w24, w45) = min {слабо, помірно, сильно) = слабо. Звідси сумарний вплив С1 на С5 дорівнює: Т (С1, С5) = max {I_1(С1, С5), I_2(С1, С5), I_3(С1, С5)} = max {сильно, помірно, слабо} = сильно. В роботі [8] запропонована модифікована модель впливів. У цій моделі вершина може перебувати в активному або пасивному стані; крім того, кожній вершині приписаний поріг. Вершина переходить в активний стан, тільки якщо сума вхідних впливів досягає порогу. Тільки в активному стані вершина передає вплив далі.

Незважаючи на описаний підхід, залишається невизначеним питання оцінки захищеності інформації в соціальних мережах в залежності від профілю зв’язків між абонентами. Для розробки методики оцінки захищеності інформації в соціальних мережах необхідно здійснити:

1) відшукати рішення системи захисту в соціальних мережах з урахуванням дії специфічного параметру – сили зв’язків між абонентами;

2) провести наочний аналіз поведінки системи.

Мета статті – розробити методику визначення ступеня захищеності інформації в соціальних мережах в залежності від профілю зв'язків між абонентами.

Основна частина

Лінійне рішення системи захисту в соціальній мережі з урахуванням дії специфічного параметру – сили зв'язків між абонентами.

У класичному підході до захисту даних розрізняють [11–15]:

$$F_i = \left[F_j, F_n, F_m \right] \tag{2}$$

де F_i – множина загроз від типу зв'язків між абонентами, F_j – слабі зв'язки між абонентами, F_n – помірні зв'язки між абонентами F_m – сильні зв'язки між абонентами.

Втрата такої якості, як зв'язок – процес, який має часовий інтервал [2–4]. 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 [10–16]. 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; Cv – 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 захищенність системи як здатність системи протистояти несанкціонованому доступу до конфіденційної даних. Отже, захищенність системи буде залежати:

від розмірів системи (як і від кількості даних);

загроз безпеки інформації від втрати зв'язків між абонентами.

Складемо рівняння:

$$\frac{dZ}{dt} = F_i - I(C_{d2} + C_{d1}) \tag{5}$$

де F_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати зв'язків між абонентами на захищеність інформаційної системи. C_{d2} – коефіцієнт, що відображає вплив

розмірів системи на захищеність; C_{d1} – коефіцієнт, що відображає вплив захищеності на витік даних. Об'єднаємо рівняння (3) і (4) в систему.

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \dfrac{dZ}{dt} = F_i - I(C_{d2} + C_{d1}) \end{cases} \tag{6}$$

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

$$\begin{cases} Z_p \bar{Z} + (C_v + C_K) \bar{I} = 0 \\ F_i - I(C_{d2} + Cd_1) = 0 \end{cases} \tag{7}$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{F_i}{(C_{d2} + C_{d1})} \tag{8}$$

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

$$Z_p \bar{Z} - \frac{(C_v + C_K) F_i}{(C_{d2} + C_{d1})} = 0 \tag{9}$$

$$\bar{Z} = \frac{(C_v + C_K) F_i)}{(C_{d2} + C_{d1}) Z_p} \tag{10}$$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \dfrac{F_i}{C_{d2} + Z_p} \\ \bar{Z} = \dfrac{(C_v + C_K) F_i}{(C_{d2} + C_{d1}) Z_p} \end{cases} \tag{11}$$

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

$$\begin{cases} \dfrac{dI}{dt} = Z_p (\bar{Z} + Z) + (C_v + C_K)(\bar{I} + I) \\ \dfrac{dZ}{dt} = F_i - (\bar{I} + I)(C_{d2} + C_{d1}) \end{cases} \tag{12}$$

