



DOI 10.28925/2663-4023.2022.15.3552

УДК 004.738.5

**Ахрамович Володимир Миколайович**

доктор технічних наук, професор

Державний університет телекомунікацій, Київ, Україна

ORCID ID: 0000-0002-6174-5300

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

## РОЗРОБКА МЕТОДУ РОЗРАХУНКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ЦЕНТРАЛЬНОСТІ МЕРЕЖІ

**Анотація.** Розроблено лінійну математичну модель і проведено дослідження моделі захисту персональних даних від параметрів центральності 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); загрози безпеці інформації від параметрів центральності 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 параметрів центральності 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 затухаючою 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:** параметри, центральність, соціальна мережа; потік; інформація; дані; витік; коефіцієнт; рівняння.

### ВСТУП

Метрики центральності – це кількісна оцінка тієї чи іншої особи в соціальній мережі. Міра центральності описує випуклість конкретного вузла в порівнянні з іншими вузлами. Середня міра центральності також відома як централізована оцінка, вона вказує, наскільки щільний граф по відношенню до кожного вузла. Центральні метрики, як правило, обчислюються на підставі всієї структури мережі або підграфа.

#### Центральність вузла

Степінь центральності вершини графа (degree centrality) – це число зв'язків даної вершини з іншими вершинами. Такий вид центральності, як правило, використовується в тих випадках коли необхідно визначити користувачів, для взаємодії які вибирають Вас та яких виберете Ви або, навпаки, від яких хочете триматися подалі. Степінь центральності вершини (вузла) визначається із залежності [3,5]

$$C_D(i) = \sum_{j=1}^n a(i, j), \quad (1)$$

де  $C_D(i)$  – степінь центральності вузла  $i$ ;  $a(i, j)$  – зв'язок між вершинами  $i$  та  $j$ ,  $n$  – число вершин в мережі;  $a(i, j) = 1$  тоді коли вершини зв'єднані ребром.

Щоб можна було порівнювати степінь центральності вузла не тільки всередині одного графа, але і між графами різної структури [8], необхідно розрахувати нормовану центральність вузла,

$$C'_D(i) = \frac{C_D(i)}{n-1} \quad (2)$$

де  $C'_D(i)$  – нормована степінь центральності вершини  $i$ ;  $C_D(i)$  – степінь центральності вершини  $i$ ;  $n$  – число вершин в мережі.  $C'_D(i)$  лежить в інтервалі від 0 до 1 і характеризує зв'язок даної вершини з іншими в мережі. По суті, нормована степінь центральності вузла  $i$  є аналогом індексу соціометричного статусу члена групи ( $C_i$ ), а нормована степінь вихідної центральності вузла є аналогом індексу емоційної експансивності члена групи.

Для порівняння структур мереж і величини валентності вершини знаходять степінь центральності всієї мережі за формулою Фрімана [8]

$$C_D = \frac{\sum_{i=1}^n (C'_D(i) - C_D(i))}{(n-1)(n-2)} \quad (3)$$

де  $C_D$  – центральність мережі;  $C'_D(i)$  – максимальна центральність вершини в мережі;  $C_D(i)$  – центральність мережі;  $n$  – число вершин в мережі.

Центральність як посередництво (betweenness). Центральність вузла в цьому випадку визначається кількістю користувачів, які проходять через цю вершину [3,8], щоб досягти іншої вершини:

$$C_B(i) = \sum_{j-k} \frac{g_{jk}(i)}{g_{jk}} \quad (4)$$

де  $C_B(i)$  – центральність як посередництво вузла  $i$ ;  $g_{jk}(i)$  – число найкоротших шляхів, що з'єднують  $j$  і  $k$  та проходять через вершину  $i$ ;  $g_{jk}$  – загальна кількість коротких ребер, що з'єднують  $j$  і  $k$ . Можна розрахувати стандартизовану оцінку центральності вузла як його посередництва (нормовану центральність як посередництво вузла)

$$C'_B(i) = \frac{C_B(i)}{\frac{(n-1)(n-2)}{2}} \quad (5)$$

де  $C_B(i)$  – нормована центральність, як посередництво вузла  $i$ .  $\frac{(n-1)(n-2)}{2}$  –

максимальна кількість зв'язків між всіма вершинами мережі [8] (за виключенням самої вершини, число пар вершин).

Стандартну оцінку центральності [8], як посередництво для всього графа можна

розрахувати за наступною залежністю:  $C_B = \frac{\sum_{i=1}^n (C_B^i(i) - C_B'(i))}{(n-1)}$ , де  $C_B'$  – нормована

ступінь центральності як посередництво для всього графа;  $(C_B^i(i))$  – нормована максимальна степінь центральності.

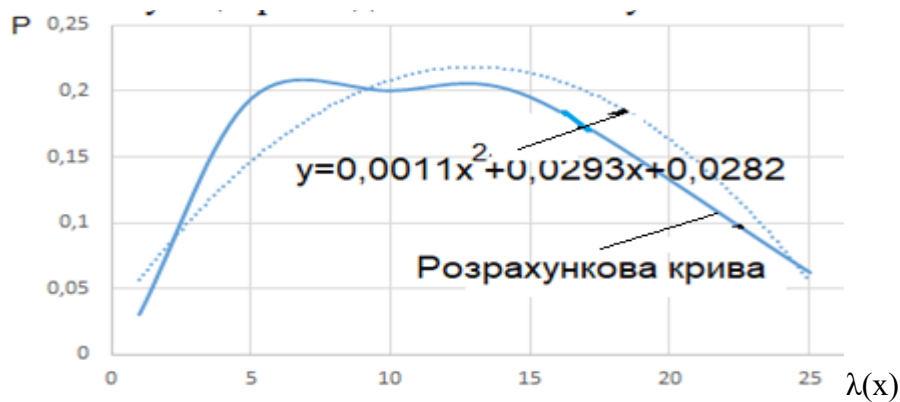
В роботі [3] запропонований варіант центральності, що не залежить від розмірів

мережі. Це відносна центральність за ступенем:  $C_D^i(i) = \frac{\sum_{j=1}^n a_{ij}}{n-1}$ , оскільки кожне ребро графа, це маршрут одиничної довжини, то можна сприймати підрахунок центральності графа як підрахунок таких шляхів які почануться або закінчуються в вершині.

