DOI: 18372/2310-5461.53.16504

УДК:004.738.5

В. М. Ахрамович, д-р техн. наук, доцент
Державний університет телекомунікацій
orcid.org/0000-0002-6174-5300
E-mail: 12z@ukr.net;

С. В. Лазаренко, д-р техн. наук, доцент,
Національний авіаційний університет
orcid.org/0000-0003-3529-4806
E-mail: zzi.lazarenko@nau.edu.ua;

Т. В. Німченко, канд. техн. наук, доцент,
Національний авіаційний університет
orcid.org/0000-0001-8196-5493
E-mail: zzi.nimchenko@nau.edu.ua;

Л. В. Рябова,
Національний авіаційний університет
orcid.org/0000-0002-9257-6626
E-mail: lubanau@ukr.net

МЕТОД РОЗРАХУНКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД РОЗШИРЕННЯ СОЦІАЛЬНИХ МЕРЕЖ

Вступ

Основна інформація, що зберігається в соціальних мережах (СМ), це самостійно генеровані та підтримувані дані користувачів та їхніх відвідувачів. Такі дані можливо класифікувати так:

- особисті контактні дані, що описують особу користувача;
- підключення, що представляє з'єднання в трафіку соціальної мережі;
- інтереси користувача;
- інформація про автобіографію користувача;
- спілкування, включаючи всі взаємодії з іншими користувачами СМ.

Ці типи даних складають особисту інформацію, яка надається безпосередньо користувачем СМ і можуть бути віднесені до персональних. Персональні дані, згідно Закону України «Про захист персональних даних», це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Додаткова інформація про користувача в СМ часто генерується та стає доступною всередині СМ іншим користувачам.

Мотиви збору інформації показаніна рис. 1. Як видно з рис. 1 існує нагальна потреба захисту персональних даних. Проблема ця є складною, важливою та комплексною. Тому, актуальною є тема дослідження захисту персональних даних в СМ з врахуванням специфіки параметрів, такої інформації, та параметрів розширення мереж.

Існує два принципово різних механізми виникнення степеневих розподілів імовірностей. Один з них ґрунтується на самоорганізації в критичний стан, який відбувається у відкритих, далеких від рівноваги нелінійних системах. Другий пов'язаний з початковою цілісністю системи і в загальному випадку не вимагає ні не лінійності, ні взаємодії елементів системи між собою. Крайнім вираженням цілісного підходу є моделі конкурентного зростання, в яких зміна розміру елемента прямо пропорційна його поточному розміру. При цьому, цілісність використовується лише на рівні знання сумарного розміру системи, необхідного для того, щоб розподілити загальний його приріст між її елементами.

Без цього було б неможливо збалансувати процеси появи в системі нових елементів і зростання вже присутніх в ній. Натомість, впровадження даного не фізичного припущення дозволяє будувати моделі, що утворюють масштабно-інваріантні системи на основі дуже простих правил. Моделі зростання соціальних мереж, зазвичай, будуються за цією ж схемою,

використовуючи принцип переважного приєднання. Згідно цього принципу вузол мережі вибирається для утворення нового зв'язку з імовірністю, пропорційною його валентності — числу вже наявних у нього зв'язків (рис. 2). Однак, на основі локальних правил знання структури графа дозволяє вибирати вузли з такою ймовірністю, яка не потребує ніякої інформації про інтегральні характеристики системи.

Рис. 1. Мотиви та цілі збору даних

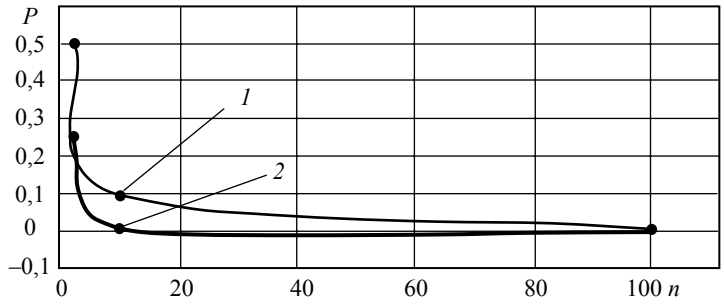


Рис. 2. Степеневий розподіл вершин за валентністю з $\dot{a} = 0.1$(крива *1*) та $\dot{a} = 2.0$ (крива *2*)

Для простоти припустимо, що ми маємо справу з ненаправленим графом. Тоді, вибравши в ньому випадковий вузол, а у цього випадкового вузла — випадкового сусіда, ми отримаємо вузол, обраний випадковим чином.

