

<https://doi.org/10.31891/2219-9365-2024-78-11>

УДК 004.738.5

АХРАМОВИЧ Володимир

Державної університет інформаційно-телекомунікаційних технологій

<https://orcid.org/0000-0002-0086-9131>

e-mail: [12z@ukr.net](mailto:12z@ukr.net)

АХРАМОВИЧ Вадим

Національна академія статистики, обліку та аудиту

<https://orcid.org/0009-0003-2787-8745>

e-mail: [12zstzi@gmail.com](mailto:12zstzi@gmail.com)

ПРИДИБАЙЛО Роман

Державної університет інформаційно-телекомунікаційних технологій

<https://orcid.org/0009-0003-1747-7518>

e-mail: [drake0103@gmail.com](mailto:drake0103@gmail.com)

ЧУПРУН Сергій

Державної університет інформаційно-телекомунікаційних технологій

<https://orcid.org/0009-0007-7336-1068>

e-mail: [ua0988888424@gmail.com](mailto:ua0988888424@gmail.com)

## МЕТОД ДОСЛІДЖЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ВІД КІЛЬКОСТІ СПІВТОВАРИСТВ В СОЦІАЛЬНИХ МЕДІА

У цій статті побудовано математичну модель (схему лінійних диференціальних залежностей) та досліджено модель безпеки приватності в залежності від кількості спільнот у соціальних медіа (СМ). В ній розглядаються лінійні схеми безпеки інформації в соціальних медіа. При описі лінійної моделі об'єкт повинен бути хоча б приблизно лінійним. Такий підхід значно полегшує розгляд математичних моделей. Якщо цього не спостерігається, слід дослідити лінійність схеми безпеки.

Дослідження показало, що схема безпеки соціальних медіа є нелінійною.

Ключові слова: соціальна мережа, кількості співтовариств, схема безпеки, нелінійність, диференціальні залежності.

AKHRAMOVYCH Volodymyr, PRYDYBAYLO Roman, CHUPRUN Serhiy

State University of Information and Communication Technologies

AKHRAMOVYCH Vadym

National Academy of Statistics, Accounting and Auditing

## METHOD OF RESEARCHING INFORMATION SECURITY FROM THE NUMBER OF COMMUNITIES IN SOCIAL MEDIA

This article builds a mathematical model (scheme of linear differential dependencies) and investigates the privacy security model depending on the number of communities in social media (SM). It considers linear schemes of information security in social media. When describing a linear model, the object must be at least approximately linear. This approach greatly facilitates consideration of mathematical models. If this is not observed, the linearity of the safety circuit should be investigated.

The components of information security of the information flow in social media, the amount of personal data, the dependence of the speed of the data flow, the dependence of the security of the scheme on the size of the scheme (including the amount of personal data), the dependence of information threats on the number of communities were studied, taking into account: - an indicator reflecting the impact of measures information security; - an indicator reflecting the impact of the speed of data leakage; - an indicator reflecting the impact of the amount of data on the leak; - an indicator reflecting the impact of the amount of communication; - an indicator reflecting the impact of data volume on data leakage; - an indicator that reflects the impact of the number of SM connections on security; - an indicator reflecting the number of vertices in the SM; - the parameter can be used to configure the media partitioning algorithm.

The solution is obtained using the dependence of the harmonic oscillator and is classified into three cases: pre-resonance, resonance and post-resonance regions.

Thus, the influence of the parameter of the number of communities on the parameters of the social media security scheme was investigated. Such research is useful and important from the point of view of information security in the media, since the parameter of the number of communities has a significant impact on the protection index up to 100%.

Research has shown that the social media security scheme is non-linear.

Keywords: social network, number of communities, security scheme, nonlinearity, differential dependencies.

## ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Члени віртуальних спільнот зазвичай організуються відповідно до рівня їхньої участі. Таким чином, є лідери (також звані менеджери спільноти), які зазвичай порушують питання для обговорення або встановлюють правила спільноти; модератори, які стежать за тим, щоб усі учасники дотримувалися цих правил; учасники, які беруть активну участь у розмові (висловлюючи думки, ставлячи запитання тощо); і,

нарешті, у віртуальному співтоваристві ви також знайдете цікавих – тих людей, які читають всю розмову, але не беруть активної участі.

Співтовариства у соціальних мережах є одним із найпоширеніших типів. Серед них Twitter, Facebook, Instagram, TikTok та інші соцмережі. Бренди зазвичай використовують соціальні спільноти для досягнення своїх маркетингових цілей, таких як поширення новин та підвищення поінформованості про бренд. Крім того, ще однією перевагою спільнот у соціальних мережах є можливість відслідковувати дії конкурентів та виявляти тренди, яким слідує цільова аудиторія.