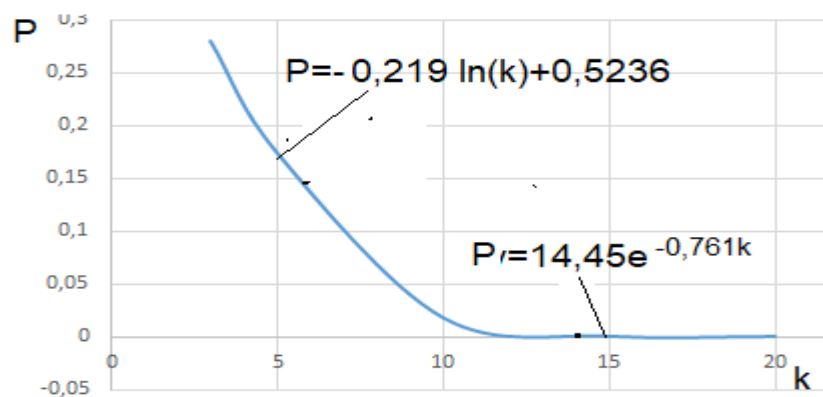
Для випадкових графів легко порахувати функцію розподілу ступеня вузлів: вона описується формулою Бернуллі:

Для випадкових графів легко порахувати функцію розподілу ступеня вузлів: вона описується формулою Бернуллі:

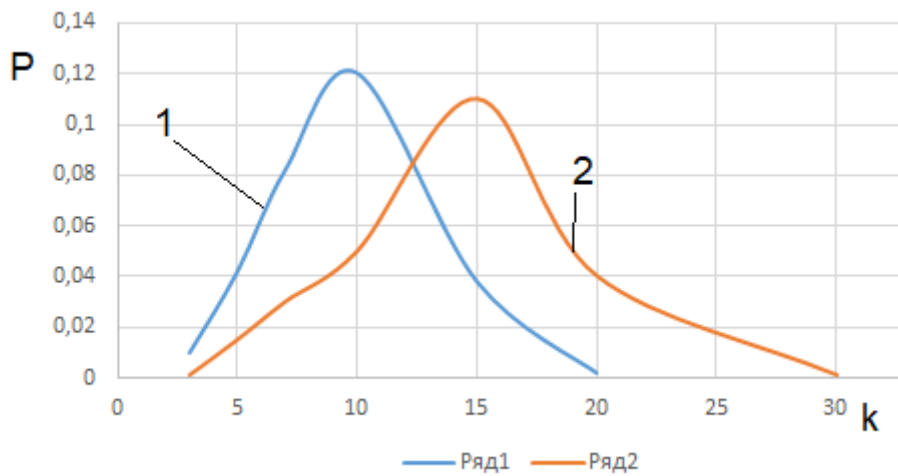
$$P(k_i = k) = P(k) = C_{n-1}^k p^k (1-p)^{n-1-k} \quad (6)$$



а)



б)



в)

Рис. 1 Функція розподілення степені вузла від  $\lambda$  а)  $k=25$ , б) від  $k \lambda=5$ , функція має розрив в точці  $k=12$ , в) від  $k$  крива 1 –  $\lambda=10$ , крива 2 –  $\lambda=15$

Відомо, що у розподілу Бернуллі є граничний випадок: якщо  $n \rightarrow \alpha$  але  $n \rightarrow \infty$  при цьому зафіксувати середнє значення,  $k=np=\lambda$  тоді це розподіл перетворюється в розподіл Пуассона

$$P(k) = \frac{k^k e^{-k}}{k!} = \frac{\lambda^k e^{-\lambda}}{k!} \quad (7)$$

Результати моделювання представлені на рис. 1.

Цей розподіл дискретний, тобто  $k$  має цілочисельне значення. З графіка рис. 1, в видно, що функція розподілення степені вузла від  $\lambda$  близька до нормального розподілу при значних величинах  $\lambda$  і має функцію з розривом (рис. 1, б) в залежності від зміни  $k$ .

### Мережева щільність.

Діада – найпростіша мережа, яка складається тільки з двох учасників. Саме за допомогою діад досліджуються найбільш типові проблеми мереж, оскільки вже в рамках діади можна зрозуміти, взаємні відносини, чи збігаються ті чи інші процеси. Так, в Україні приблизно половина натурального обороту фірм обслуговується юридичними особами за кордоном, і класична задача для податкових органів – визначити, чи збігається рух фінансових і матеріальних потоків фірм А і В, між якими існує діада. На основі балансу кожної з фірм цього зрозуміти неможливо, а на основі діади можна побачити, що, скажімо, там, де назустріч один одному повинні йти товар і гроші, товар йде, а гроші не йдуть взагалі або йдуть у вигляді 10% ринкової вартості товару.

Щільність – це відношення числа наявних ребер графа до максимально можливої кількості ребер даного графа. Щільність – поширена метрика, вона використовується в першу чергу при порівнянні графів одного розміру, або при порівнянні графа з самим собою в часі. Обчислюється вона за формулою:  $m(n,p) = n$  існуючих зв'язків /  $n$  максимально можливих  $m(n,p) = 2 \cdot np / (n(n-1))$  – де  $np$  – число зв'язків,  $p$  – ймовірність підключення, а  $n$  – число вершин в графі (рис. 2).