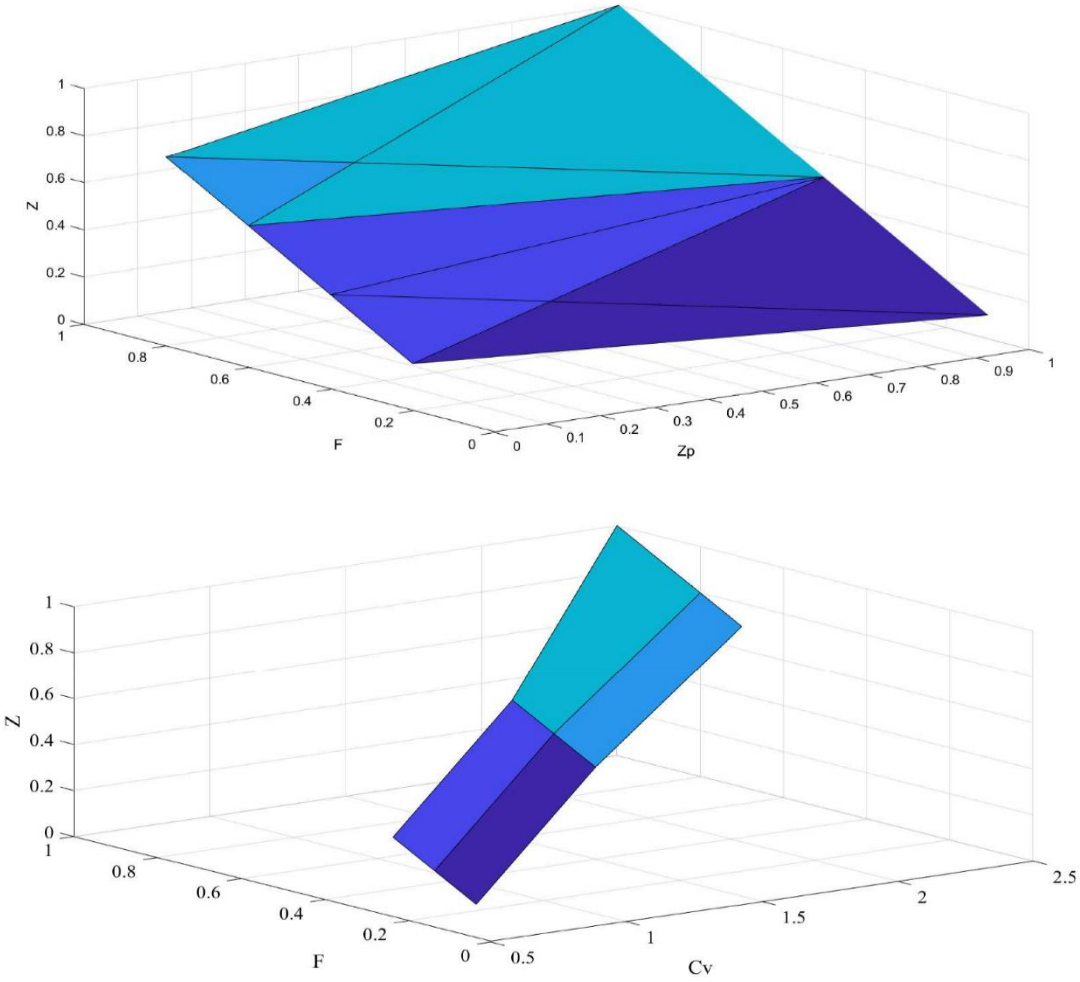


Рис. 4 Результати обрахунків за рівнянням (10)

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + F_i) \end{cases} \tag{13}$$

Диференціюючи перше рівняння системи (13) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + F_i) - (C_v + C_K)\frac{dI}{dt} \tag{14}$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + F_i)I = 0 \tag{15}$$

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

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})(Z_p + F_i)} \tag{16}$$

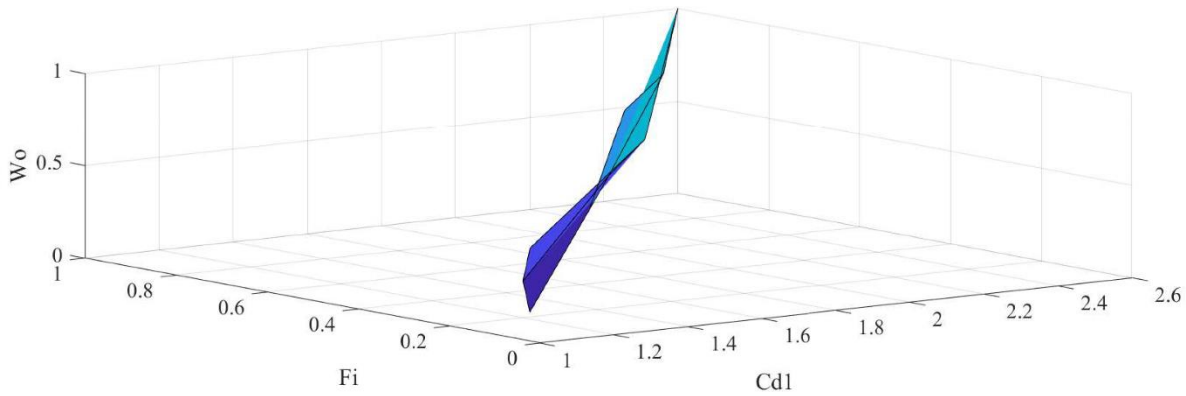


Рис. 5 Особиста частота системи захисту

$$\omega = \sqrt{(C_{d1} + C_{d2})(Z_p + F_i) - \frac{(C_v + C_K)^2}{4}} \tag{17}$$