У [1] запропоновано метод виявлення структури спільнот на основі методу максимальної правдоподібності та описано чисельний алгоритм випадкового пошуку з використанням розподілу Больцмана-Гіббса на його основі.

Розбиття  $\Pi^*$ , для якого залежність  $\Pi$  максимізується для всіх можливих розбиттях, називається оптимальним.

Показано, що метод максимальної правдоподібності зводиться до задачі максимізації цільової залежності. Для знаходження максимального значення цільової залежності застосовано підхід, що ґрунтується на методах статистичної термодинаміки. А саме, випадкова конфігурація  $\Pi$  моделюється розподілом Больцмана (Гіббса).

У статті описано математичну модель, в якій граф генерується випадковим чином шляхом завдання параметрів внутрішніх і зовнішніх зв'язків між вершинами і припущення, що спільноти не перетинаються.

Ітерація алгоритму визначається як  $n$  оновлень вершин. Випадкове блукання, що описується розподілом ймовірностей, як відомо, приводить схему до стабільної конфігурації з часом.

Метод максимальної правдоподібності зводиться до задачі максимізації цільової залежності (1). Зауважимо, що ця залежність є потенціалом гедоністичної гри, пов'язаної з графом.

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

де  $m_k$  – кількість зв'язків між вершинами в соціальних медіа,  $n_k$  – кількість вершин в соціальних медіа, а параметр  $\alpha$  може бути використаний для налаштування алгоритму розбиття медіа. Наприклад, в [1] розглянуто два граничних випадки,  $\alpha \rightarrow 0$  та  $\alpha \rightarrow 1$ . У першому з них максимальне значення цільової залежності досягається розбиттям графа в ігровій постановці відповідної великої коаліції  $\Pi N = \{N\}$ , а в другому – розбиттям графа за максимальною кількістю кліків виявилося вірним.

Виникли теоретичні та практичні питання щодо того, як дослідити вплив кількості спільнот на схеми безпеки приватності соціальних медіа.

### АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

В статті [1] досліджено утворення (розбиття) соціальної медіа на співтовариства на основі методу максимальної правдоподібності з максимізацією цільової залежності. Застосовано підхід, заснований на методах статистичної термодинаміки, а саме моделювання випадкової конфігурації  $\Pi$  з розподілом Больцмана (Гіббса).

В роботі [2] представлена математична теорія інфекційних хвороб та її застосування. В статті [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 медіа. 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 безпеки інформації в соціальних медіа від кластеризації, взаємовідносин, середньої довжини шляху між користувачами в соціальних медіа.

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

Не зважаючи на значну кількість публікацій, наразі ще не створено достатньо простого методу дослідження безпеки інформації від кількості співтовариств в соціальних медіа.

### ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою цієї статті є дослідження впливу кількості спільнот та окремих компонентів параметрів соціальних медіа на параметри безпеки персональних даних.

Завдання дослідження побудова математичної моделі (схеми лінійних диференціальних залежностей) та дослідження моделі безпеки приватності в залежності від кількості спільнот у соціальних

медіа (СМ). Розглянути лінійні схеми безпеки інформації в соціальних медіа. Дослідити лінійність схеми безпеки.

### ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Класичний підхід до безпеки персональних даних розрізняє наступне[4,5,11,12]:

$$T_i = [P_i] \quad (2)$$

де:  $T_i$  - набір загроз, що залежить від кількості спільнот,  $P_i$  - це кількість спільноту соціальних медіа.

Така якість, як спільнота, втрачається в процесах з часовими інтервалами [4,7,11]. Кількість інформації в системі дорівнює  $I$ , потік інформації з інформаційної схеми дорівнює  $dI$ , а швидкість зміни цього потоку приймається рівною  $\frac{dI}{dt}$ . Якщо швидкість зміни між кількістю вхідної інформації та швидкістю вихідної інформації дорівнює нулю, то витік інформації відсутній:

$$dI = 0; \frac{dI}{dt} = 0 \quad (3)$$

Від чого залежить витік інформації? По-перше, він залежить від захищеності схеми, тобто від заходів, вжитих для усунення загроз безпеки даних:  $Z$ -показник захищеності інформаційної схеми. Сформулюємо залежність:

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

де-  $Z_p$  показник, що відображає вплив заходів інформаційної безпеки,  $C_v$  - показник, що відображає вплив швидкості витоку даних і  $C_k$  - показник, що відображає вплив обсягу даних на витік.

Це залежність можна інтерпретувати наступним чином. Витік інформації залежить від наступних факторів:

Розміру інформаційної схеми (а отже, певною мірою, і обсяг даних);

Швидкості витоку даних.