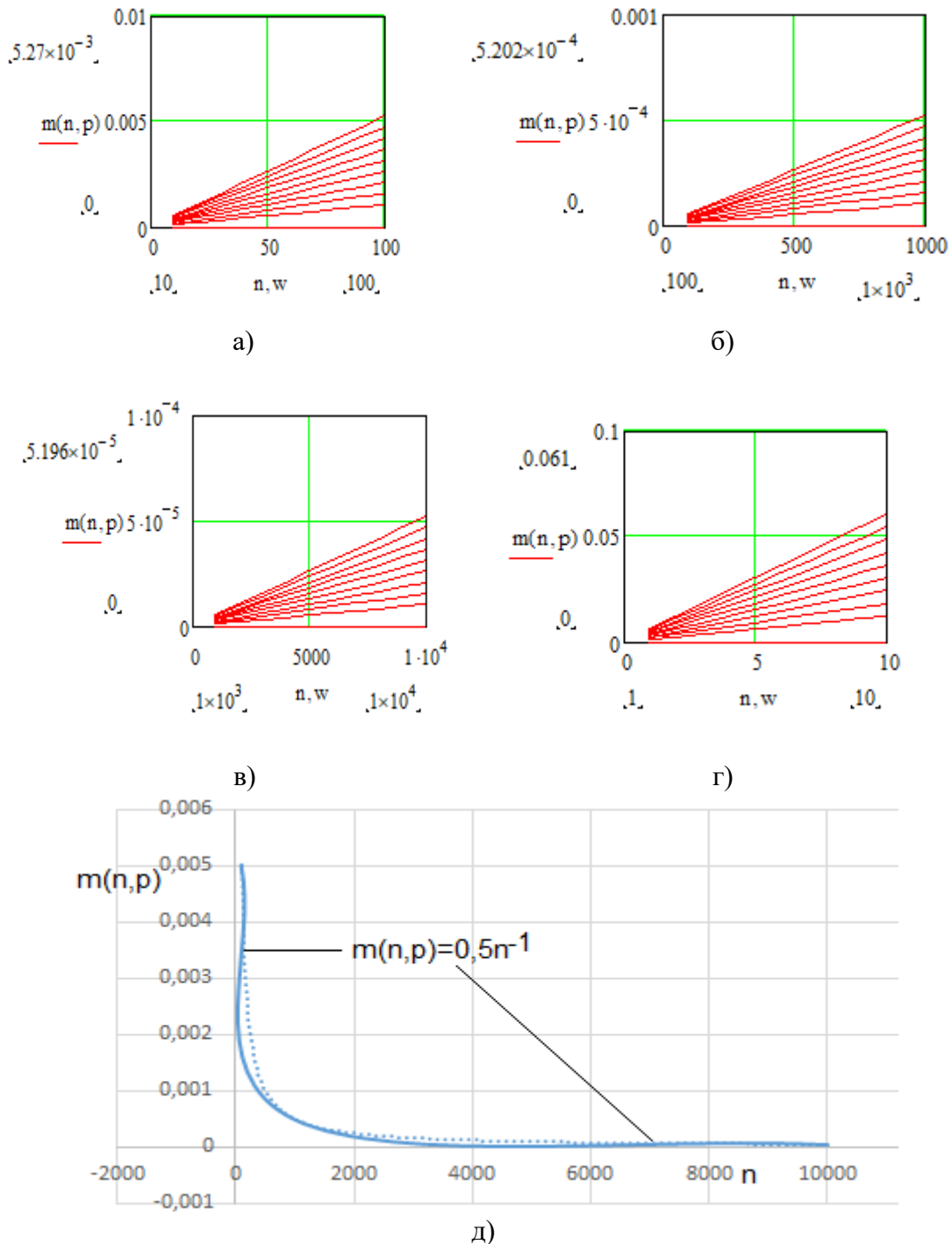


Рис.2 Щільність графа а)  $p=(0, 0.1 \ 1)$ ,  $n=(10, 10 \ 100)$ ; б)  $p=(0, 0.1 \ 1)$ ,  $n=(100, 100 \ 1000)$ ; в)  $p=(0, 0.1 \ 1)$ ,  $n=(1000, 1000 \ 10000)$ ; г) залежність щільності графа від кількості вершин при  $p=1$

Група – це набір користувачів, чії відносини можна виміряти. Проводячи прикладні дослідження, ми повинні виділити якусь групу, про членів якої у нас є статистика, хто погодився відповісти на питання та ін. Але слід пам'ятати, що в мережі існує ще цілий ряд цих же користувачів, якісь ми не можемо виміряти, або нам занадто дорого їх вимірювати. Підгрупа – це виділений в рамках даної групи більш вузький

набір користувачів, для яких характерний особливий тип зв'язку один з одним. Наприклад, в потоці студентів, що нараховує 200 чоловік, є 10 викладачів (одна підгрупа) [8,9], є перша група (інша підгрупа, яка, можливо, перетинається з першою) і т. д. І ми можемо досліджувати взаємодії не тільки окремих користувачів, а й підгруп між собою, виділяючи їх в якості об'єктів дослідження.

Мережа може бути розділена на групи, і кожен індивідуум може належати до будь-якого числа груп. Особистості не обов'язково знають тих, з ким вони розділяють групу, але є ймовірність  $p$  знайомства, яка дорівнює нулю для тих, хто не поділяє групу. Отже, для моделі кластерності характерна тенденція до розбиття мережі на кліки-кластери, які супроводжують визначенням коефіцієнта кластеризації. Для цього спочатку вибирають в мережі деяку вершину  $i$ , що має  $k_i$  ребер, які з'єднують її з іншими вершинами. Якщо перші ближні сусіди цієї вершини є частиною кліки, між ними існує  $\frac{k_i(k_i-1)}{2}$  зв'язків. Відношення між числом  $R_i$  ребер, дійсно існують між розглянутими вершинами, і загальним числом ребер є значенням коефіцієнта кластерності вершини  $i$ :  $\frac{k_i(k_i-1)}{2}$ . Загальний коефіцієнт кластерності мережі знаходиться як сума коефіцієнтів окремих вершин. Коефіцієнт кластерних в середньому по мережі:

$$C^{cp} = \frac{1}{n} \sum_{i=1}^n C_i \quad (8).$$

Діаметром графа є найбільша відстань між двома будь-якими його вершинами. Так, діаметр незв'язною графа (наприклад,

Ердос і Рен) було показано, що середня відстань між двома вершинами у випадковому графі зростає як логарифм від числа вершин)  $\approx \log(n)$  (3.96)

Тим не менше, випадкові графи є малими світами.