Формули для показника розподілу, отримані з середньо-польового квазілінійного наближення, розраховуються з високою точністю. Їх емпіричні характеристики визначаються з результатів моделювання.

Аналіз останніх досліджень та публікацій

У статті [1] розроблена та досліджена математична модель пошуку співтовариств в соціальній мережі, у тому числі, з врахуванням параметрів розширення мережі. 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.

У працях [2–3] представлені моделі параметрів СМ, у тому числі її розширення. Основна ідея заснована наприпущенні, що особи зі спільними характеристиками спілкуються один з одним. Це свого роду епідемічна модель з можливістю відправки певної інформації, як функція відстані між джерелом і потенціалом призначення. Основний підхід у статті заснований на кластеризація локальних характеристик мережі. Вони характеризують ступінь взаємодії між найближчими сусідами. Розрахунки проілюстровані графічними матеріалами. Представлено відповідні рівняння, вузол графа.

У статті [4] досліджується лінійна модель системи захисту інформації від специфіки параметрів СМ та параметрів репутації користувачів.

У статтях [5–9] представлені математичні теорії розповсюдження вірусів, хробаків із випадковим постійним скануванням в соціумі та СМпроблеми, що виникають від них. Розкривається актуальність боротьби з ними.

У праці [8] представлені математичні моделі нелінійних систем. У статтях [10–11] представлені математичні моделі розповсюдження слухів в СМ. Розглядаються моделі сприйнятливо-інфекційно-контратакувально рефрактерна (SICR) та скоригована модель SICR. Виведене рівняння середнього поля для опису динаміки слухів в однорідних мережах і проведено стаціонарний аналіз. Виконано чисельне моделювання, для порівняння моделі SICR із моделлю SIR та моделлю скоригованого SICR. Дослідження розкриває деякі цікаві закономірності поширення чуток, пов'язаних із контратакувальною силою.

У статті [12] представлена модель впливу розповсюдження інформації та інвестиційної поведінки користувачів на розповсюдження інвестиційних продуктів в Інтернеті. Розглядається процес поширення інформації, тимчасові інвестиції, регулярні інвестиції та продаж. Результати показують, що позитивний вплив регулярних інвестицій та негативний вплив вибуття (виходу) не чутливі до часового масштабу. Крім того, позитивний вплив звичайної ставки інвестування очевидний лише тоді, коли ставка тимчасового інвестування не надто мала, і навпаки. Крім того, негативний вплив вилучення та відхилення інформації навряд чи можна компенсувати збільшенням звичайної ставки інвестицій.

Постановка проблеми

Модель росту соціальної мережі. Для малих світів типовий степеневий розподіл вершин за валентністю з відповідною щільністю ймовірності має вигляд

$$u(x) \approx x' + a. \quad (1)$$

Для соціальних мереж показник розподілу відповідає розмірності $1< a <2$, хоча для малих світів іншої природи він може бути і більше.

Якщо для відносин людей в реальному світі безпосередній підрахунок зв'язків ускладнений, то для Інтернет-спільнот він не становить особливих труднощів. Інструменти створення блогів (мережевих щоденників) дають можливість підрахунку числа читачів — користувачів, які підписалися на блог для отримання інформації, що публікується в ньому або які виявили особистий інтерес до його власника.

Механізм виникнення розподілів вигляду (1) в зростаючих системах добре відомий. Він пов'язаний з конкуренцією за ресурс, при якій подальший розвиток відбувається тим швидше, чим більше вже досягнуті результати. Стосовно зростання соціальних мереж це означає, що чим вище валентність, тим швидше вона збільшується. Це цілком логічно, оскільки і при реальному, і при мережевому спілкуванні людина в одиницю часу знайомиться з тим великим числом нових цікавих йому людей, чим більше його контакти. Прискорений розвиток передбачає принципову відкритість системи, тобто постійне приєднання до мережі нових вершин.