Витік інформації контролюється безпекою схеми (заходами, які зводять нанівець загрози інформаційній безпеці).

Розглянемо, від чого залежить безпека схеми. Безпека схеми визначається як здатність схеми протистояти несанкціонованому доступу до приватних даних. Отже, безпека схеми залежить від:

Розміру схеми (а також обсягу даних);

Загрози інформаційній безпеці від порушення комунікації між користувачами.

Сформулюємо залежність:

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

де:  $C_{d2}$  - показник, що відображає вплив розміру схеми на безпеку,  $C_{d1}$  - показник, що відображає вплив безпеки на витік даних,  $m_k$  - кількість зв'язків у СМ,  $n_k^2$  - квадрат кількості вершин у СМ, та параметр  $\alpha$ , який може бути використаний для налаштування алгоритму розбиття медіа. Наприклад, в [1] розглянуто два граничних випадки  $\alpha \rightarrow 0$  та  $\alpha \rightarrow 1$ , в першому з яких максимум цільової залежності досягається розбиттям графа в умовах гри від провідної великої коаліції  $PN = \{N\}$ , а в другому - розбиттям графа за максимальну кількість кліків. Об'єднаємо залежність (4) і (5) в одну систему.

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

Знайдемо стаціонарне положення схеми, що описується системою залежностей (6). Умови стаціонарності  $dI = 0, \frac{dI}{dt} = 0$ . Отже:

$$\begin{cases} Z_p \bar{Z} + (C_v + C_K) \bar{I} = 0 \\ \sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha_i - I(C_{d2} + C_{d1}) = 0 \end{cases} \quad (7)$$

З другого залежності схеми слідує:

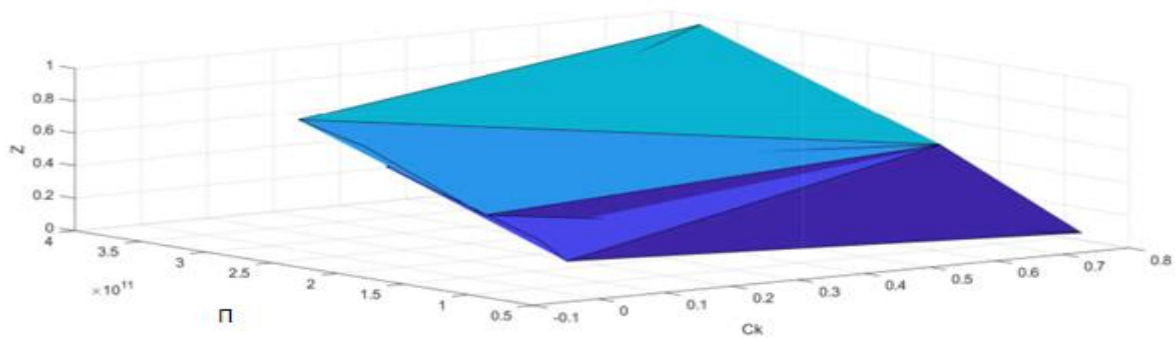
$$\bar{I} = \frac{\sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha_i}{(C_{d2} + C_{d1})} \quad (8)$$

Далі з першого рівняння схеми залежностей (7) знаходимо  $\bar{Z}$ .

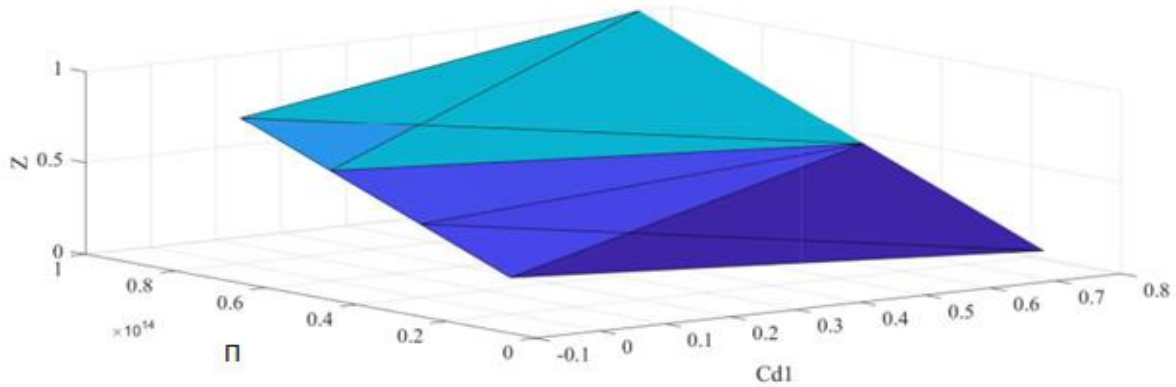
$$Z_p \bar{Z} - \frac{(C_v + C_K) \left( \sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha \right)}{(C_{d2} + C_{d1})} = 0 \quad (9)$$