Для графів з  $N$  вершинами і ймовірністю зв'язності  $p$ , діаметри можуть лише незначно розрізнятися зазвичай приймають значення.  $d = \ln(N) / \ln(pN) = \ln(N) / \ln\langle k \rangle$ .

Зазвичай під мережевою щільністю розуміють силу зв'язаності в мережі або відношення існуючих та можливих зв'язків. Максимально можлива кількість зв'язків в неорієнтованому графі дорівнює  $g(g-1)/2$ . Щільність зв'язків неорієнтованого графа вираховується за рівнянням

$$\Delta = L / [g(g-1)/2] = 2L / g(g-1), \quad (9)$$

де  $L$  – наявна кількість зв'язків в даному графі, або підграфі. Щільність зв'язків в орієнтованому графі обчислюється за рівнянням:  $\Delta = L / g(g-1)$

З іншого боку, емпіричні результати говорять про те, що для більшості мереж розподіл степені значно відрізняється від розподілу Пуассона. Так, для багатьох мереж, розподіл ступенів вершин має вигляд:  $P(k) \approx k^{-\gamma}$ . Такі мережі називають нешкальованими (масштабно незалежними). Тоді коефіцієнт групування всієї мережі це середня щільність:

$$C = \frac{2E_i}{k_i(k_i-1)}. \quad (10)$$



**Аналіз останніх досліджень і публікацій.** В статті [1,6,10], представлений метод лінійного розрахунку захисту інформації від репутації та взаємовпливу користувачів в соціальних мережах. Розроблена математична модель та проведено дослідження моделі захисту персональних даних від репутації користувачів та інтенсивності передачі даних в соціальних мережах. Розглянуто залежності: величини потоку інформації в соціальній мережі від складових захисту інформації, кількості персональних даних, та швидкості потоку даних; захищеності системи від розмірів системи (як і від кількості персональних даних); загроз безпеки інформації від втрати репутації користувачів. Отримано рішення - рівняння гармонічного осцилятора, яке розпадається на три випадки: дорезонансна зона, резонансна та зарезонансна. Доказано, що система захисту соціальної мережі нелінійна. В статті [2] досліджені математичні моделі оцінки показника захисту інформації в засобах персонального використання та локальній мережі з врахуванням особливостей параметрів, а також функціонування складових в сучасних умовах вказаних засобів та наведена графічна інтерпретація. В статті [3] розглянуті елементи взаємовідносин користувачів в соціальних мережах: показано, що соціальне відношення користувачів мережі являє собою таблицю зв'язності; перетин матриць соціальних відносин та зв'язності; композицію відношень: елементи та типи графів мережі; набір статистики для соціальних відносин; інтенсивність взаємодії груп, ступінь центральності різних користувачів; характеристики мережі соціальних взаємодій - збалансованість і транзитивність; сила структурної позиції користувача; стани діад; вплив структури мережі на модель  $p$ ; ймовірність існування зв'язку між користувачами; залежні та незалежні ребра графа; оцінка параметрів моделі; логіт-моделі. В статті [4] розглянуто нелінійну математичну модель залежності між довірою та показником захисту інформації в соціальній мережі. В статті [5,8] наведені математичні моделі та їх графічна інтерпретація параметрів соціальних мереж, в тому числі, середньої довжини шляху між користувачами. В роботі [7] досліджуються нелінійні моделі та представлена їх графічна інтерпретація. В статті [9] розглядаються соціальні мережі як феномен організації суспільства: сутність та підходи до використання та моніторингу. В статті [11] визначається можливість встановлення дружніх відносин на основі відстані, де дружба є не тільки функцією відстані. Проте, деякі важливі особливості OSN залишаються невідомими, проаналізовані атрибути користувачів. По суті, OSN функціонує відповідно до чотирьох основних властивостей користувача: геолокація користувача, вага користувача, кількість взаємодій з користувачем і тривалість життя користувача. Дослідження, наведене тут, було спрямоване на те, щоб визначити, чи можна використовувати шаблон мобільності користувачів для прогнозування поведінки взаємодії користувачів. Він також досліджував, чи, крім відстані, заважає кількість друзів (відоме як вага користувача) формуванню зв'язків у соціальних мережах. З цією метою проаналізовано вищезазначені особливості у трьох великомасштабних OSN. Виявлено, що, незалежно від високого ступеня свободи мобільності користувачів, частка кількості зовнішніх дій над внутрішньою активністю є значною частиною, яка допомагає нам вирішувати проблему поведінки взаємодії з користувачем.

**Мета статті.** Метою дослідження є дослідження впливу параметрів центральності мережі та інших специфічних параметрів соціальної мережі на параметри захисту інформації.

Завдання дослідження - провести дослідження лінійної моделі параметрів центральності мережі в СМ та на її основі перевірити лінійність системи захисту інформації.



## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У класичному підході до захисту персональних даних розрізняють:

$$T_i = [C_D'(i), C_D(i), n] \quad (11)$$

де де  $C_D'(i)$  – максимальна центральність вершини в мережі;  $C_D(i)$  – центральність мережі;  $n$  – число вершин в мережі.

Втрата такої якості, як центральність 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:

$$dI = 0; \frac{dI}{dt} = 0 \quad (12)$$

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:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I \quad (13)$$

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

Інтерпретувати дане рівняння можна наступним чином. Витік інформації залежить:

- від розміру інформаційної системи (отже, в якійсь мірі і від кількості персональних даних);
- від швидкості витоку персональних даних
- витік інформації купірується захищеністю 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:



$$\frac{dZ}{dt} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} - I(C_{d2} + C_{d1}) \quad (14)$$

де:  $n$  - кількість вершин графа;

$C_{d2}$  - коефіцієнт, що відображає вплив розмірів системи на захищеність;

$C_{d1}$  - коефіцієнт, що відображає вплив захищеності на витік інформації.