У моделі приєднання за допомогою посередника (англ. *Mediation-driven attachment, MDA*) новий вузол приходить з m ребрами, для чого вибирається випадковим чином існуючий, пов'язаний вузол, і новий вузол з'єднується, не тільки з цим випадково обраним вузлом, а й також з m його сусідами, обраними також випадково [2; 3]. Нехай Ui — спільнота вузлів і нехай $\mathrm{CS}(t) = Ui$, Ui — скупність всіх існуючих спільнот (CS, спільноти) у момент часу t з $Ui \cap Uj = \geq$ для $i = j$. На початку ($t = t_0$) граф складається тільки з однією спільнотою $U_0 = \mathrm{CS}(t_0)$. Якщо до графа в момент $t + 1$ буде доданий новий вузол U, який додає ймовірність $P(X \geq N)$ до існуючої спільноти $Ui \geq \mathrm{CS}(t)$. З імовірністю $P(X < N)$, U створює нову спільноту $Ui + 1$ і стає її членом. Ми маємо $\mathrm{CS}(t + 1) = \mathrm{CS(t)} \geq U_{i+1}$ — параметр конфігурації моделі, а числове значення N відповідає ймовірності формування нової спільноти. Чим менше буде вибір N, тим менше буде співтовариств. Імовірність того, що новий вузол U генерує нову спільноту $Ui + 1$ і з'єднується з існуючим вузлом $v \geq Ui$, обчислюється за рівнянням (2).

$$P_{Ui+1}\left(\deg(v)X\right) = P\left(\deg\rrbracket(v)P(X < N),\right. \quad (2)$$

де $\deg(v)$ — кількість ребер, що підходять до вершини v.

Імовірність того, що новий вузол U приєднується до існуючої спільноти Ui ($\mathrm{CS}(t)$ і з'єднується з існуючим вузлом $v \geq Ui$ (рис. 3), обчислюється за рівнянням 3.

$$P_{Ui}\left(\deg(v)X\right) = P\left(\deg\rrbracket(v)\right)P(X \geq N). \quad (3)$$

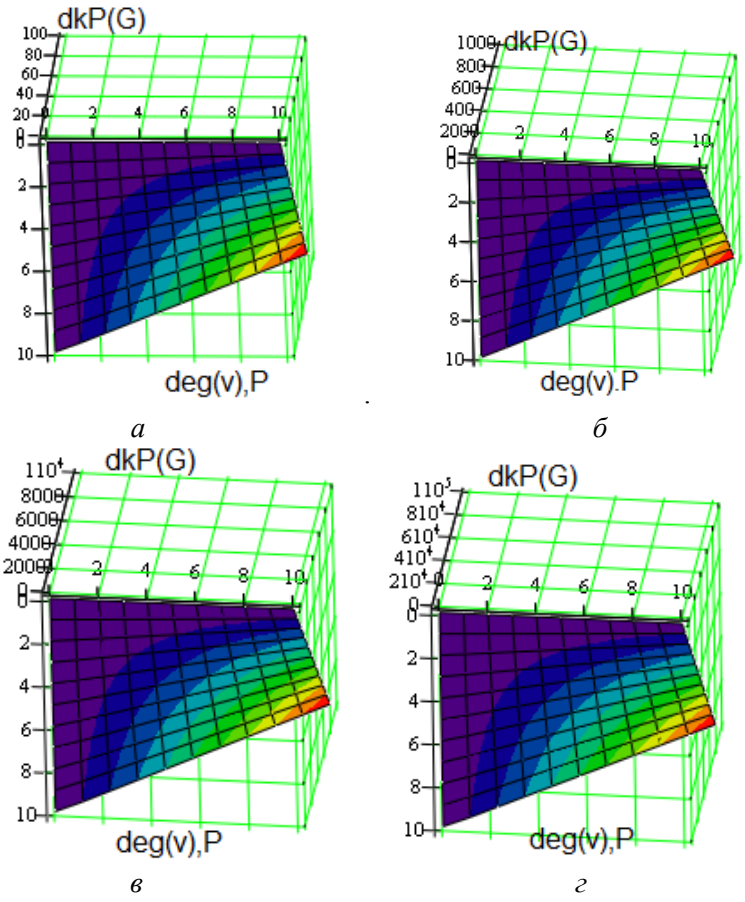
де $d(u, v)$ — сума всіх відстаней між вузлами U, v, V — безліч вузлів U.

Імовірність $P(\deg(U))$, що вузол U обраний для ініціювання взаємодії, обчислюється за рівнянням:

$$P_{(\deg(U))} = \frac{\deg(U)}{\sum_{U \in V} \deg(v)}. \quad (4)$$

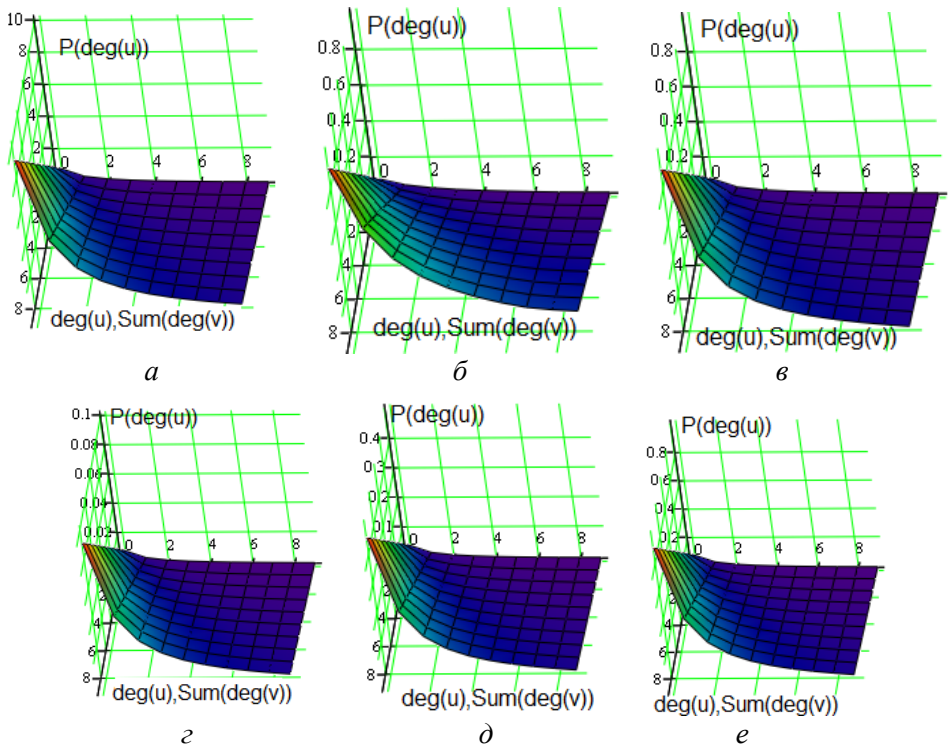
Таким чином, взаємодія вузлів інтерактивної моделі регулює розподіл мережевих взаємодій.

Результати моделювання представлені на рис. 4, 5.



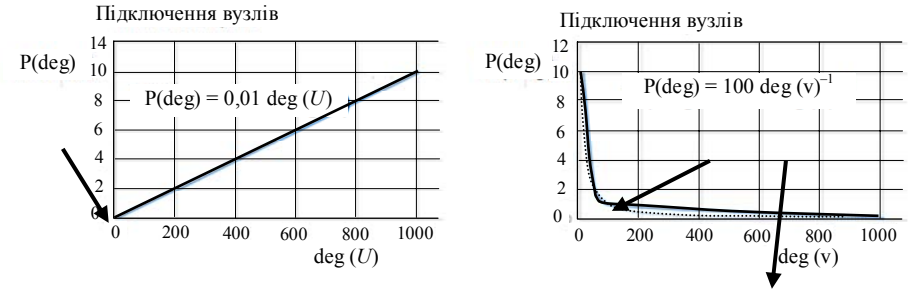
а *б* *в* *г*

Рис. 3. Імовірність нових підключень до мережі:
а — P(deg(*v*) = (0, 10, 100), P = (0, 0.1, 1); *б* — P (deg(*v*) = (0, 100, 1000), P = (0, 0.1, 1);
в — P (deg(*v*) = (0, 1000, 10000), P = (0, 0.1, 1); *г* — P (deg(*v*) = (0, 10000, 100000), P = (0, 0.1, 1)



а *б* *в* *г* *д* *е*

Рис. 4. Взаємодія вузлів в мережі:
а) при deg(u) (1, 1, 10), deg(v) (1, 1, 10);б) при deg(u) (1, 1, 10), deg(v) (5, 10, 50);
в) при deg(u) (1, 1, 10), deg(v) (10, 10, 100);г) при deg(u) (1, 1, 10), deg(v) (100, 100, 1000);
д) при deg(u) (5, 5, 50), deg(v) (100, 100, 1000); е)при deg(u) (10, 10, 100), deg(v) (100, 100, 1000)



а *б*

Рис. 5. Графік та рівняння залежності можливого максимального підключення вузлів:
а — deg(U), deg(v)= (100, 100, 1000); *б* — deg(v), deg(^{u}), (1, 1, 10)

Будемо розрізняти первинні зв'язки, які утворюються з приєднанням нових вершин, і вторинні, які пов'язують вже існуючі вершини.

Вибір вершин для утворення зв'язку може здійснюватися за різними алгоритмами, найпростішими з яких є алгоритми, що використовують тільки інформацію про валентності даної вершини. При цьому ймовірність утворення зв'язку з даною вершиною приймається пропорційною xz, оскільки немає підстав вважати наявність будь-яких характерних масштабів для даного процесу, що означає можливість використання тільки однорідних функцій x.