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

Позначимо  $\sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha = \Pi$ . Результати графічної інтерпретації - (рис. 1)



а)



б)

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

Отже, умови позиції стаціонарності схеми:

$$\left\{ \begin{array}{l} \bar{I} = \frac{\sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha_i}{C_{d2} + Z_p} \\ \bar{Z} = \frac{(C_v + C_K) \left( \sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha_i \right)}{(C_{d2} + C_{d1}) Z_p} \end{array} \right. \quad (11)$$

Способом «малих відхилень» обчислимо схему залежностей (6)

$I = \bar{I} + I; Z = \bar{Z} + Z$  ;, тоді, схема залежностей має вигляд:

$$\left\{ \begin{array}{l} \frac{dI}{dt} = Z_p (\bar{Z} + Z) + (C_v + C_K) (\bar{I} + I) \\ \frac{dZ}{dt} = \left( \sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha \right) - (\bar{I} + I) (C_{d2} + C_{d1}) \end{array} \right. \quad (12)$$

$$\left\{ \begin{array}{l} \frac{dI}{dt} = (C_{d1} + C_{d2}) Z - (C_v + C_K) I \\ \frac{dZ}{dt} = -I (C_{d2} + C_K) + \left( \sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha_i \right) \end{array} \right. \quad (13)$$

Результат диференціювання першої залежності схеми (13):

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

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

Графічна інтерпретація представлена на рис. 2.

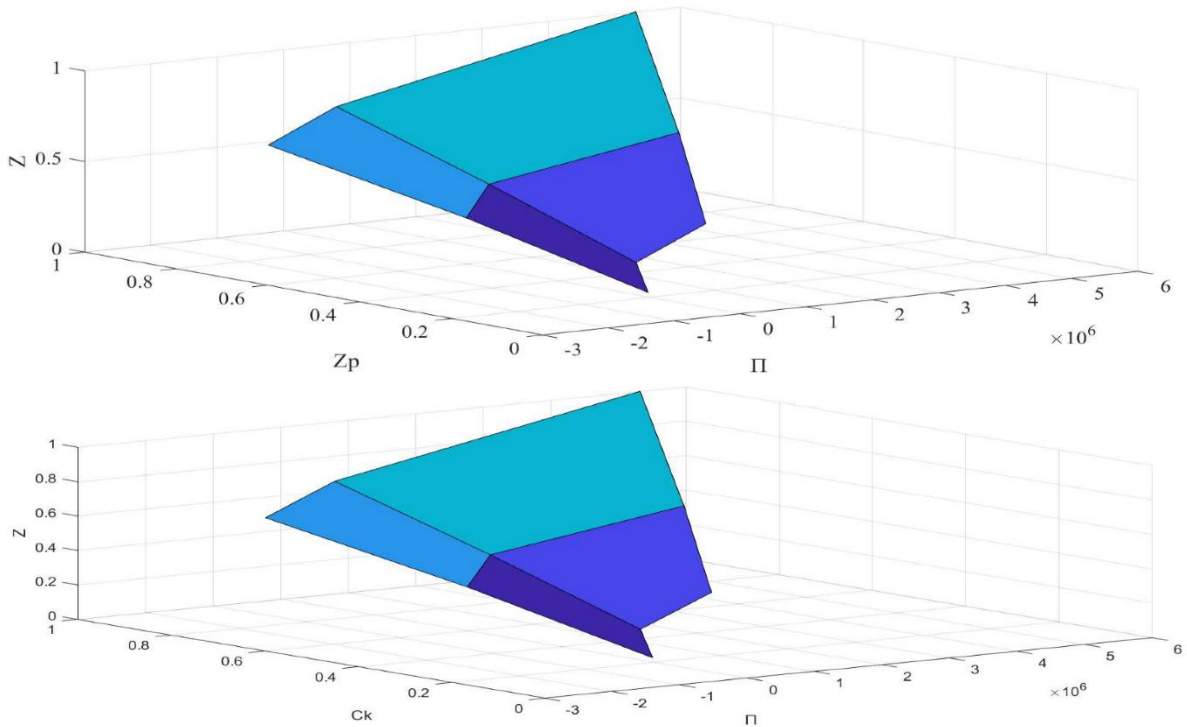


Рис. 2 Значення показника безпеки від складових за (15) при  $n = 100000$   $m = 500000$

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

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

Графічна інтерпретація представлена на рис. 3.