Об'єднаємо рівняння (13) і (14) в систему.

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_k) I \\ \frac{dZ}{dt} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} - I(C_{d2} + C_{d1}) \end{cases} \quad (15)$$

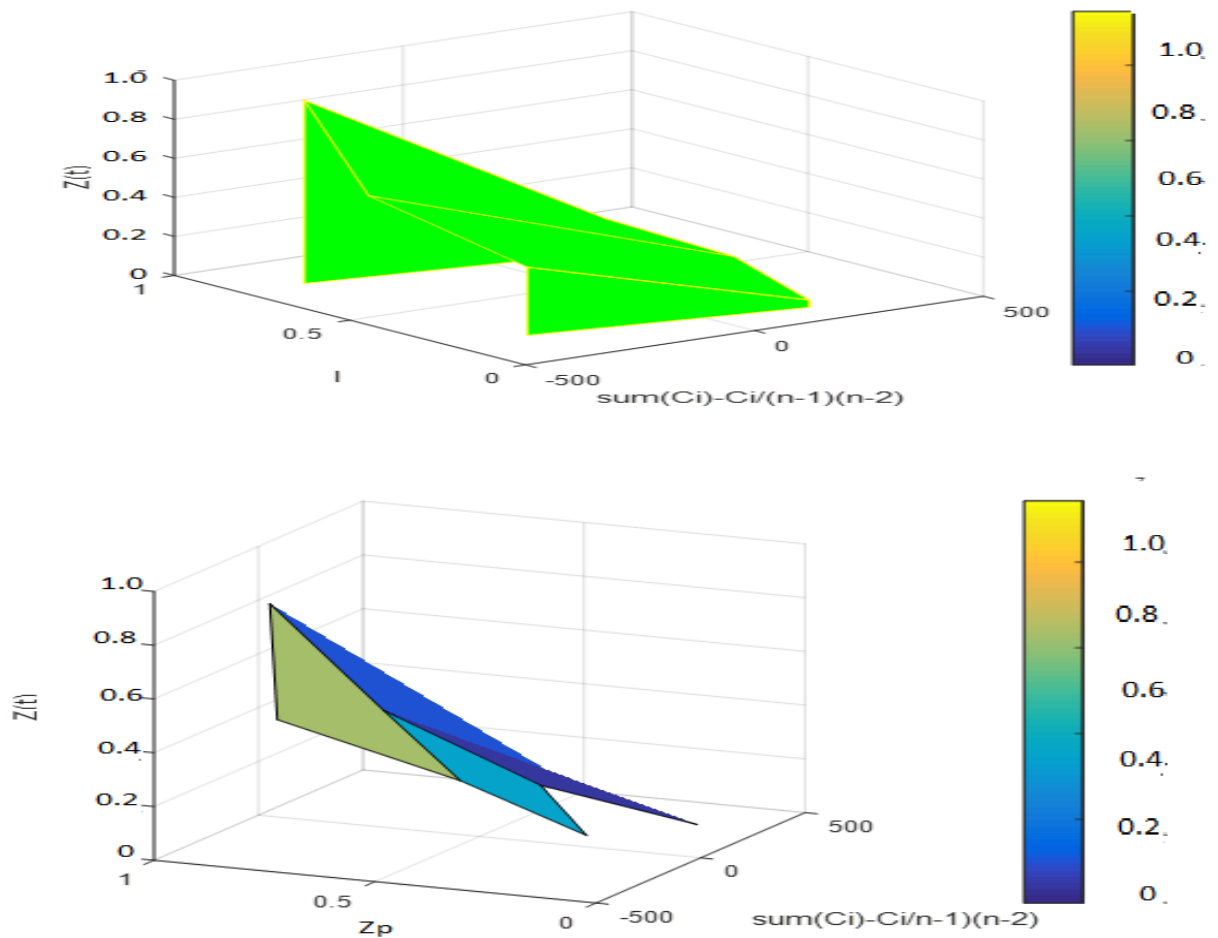


Рис. 3 Залежність показника захисту інформації від складових за (15)

Знайдемо стаціонарну позицію системи, що описується рівняннями (15). Умови

стаціонарності  $dI = 0; \frac{dI}{dt} = 0$ . Отже:

$$\begin{cases} Z_p \bar{Z} + (C_v + C_k) \bar{I} = 0 \\ \sum_{i=1}^n (C_D'(i) - C_D(i)) \\ (n-1)(n-2) - I(C_{d2} + C_{d1}) = 0 \end{cases} \quad (16)$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)(C_{d2} + C_{d1})} \quad (17)$$

Далі з першого рівняння системи рівнянь (16) знаходимо  $\bar{Z}$ .

$$Z_p \bar{Z} - \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))(C_v + C_k)}{(n-1)(n-2)(C_{d2} + C_{d1})} = 0 \quad (18)$$

$$\bar{Z} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))(C_v + C_k)}{(n-1)(n-2)(C_{d2} + C_{d1})Z_p} \quad (19)$$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))(C_v + C_k)}{(n-1)(n-2)(C_{d2} + C_{d1})} \\ \bar{Z} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))(C_v + C_k)}{(n-1)(n-2)(C_{d2} + C_{d1})Z_p} \end{cases} \quad (20)$$

Вирішимо систему рівнянь (15) методом «малих відхилень»

$I = \bar{I} + I; Z = \bar{Z} + Z$  ;, отже, система рівнянь прийме вигляд:

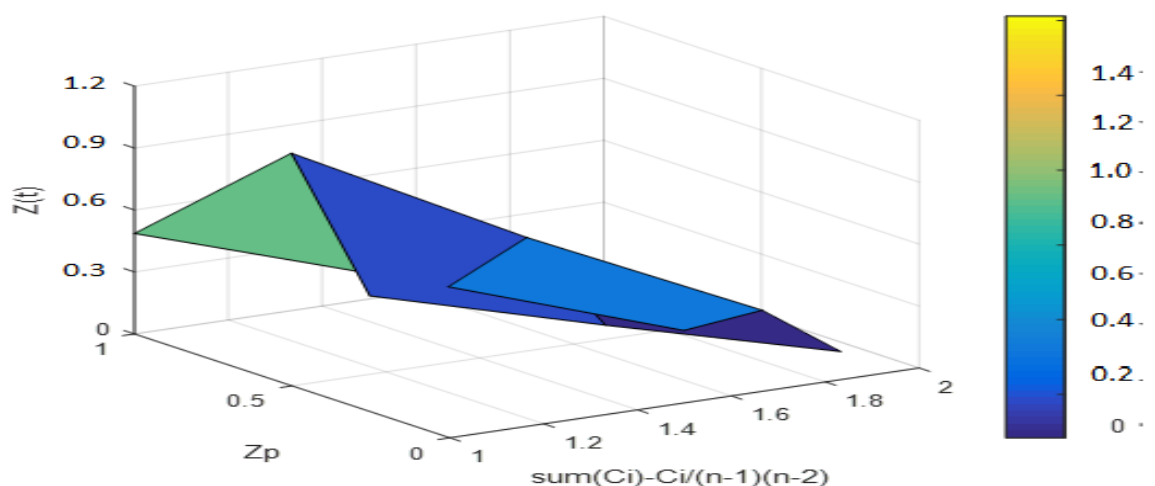
$$\begin{cases} \frac{dI}{dt} = Z_p (\bar{Z} + Z) + (C_v + C_k)(\bar{I} + I) \\ \frac{dZ}{dt} = \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))(C_v + C_k)}{(n-1)(n-2)(C_{d2} + C_{d1})Z_p} - (\bar{I} + I)(C_{d2} + C_{d1}) \end{cases} \quad (21)$$

$$\begin{cases} \frac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_k)I \\ \frac{dZ}{dt} = -I(C_{d2} + C_k) - \frac{\sum_{i=1}^n (C_D'(i) + C_D(i))}{(n-1)(n-2)} (C_v + C_k)_i (C_v + C_k) \end{cases} \quad (22)$$

Диференціюючи перше рівняння системи (15) отримуємо:

$$\frac{d^2 I}{dt^2} = -I(C_{d1} + C_{d2})\left(Z_p - \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} (C_v + C_k)\right) - (C_v + C_k) \frac{dI}{dt} \quad (23)$$

$$\frac{d^2 I}{dt^2} + (C_v + C_k) \frac{dI}{dt} + (C_{d1} + C_{d2})\left(Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} (C_v + C_k)\right)I = 0 \quad (24)$$



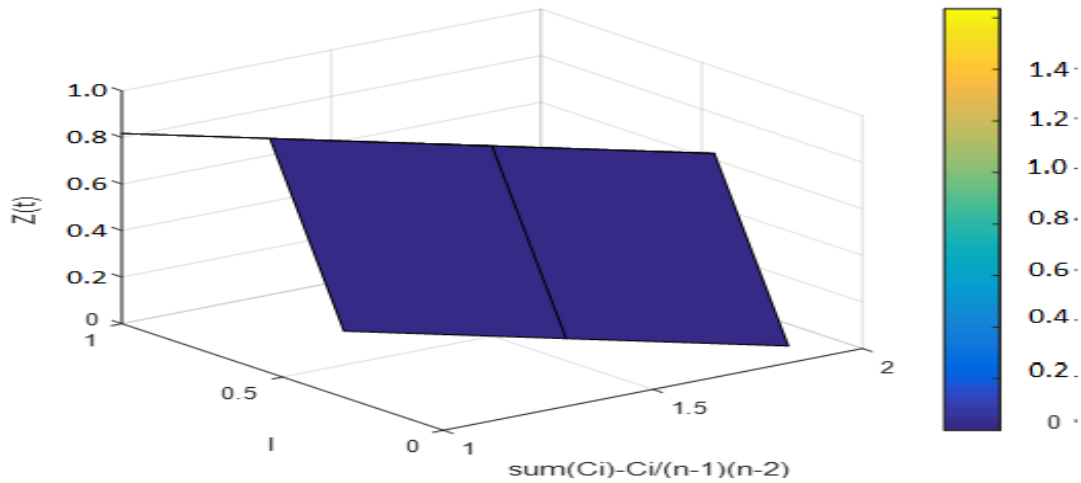


Рис. 4 Значення показника захисту від складових за (24)

Рівняння (22) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де:

$$\omega_0 = \sqrt{(C_{d1} + C_{d2}) \left( Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} \right)} \quad (25)$$

$$\omega = \sqrt{(C_{d1} + C_{d2}) \left( Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} - \frac{(C_v + C_k)^2}{4} \right)} \quad (26)$$

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2}) \left( Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} - (C_v + C_k) - \frac{(C_v + C_k)^2}{4} \right)}} \quad (27)$$

$$\beta = \frac{(C_v + C_k)}{2} \quad (28)$$

Рішення рівняння гармонічного осцилятора розпадається на три випадки.

$$1. \quad \beta < \omega_0 : I = A_0 \exp\left(-\frac{(C_v + C_k)}{2} t\right) \cos\left(\sqrt{\frac{(C_{d1} + C_{d2}) + Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} (C_v + C_k)}{4}} t + \varphi_0\right) \quad (29)$$

Рис. 3 Залежність захисту персональних при умові (27)

$$2. \quad \beta = \omega_0 : I = (A_0 + B_0 t) \exp\left(-\frac{(C_v + C_k)}{2} t\right) \quad (30)$$

$$3. \quad \beta > \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t) \quad (31)$$

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_k)^2}{4} - (C_{d1} + C_{d2} + Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} (C_v + C_k))} \quad (31)$$