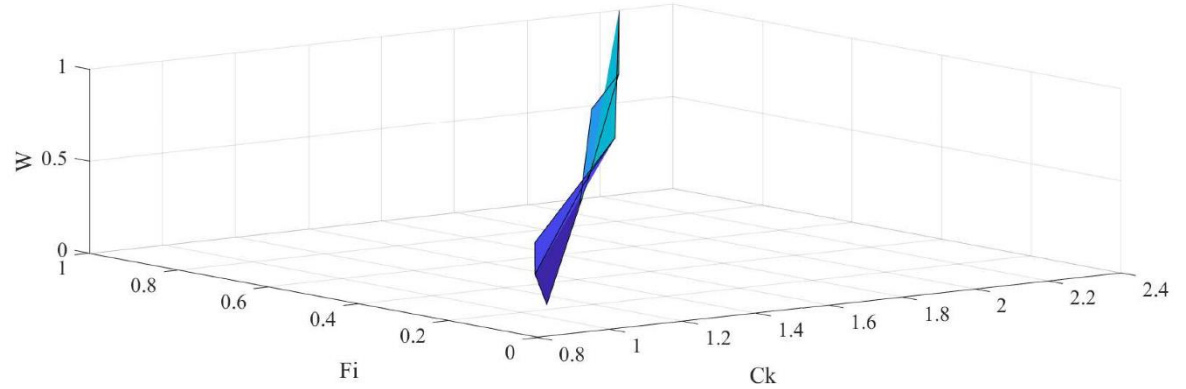


Рис. 6 Частота системи захисту

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2})(Z_p + F_i) - \frac{(C_v + C_K)^2}{4}}} \tag{18}$$

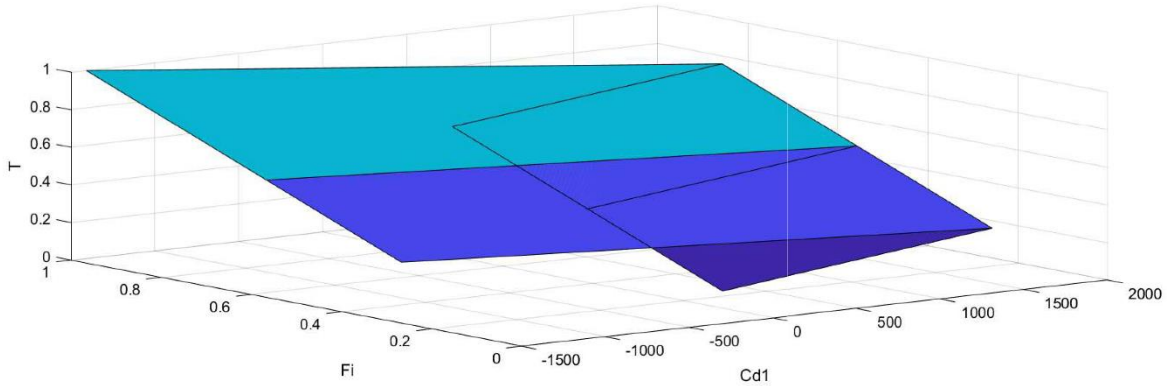


Рис. 7 Період коливань системи захисту

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

Рішення рівняння гармонічного осцилятора розпадається на три випадки [2].

$$1.\ \beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2} \cos(\sqrt{(C_{d1} + C_{d2} + Z_p + F_i) - \frac{(C_v + C_K)^2}{4}} t + \varphi_0) \quad (20)$$

Рис. 8 Залежність захисту при умові (20)