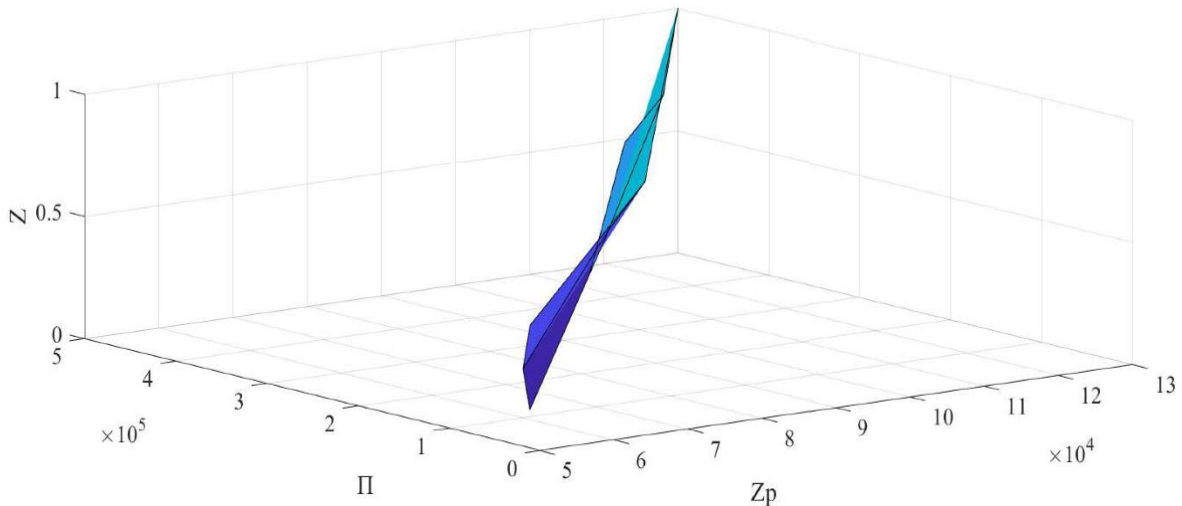


Рис. 3 Особиста частота схеми безпеки при  $n = 100000$   $m = 500000$

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

Графічна інтерпретація представлена на рис. 4.

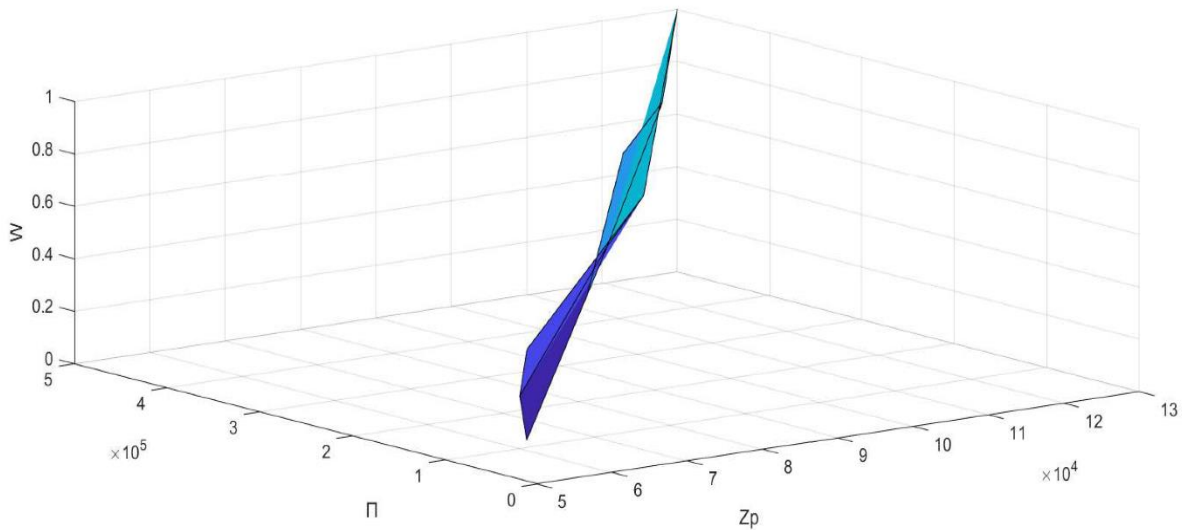


Рис. 4 Частота схеми безпеки при  $n= 100000$   $m= 500000$

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

Графічна інтерпретація представлена на рис. 5.