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. Виконаємо більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь (14, 15) до дискретної і промодельовавши деякий інтервал існування системи. А саме:

$$\begin{cases} \frac{I_{n+1} - I_n}{\Delta t} = (C_{d1} + C_{d2})Z_n - (C_v + C_k)I_n \\ \frac{Z_{n+1} - Z_n}{\Delta t} = Z_p - (C_{d2} + C_{d1})I_n - (Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} (C_v + C_k))(C_v + C_k)I_n \end{cases} \quad (32)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1} + C_{d2})Z_n - (C_v + C_k)I_n \Delta t \\ Z_{n+1} = Z_n + (Z_n - I_n(C_{d2} + C_{d1} + Z_p + \frac{\sum_{i=1}^n (C_D'(i) - C_D(i))}{(n-1)(n-2)} (C_v + C_k))(C_v + C_k) \Delta t \end{cases} \quad (33)$$

Слідуючи з умови стаціонарної позиції системи,  $I$  і  $Z$  будуть рівні 0.5 і 0.5. Крок моделювання прийемо 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  $\beta < \omega_0, \beta = \omega_0, \beta > \omega_0$  відхиленням від стаціонарної позиції системи. Дані представимо в табл. 1 .

Таблиця 1

**Параметри моделювання**

№ з/П	$Z_p$	I	Z	$C_v$	$C_{d1}$	$C_{d2}$	$C_K$	$C_D(i)$	$C_D(i)$	n	Параметри
1	4,5	0,5	1	1	1	0,5	1	100000	2000	100000	$\beta < \omega_0$
2	4,5	0,5	1	3	1,5	1,5	3	100000	2000	100000	$\beta = \omega_0$
3	4,5	0,5	1	4	1	1	4	100000	2000	100000	$\beta > \omega_0$

Візуалізація результатів (рис. 5-7).

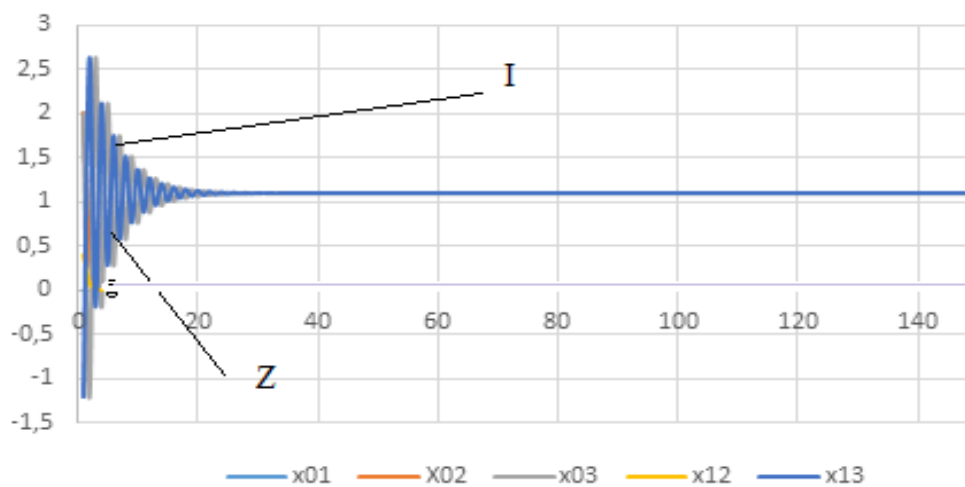


Рис. 5 Залежність інтенсивності та захисту даних від кількості ітерацій (140).

Дані складових взяті з табл. 2.1.  $\beta < \omega_0$ , через і позначено кількість ітерацій.

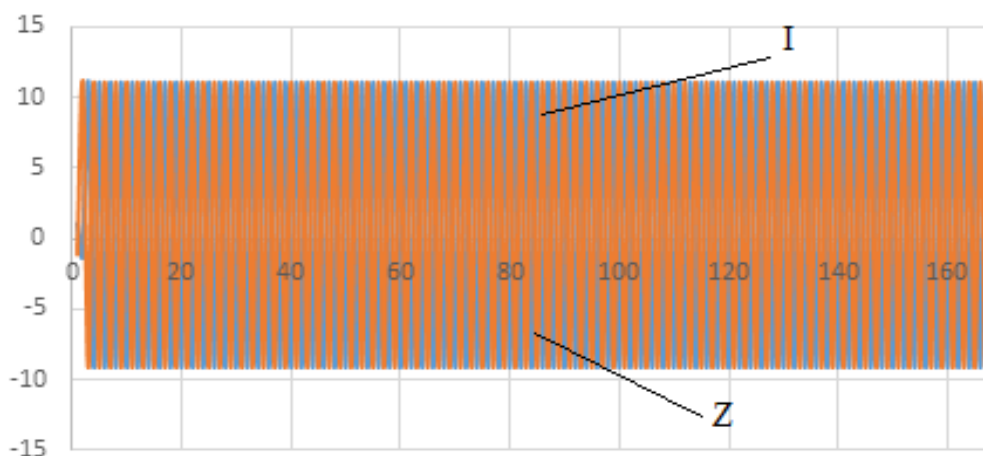


Рис. 6 Залежність інтенсивності та захисту даних від кількості ітерацій (140).  $\beta = \omega_0, Di=0,5$

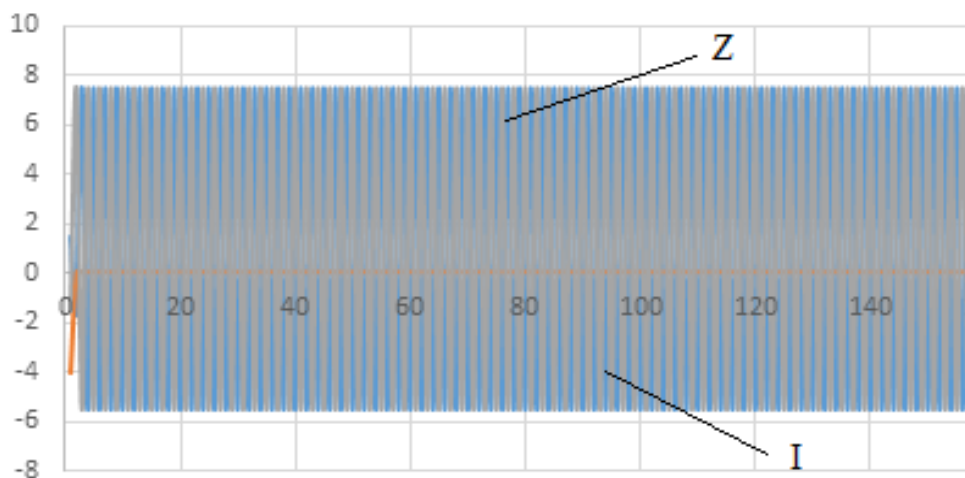


Рис. 7 Залежність інтенсивності та захисту даних від кількості ітерацій (140).  $\beta > \omega_0$ ,  $D_i=0,1$