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

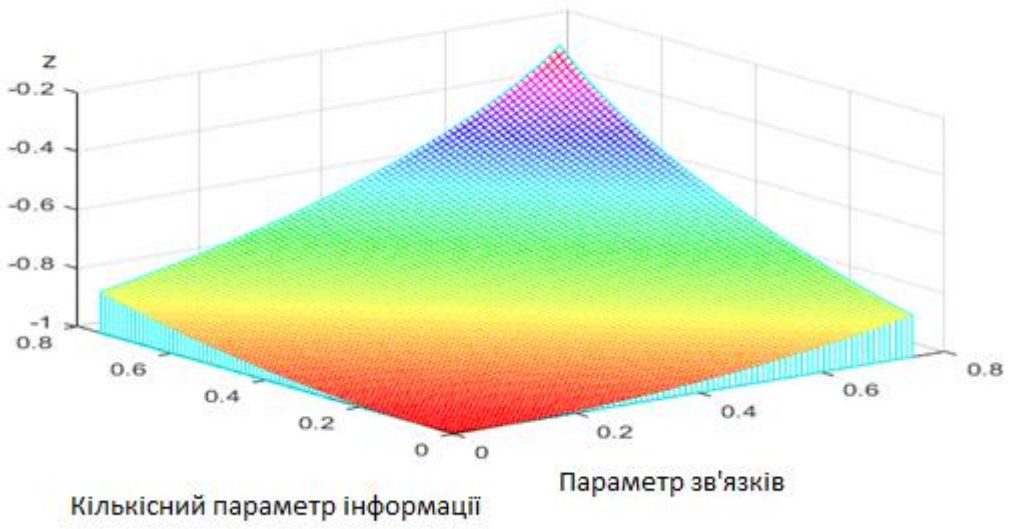


Рис.9 Залежність захисту при умові (21)

$$3.\ \beta \succ \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t) \quad (22)$$

де $y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + Z_p + F_i)}$.

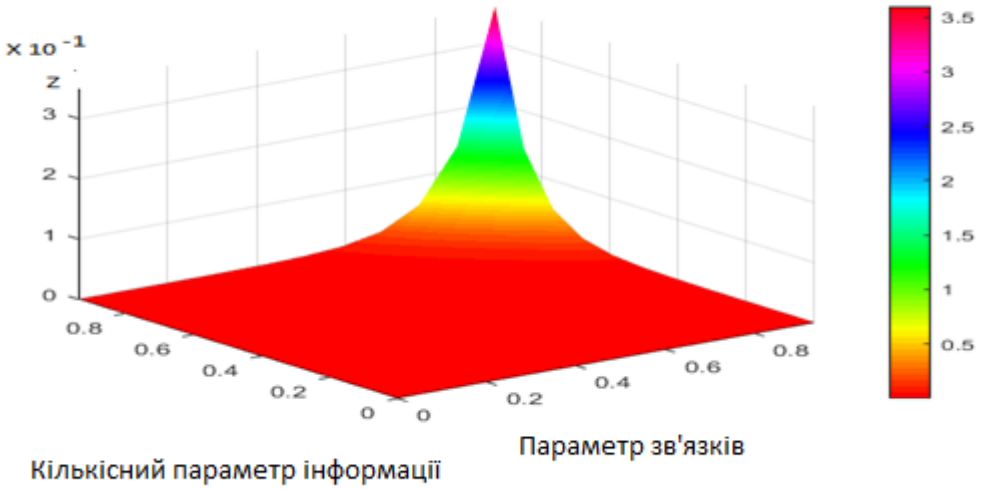


Рис. 10 Залежність захисту при умові (22)

Наочний аналіз поведінки системи

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 затухаючою амплітудою, або за експоненціально загасаючим законом [2]. Виконаємо більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь (5, 6) до дискретної і промоделювавши деякий інтервал існування системи. А саме:

$$\begin{cases} \dfrac{I_{n+1}-I_n}{\Delta t} = (C_{d1}+C_{d2})Z_n - (C_v + C_K)I_n) \\ \dfrac{Z_{n+1}-Z_n}{\Delta t} = Z_p - (C_{d2}+C_{d1})I_n - (Z_p + F_i)I_n) \end{cases} \quad (23)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1}+C_{d2})Z_n - (C_v + C_K)I_n)\Delta t \\ Z_{n+1} = Z_n + (Z_n - I_n(C_{d2}+C_{d1}+Z_p + F_i))\Delta t \end{cases} \quad (24)$$

Спочатку приймемо коефіцієнти $C_{d1}, C_v, C_{d2}, Z_p, D_i, C_K$ 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 $\beta \prec \omega_0, \beta = \omega_0, \beta \succ \omega_0$ з відхиленням від стаціонарної позиції системи. Дані представимо в табл. 1.