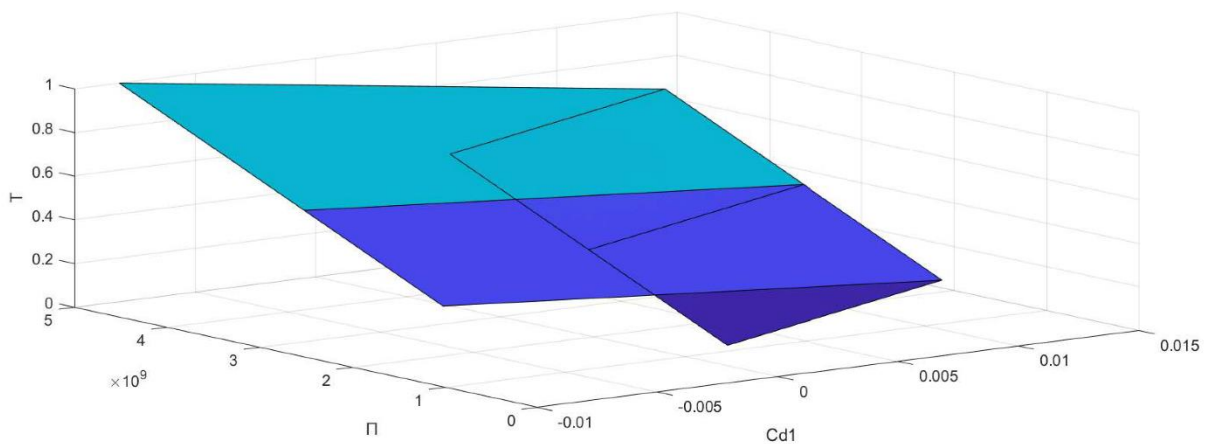


Рис. 5 Період коливань схеми безпеки при  $n= 100000$   $m= 500000$

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

Розв'язок залежності гармонічного осцилятора можна розділити на три випадки.

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

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

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

де

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

Розглянувши три варіанти залежностей поблизу стаціонарного стану схеми, можна зробити висновок, що, виходячи з умов співвідношення дисипації та власних частот коливань величин, останні спадають до певного значення періодично, із затухаючими амплітудами або за законом експоненціального спаду [1,3,13]. Проаналізуємо поведінку схеми більш наочно, перейшовши від диференціальної форми залежностей (5,6) до дискретної та змодельовавши певний інтервал існування схеми. А саме:

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

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

Спочатку коефіцієнти  $C_{d1}, C_v, C_{d2}, Z_p, C_k, P$  дорівнюють 1. Відповідно до умови стаціонарного положення схеми,  $I$  та  $Z$  дорівнюють 0,5 та 0,5. Крок моделювання приймається рівним 0,1 для всіх ітерацій моделювання і тому не показаний в таблиці. Значення  $I_{sp}, Z_{sp}$  відображає стаціонарне значення параметра, яке досягається за скінченну кількість ітерацій. Потім моделювання виконується для значень  $\beta < \omega_0, \beta = \omega_0, \beta > \omega_0$ , які відхиляються від стаціонарного положення схеми. Дані представлені в таб.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	$\beta < \omega_0$
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	$\beta > \omega_0$

Графічна інтерпретація результатів.

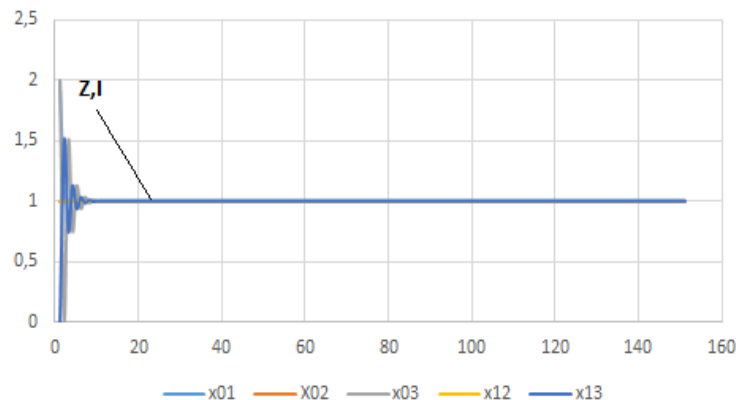


Рис 6 Залежність інтенсивності та безпеки даних від кількості ітерацій (140). Дані складових взяті з табл. 1.  $\beta < \omega_0$ , через  $i$  позначено кількість ітерацій.