Аналіз графічних залежностей лінійної системи рис. 7 вказує на нелінійність системи [1,4,7,8]. Необхідне подальше дослідження системи захисту, наприклад, в вигляді нелінійної системи диференціальних рівнянь

**ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ.** Таким чином розроблена математична модель та проведено дослідження моделі захисту персональних даних від параметрів середньої довжини шляху між користувачами мережі та інтенсивності передачі даних в соціальних мережах.

В результаті математичного моделювання доказано, що система захисту соціальної мережі нелінійна [7] на що вказують результати імітаційного моделювання (рис. 9).

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 Akhramovich, V., Hurenko, M. (2020). Estimation of the indicator of protection of information in means of personal use and a local area network. *Colloquium-journal*, 19(116), 36-41.
- 3 Akhramovych, V. (2019). Model of strong and weak connections of users in social networks. *Communication. K. SUT*, 3, 8–12.
- 4 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 1, 15-21.
- 5 Shchypanskyi, P., Savchenko, V., Akhramovych, V., Muzshanova, T., Lehominova, S., Chegrenets, V. (2020). The Model of Secure Social Networks Activity Based on Graph Theory. *International Journal of Innovative Technology and Exploring Engineering*, 9(4), 1803–1810. <https://doi.org/10.35940/ijitee.d1768.029420>.
- 6 Savchenko, V. A., Akhramovych, V. M., Dzyuba, T. M., Laptiev, S. O., Matvienko, M. V. (2021). The method of calculating the protection of information from the interaction of users in social networks. *Modern information security*, 45(1), 6-13. <https://doi.org/10.31673/2409-7292.2021.010613>.
- 7 Trubetskov, D.(2004). *Introduction to Synergetics. Chaos and structures. Edition 2 revised*. M. Edytorial. MDFS.



- 8 Savchenko, V., Akhramovych, V., Tushych, A., Sribna, I., Vlasov, I. (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>.
- 9 Vynnyk, V. D. (2012). Social networks as a phenomenon of the organization of society: the essence and approaches to the use and monitoring. *Philosophy of Science*, 4(55), 110-126.
- 10 Ахрамович, В. М., Вдовиченко, О. В., Загиней, А. Ю. (2021). Метод розрахунку захисту персональних даних від довіри між користувачами та інтенсивності передавання даних у соціальних мережах. *Зв'язок*, 3, 27-34.
- 11 Mahmoudi, A., Yaakub, M. R., & Bakar, A. A. (2019). The Relationship between Online Social Network Ties and User Attributes. *ACM Transactions on Knowledge Discovery from Data*, 13(3), 1–15. <https://doi.org/10.1145/3314204>.





**Akhramovich Volodymyr Mykolayovych**

Doctor of Technical Sciences, Professor

State University of Telecommunications, Kyiv, Ukraine

ORCID ID: 0000-0002-6174-5300

[I2z@ukr.net](mailto:I2z@ukr.net)

## DEVELOPMENT OF A METHOD FOR CALCULATING THE PROTECTION OF PERSONAL DATA FROM THE CENTRALITY OF THE NETWORK

**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 Akhramovich, V., Hurenko, M. (2020). Estimation of the indicator of protection of information in means of personal use and a local area network. *Colloquium-journal*, 19(116), 36-41.
- 3 Akhramovych, V. (2019). Model of strong and weak connections of users in social networks. *Communication. K. SUT*, 3, 8–12.
- 4 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 1, 15-21.
- 5 Shchypanskyi, P., Savchenko, V., Akhramovych, V., Muzshanova, T., Lehominova, S., Chegrenets, V. (2020). The Model of Secure Social Networks Activity Based on Graph Theory. *International Journal of Innovative Technology and Exploring Engineering*, 9(4), 1803–1810. <https://doi.org/10.35940/ijitee.d1768.029420>.
- 6 Savchenko, V. A., Akhramovych, V. M., Dzyuba, T. M., Laptiev, S. O., Matvienko, M. V. (2021). The method of calculating the protection of information from the interaction of users in social networks. *Modern information security*, 45(1), 6-13. <https://doi.org/10.31673/2409-7292.2021.010613>.
- 7 Trubetskov, D. (2004). *Introduction to Synergetics. Chaos and structures. Edition 2 revised*. M. Edytorial. MDFS.
- 8 Savchenko, V., Akhramovych, V., Tushych, A., Sribna, I., Vlasov, I. (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>.
- 9 Vynnyk, V. D. (2012). Social networks as a phenomenon of the organization of society: the essence and approaches to the use and monitoring. *Philosophy of Science*, 4(55), 110-126.



- 10 Akhramovych, V. M., Vdovychenko, O. V., Zahynei, A. Yu. (2021). Metod rozrakhunku zakhystu personalnykh danykh vid doviry mizh korystuvachamy ta intensyvnosti peredavannia danykh u sotsialnykh merezhakh. *Zviazok*, 3, 27-34.
- 11 Mahmoudi, A., Yaakub, M. R., & Bakar, A. A. (2019). The Relationship between Online Social Network Ties and User Attributes. *ACM Transactions on Knowledge Discovery from Data*, 13(3), 1–15. <https://doi.org/10.1145/3314204>.



This work is licensed under Creative Commons Attribution-noncommercial-sharelike 4.0 International License.