Таблиця 1

Параметри моделювання

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

Візуалізація результатів

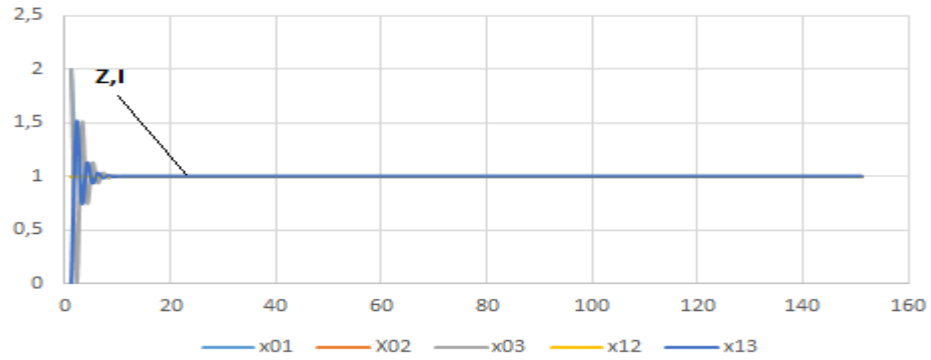


Рис 11 Залежність інтенсивності та захисту даних від кількості ітерацій (140). Дані складових взяті з табл. 1. $\beta \prec \omega_0$, через i позначено кількість ітерацій.

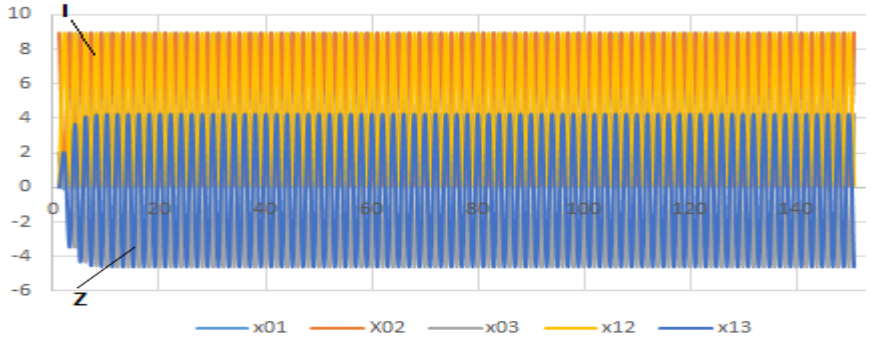


Рис 12 Залежність інтенсивності та захисту даних від кількості ітерацій (140). $\beta = \omega_0$, Fi=0,5

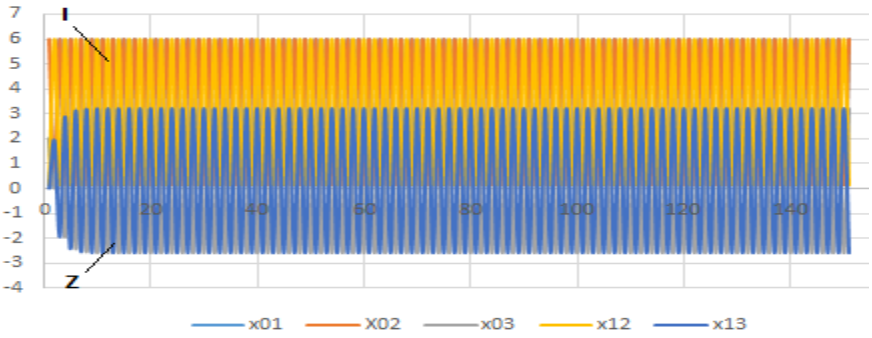


Рис 13 Залежність інтенсивності та захисту даних від кількості ітерацій (140). $\beta \succ \omega_0$, Fi=0,1

Висновки

На відміну від класичного підходу (2) створена лінійна математична модель (система диференційних рівнянь (6) та в процесі дослідження знайдено стаціонарну позицію системи (11) і отримано рівняння гармонічного осцилятора з затухаючою амплітудою (23). Визначено власну частоту коливань, період та коефіцієнт демпфування системи захисту. Розглянуто три варіанти вирішення рівняння близько стаціонарного стану системи. Зроблено висновок, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за

експоненціально загасаючим законом. При переході від диференціальної форми рівнянь (6) до дискретної (23) і моделювання деякого інтервалу існування системи та проведення ітерації коливань (рис. 11–13), зроблено висновок, що система захисту соціальної мережі є нелінійною.

Таким чином, необхідні подальші дослідження нелінійної моделі захисту інформації.