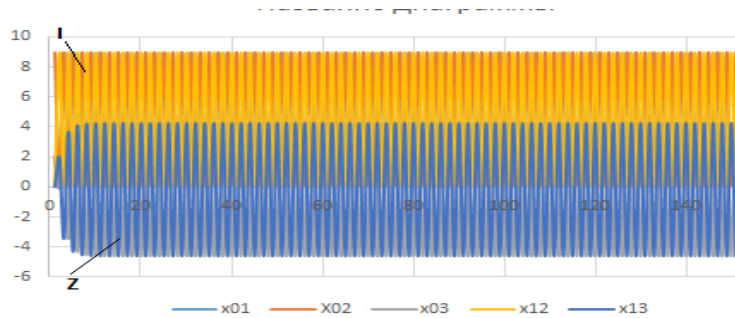


Рис 7 Залежність інтенсивності та безпеки даних від кількості ітерацій (140).  $\beta = \omega_0$ ,

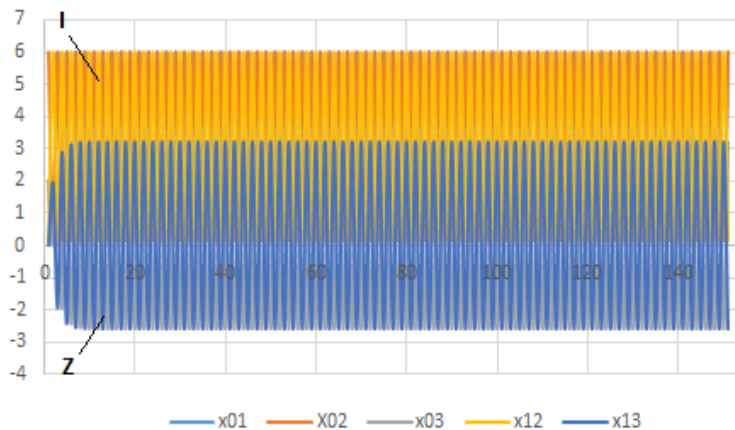


Рис 8 Залежність інтенсивності та безпеки даних від кількості ітерацій (140).  $\beta > \omega_0$ ,

### ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Залежність (2) відображає класичний підхід до безпеки персональних даних. Отримано схему лінійних диференціальних залежностей (6), що описує схему безпеки соціальних медіа. Досліджено стаціонарне положення схеми, що описується системою залежностей (7) та (11). Розв'язок схеми залежностей (6) отримано методом "малого відхилення"(13). Залежність гармонічного осцилятора отримано шляхом диференціювання першої залежності схеми (13). Розв'язки залежностей гармонічного осцилятора (14), (15) були розділені на три випадки відповідно до відношення частоти схеми до коефіцієнта демпфування(20)-(22).

Результати показують, що система інформаційної безпеки є нелінійною. Це пов'язано з тим, що за межами резонансної області були виявлені незатухаючі коливання схеми безпеки (рис.8) [13]. Що зумовило подальші дослідження нелінійної схеми безпеки.

Особливістю запропонованого методу та отриманих результатів є те, що кількісні показники безпеки інформації отримуються з певних параметрів соціальних медіа, зокрема кількості спільнот. Існуючі методи дослідження не дозволяють отримати такі показники. На відміну від попередніх досліджень, отримані результати свідчать про нелінійність схеми безпеки СМ. Розроблено математичну модель впливу певного набору параметрів медіа на схему безпеки.

1. Дослідження лінійної моделі і рекомендації впливу спільнот в СМ на схему безпеки дозволило перейти від класичного підходу до схеми диференціальних залежностей, отримавши математичні залежності між певними параметрами соціальних медіа, зокрема кількістю спільнот та показниками безпеки. Результатом дослідження стали залежність для гармонічних осциляторів із загасаючими амплітудами. Це дозволило визначити частоту, період і показник загасання схеми безпеки. Отримано математичні залежності поведінки схеми безпеки в дорезонансному та післярезонансному режимах. Такий підхід дозволив перейти до дослідження лінійності схеми безпеки.

2. Дослідження лінійності схеми безпеки інформації показали її нелінійність. Це було доведено шляхом розгляду трьох розв'язків залежностей осцилятора поблизу стаціонарного стану схеми. Що дозволило акцентувати увагу на періодичному спаді останнього до певного значення, виходячи з умов співвідношення дисипації та власної частоти коливань. Амплітуда коливання-це амплітуда, яка спадає за експоненціальним законом спаду. Перехід від диференціальної форми залежності до дискретної та моделювання певної ділянки, де присутня схема, дозволяє більш наочно проаналізувати поведінку схеми.

Аналіз повторних коливань схеми безпеки виявляє її нелінійність. Це дозволяє перейти до вивчення нелінійних систем безпеки.

Подальшим розвитком цього дослідження є виявлення нових факторів і параметрів з використанням відомих специфічних для соціальних медіа параметрів (наприклад, взаємний вплив, медіа-експансія, показник кластеризації, дифузія інформації, медіа-центральність і т.п.). Подальшого дослідження потребують нелінійні схеми безпеки персональних даних соціальних медіа.

### Література

1. Ахрамович Володимир, Лазаренко Сергій, Мартинюк Ганна, Баланюк Юрій. Модель пошуку співтовариств в соціальній медіа. Безпека інформації. К. НАУ:-2020.Том 26, -№1.-с. 35-41.
2. N. Bailey, "The Mathematical Theory of Infectious Diseases and Its Applications", New York: Hafner Press, 1 Applications, Vol. 405, pp. 159–170, July 2014.
3. F. Cohen, "Computer viruses, theory and experiments", Computers & Security. Vol. 6. - pp. 22 – 35, 2020.
4. D. Gubanov, 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, S. White, «Directed-Graph Epidemiological Model of Computer Viruses». IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 343, 2021.
6. 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. (Scopus).
7. Volodymyr Akhramovych, Yuriy Pepa, Anton Zahynei1, Vadym Akhramovych, Taras Dzyuba, Ihor Danylov. Method for calculating the information security indicator in social media with consideration of the path duration between clients. Informatyka, Automatyka, Pomiar w Gospodarce i Ochronie Środowiska" – IAPGOS. Volume № 14, Number 1 (2024), pp. 71–77. DOI: <http://doi.org/10.35784/iapgos.5720.2024.03.31>. Scopus/
8. V. Akhramovych, G. Shuklin, Y. Pepa, T. Muzhanova, S. Zozuli. "Devising a procedure to determine the level of informational space security in social networks considering interrelations among users", Eastern-European Journal of Enterprise Technologies, Kharkiv, № 1/9 (115). pp. 63-74, 2022.
9. T. Williamson, M. Matthew; L. Jasmin, "Epidemiological model of virus spread and cleanup", Hewlett-Packard Laboratories Bristol, February 27th, 2023. [URL: <http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf>].
10. Y. Zan, J. Wu, P. Li, 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, J. Zhu, "Stability analysis of I2S2R rumor spreading model in complex networks", Physica A: Statistical Mechanics and its Applications, Vol. 503,. pp. 862–881, 2020.
12. N. Zhao, X. Cheng, "Impact of information spread and investment behavior on the diffusion of internet investment products", Physica A: Statistical Mechanics and its Applications, Vol. 512,. pp. 427–436, 2021.
13. Д.И. Трубецков, " Введение в синергетику. Хаос и структуры", Изд. 2–е испр. И доп.– М. Едиториал. УРСС, 240с, 2004.

### References

1. Akhramovych Volodymyr, Lazarenko Serhiy, Martyniuk Hanna, Balanyuk Yuriy. A model for finding communities in social media. Information security. K. NAU: - 2020. Volume 26, - No. 1. - p. 35-41.
2. N. Bailey, "The Mathematical Theory of Infectious Diseases and Its Applications", New York: Hafner Press, 1 Applications, Vol. 405, pp. 159–170, July 2014.
3. F. Cohen, "Computer viruses, theory and experiments", Computers & Security. Vol. 6. - pp. 22 – 35, 2020.
4. D. Gubanov, 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, S. White, «Directed-Graph Epidemiological Model of Computer Viruses». IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 343, 2021.
6. 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. (Scopus).
7. Volodymyr Akhramovych, Yuriy Pepa, Anton Zahynei1, Vadym Akhramovych, Taras Dzyuba, Ihor Danylov. Method for calculating the information security indicator in social media with consideration of the path duration between clients. Informatyka, Automatyka, Pomiar w Gospodarce i Ochronie Środowiska" – IAPGOS. Volume № 14, Number 1 (2024), pp. 71–77. DOI: <http://doi.org/10.35784/iapgos.5720.2024.03.31>. Scopus/
8. V. Akhramovych, G. Shuklin, Y. Pepa, T. Muzhanova, S. Zozuli. "Devising a procedure to determine the level of informational space security in social networks considering interrelations among users", Eastern-European Journal of Enterprise Technologies, Kharkiv, № 1/9 (115). pp. 63-74, 2022.

9. T. Williamson, M. Matthew; L. Jasmin, "Epidemiological model of virus spread and cleanup", Hewlett-Packard Laboratories Bristol, February 27th, 2023. [URL: <http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf>].
10. Y. Zan, J. Wu, P. Li, 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, J. Zhu, "Stability analysis of I2S2R rumor spreading model in complex networks", *Physica A: Statistical Mechanics and its Applications*, Vol. 503., pp. 862–881, 2020.
12. N. Zhao, X. Cheng, "Impact of information spread and investment behavior on the diffusion of internet investment products", *Physica A: Statistical Mechanics and its Applications*, Vol. 512., pp. 427–436, 2021.
13. D.I. Trubetskov, "Introduction to Synergetics. Chaos and Structures", *Izd. 2nd expt. And supplement. – M. Editorial. URSS*, 240 p., 2004.