Перелік посилань

1. Granovetter, Mark S. The strength of weak ties // American journal of sociology. 2017. pp. 1360–1380. https://www.jstor.org/stable/2776392

2. Volodymyr Akhramovych, German Shuklin, Yuriy Pepa, Tetiana Muzhanova, Serhii Zozuli. Devising a procedure to determine the level of informational space security in social networks considering interrelations among users. Східно-Європейський журнал передових технологій. Харків .- 2022 № 1/9 (115). Pp. 63-74. https://doi.org/10.15587/1729-4061.2022.252135 · https://doi.org/10.15587/1729-4061.2022.252135

3. Akhramovych, V , Shuklin G , Pepa Y , Lehominova S , Muzhanova T , Dzyuba T , Yakymenko Y. Methodology for Calculating the Index of Protection of a Social Media from its Centrality. International Journal of Emerging Technology and Advanced Engineering. Volume 13, Issue 04, April 2023.- pp. 17-26. doi: 10.46338/ijetae0423_03. https://ijetae.com/Volume13Issue4.html·

4. Vitalii Savchenko, Volodymyr Akhramovych, Taras Dzyuba, Serhii Laptiev, Nataliia. Lukova-Chuiko, Tetiana Laptieva. Methodology for Calculating Information Protection from Parameters of its Distribution in Social Networks. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT). Conference Proceedings. December 15-16, 2021. Kyiv, Ukraine. Pp. 99-105. http://atit.ieee.org.ua/wp-content/uploads/2021/12/Program-ATIT-2021-02-14.12.21.pdf

5. Vitalii Savchenko, Volodymyr Akhramovych, Oleksander Matsko, Ivan Havryliuk Method of Calculation of Information Protection from Clusterization Ratio in Social Networks. Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021) co-located with 1st International Forum "Digital Reality" (DRForum 2021) Odesa, Ukraine, September 13-19, 2021.-pp. 24-31. https://ceur-ws.org/Vol-3200.

6. Albert, R., Jeong H., Barab´asi A. Attack and error tolerance of complex networks. Nature. 2016. Vol. 406, pp. 378–382. https://doi.org/10.1038/35019019

7. Ballester, C., Zenou Y. Key Player Po licies When Contextual Effects Matter. Jour nal of Mathematical Sociology. 2018. №. 38. pp. 233–248. https://pdfs. semanticscholar.org.

8. Basilisa Mvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior. Dec. 2019. pp. 20–34. https://doi.org/10.1016/j.chb.2014.11.023

9. Kosko, B. Fuzzy cognitive maps. International Journal of Man–Machine Studies, 2019. Vol.1. pp. 65–75.

10. Benson Vladlena, George Saridakis, Hemamali Tennakoon, Jean Noel Ezingeard, The role of security notices and online consumer behaviour: An empirical study of social networking users, International Journal of Human Computer Studies. Aug. 2015. pp. 36–44. https://doi.org/10.1016/j.ijhcs.2015.03.004

11. Borgatti, S. P. Identifying sets of key players in a network. Computational, Mathematical and Organizational Theory. 2016. V. 12. iss. 1. pp. 21–34. https://doi.org/10.1007/s10588-006-7084-x

12. X.W. Liu, H.Q. Wang, H.W. Lü, J.G. Yu, S.W. Zhang, Fusion–based cognitive awareness–control model for network security situation[J]. J. Soft. 2016. №27(8). pp. 2099–2114. http://dx.doi.org/10.13328/j.cnki.jos.004852

13. Leucio Antonio Cutillo, Re–k Molva, and Melek Önen. Analysis of privacy in online social networks from the graph theory perspective. In GLOBECOM 2019, Selected Areas in Communications Symposium, Social Networks Track. Houston, Texas, USA. December 2019. doi: 10.1109/GLOCOM.2011.6133517

14. M. Dürr, V. Protschky, and C. Linnhoff–Popien. Modeling Social Network Interaction Graphs, in Proceedings of the 2016 International Conference on Advances in Social Networks Analysisand Mining (ASONAM), ASONAM'12. Washington,DC, USA, IEEE Computer Society. 2016. pp. 660–667. doi: 10.1109/ASONAM.2012.110

15. Simmonds, A; Sandilands, P; van Ekert, L. An Ontology for Network Security Attacks. Lecture Notes in Computer Science. Lecture Notes in Computer Science. 3285. 2016. pp. 317–323. https://doi.org/10.1007/978-3-540-30176-9_41

Надійшла: 16.10.2023 Рецензент: д.т.н., професор Гайдур Г.І.