Найцікавіші тут випадки $z = 0$ і $z = 1$, які відповідають випадковому і переважному способам приєднання.

При випадковому приєднанні ймовірність того, що зв'язок буде створений з даної вершиною, не залежить від її характеристик і дорівнює просто $\frac{1}{n(t)}$, де $n(t)$ — загальне число вершин графа в момент часу t. При переважному приєднанні ймовірність утворення зв'язку з вершиною i, яка вже має x_i зв'язків дає відношення $x_i/S(t)$, де сумарна валентність $S(t) = \sum_{i=1}^{n(t)} x_i(t)$ дорівнює подвоєному числу зв'язків графа в момент часу t. Нехай на черговому кроці часу до графу додаються p_0 і p_1 нових вершин, приєднуються, відповідно, випадковим і переважним чином. При цьому утворюється $p = p_0 + p_1$ нових зв'язків. Таким чином, загальне число вершин графа $n(t) = pt$, якщо вважати, що його зростання починається при $t = 0$ з пустого місця.

Мета статті

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

Виклад основного матеріалу

У класичному підході до захисту персональних даних важливим є загрози від розширення мережі, які можливо розрахувати наступним виразом:

$$T_i = \left[P_i, P_j \right], \qquad (5)$$

де T_i — множина загроз від розширення мережі; P_i — імовірність того, що зв'язок буде створений з даною вершиною при випадковому приєднанні; P_j — імовірність того, що зв'язок буде створений з даною вершиною при переважному приєднанні.

Втрата такої якості, як приєднання — 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:

$$dI = 0;\ \frac{dI}{dt} = 0\,. \qquad (6)$$

Відповімо на питання: від чого може залежати виток інформації? Перш за все від захищеності системи — вжитих заходів з нейтралізації загроз для безпеки персональних даних. Припустимо що Z — показник захищеності інформаційної системи. Складемо рівняння:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I, \qquad (7)$$

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 виток.

Інтерпретувати дане рівняння можливо наступним чином. Виток інформації залежить:

– від розміру інформаційної системи (отже, якоюсь мірою і від кількості персональних даних);

– від швидкості витоку персональних даних;

– виток інформації блокується захищеністю системи (заходами щодо нейтралізації загроз для 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 (у тому числі і від кількості персональних даних);

– загроз безпеки інформації від приєднаннями між користувачами.

Складемо рівняння:

$$\frac{dZ}{dt} = \frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i} - I(C_{d2} + C_{d1}) \qquad (8)$$

де n_i — загальне число вершин графа в момент часу *t*; x_i — кількість зв'язків які має вершина графа в момент часу *t*.

Об'єднаємо рівняння (7) та (8) в систему (9).

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + \tilde{N}_K) I; \\ \dfrac{dZ}{dt} = \dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i} - I(C_{d2} + C_{d1}). \end{cases} \qquad (9)$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (9). Умови стаціонарності $dI = 0; \frac{dI}{dt} = 0$. Отже отримаємо систему (10):

$$\begin{cases} Z_p \overline{Z} + (C_v + C_K)\overline{I} = 0; \\ \dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i} - I(C_{d2} + C_{d1}) = 0. \end{cases} \qquad (10)$$

З другого рівняння системи випливає:

$$\overline{I} = \frac{\dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}}{(C_{d2} + C_{d1})}. \qquad (11)$$

Далі з першого рівняння системи рівнянь (10) знаходимо $\overline{Z}$.

$$Z_p \overline{Z} - \frac{\dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}(\tilde{N}_v + C_k)}{(C_{d2} + C_{d1})} = 0; \qquad (12)$$

$$\overline{Z} = \frac{\dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}(\tilde{N}_v + C_k)_i}{(C_{d2} + C_{d1}) Z_p}. \qquad (13)$$

Отже, умови позиції стаціонарності системи визначаються системою (14):

$$\begin{cases} \overline{I} = \dfrac{\dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}(\tilde{N}_v + C_k)}{(C_{d2} + C_{d1})}; \\ \overline{Z} = \dfrac{\dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}(\tilde{N}_v + C_k)_i}{(C_{d2} + C_{d1}) Z_p}. \end{cases} \qquad (14)$$

Вирішимо систему рівнянь (9) методом «малих відхилень» $I = \overline{I} + I;\ Z = \overline{Z} + Z$, отже, система рівнянь прийме вигляд (15), (16) (рис. 6, 7).

$$\begin{cases} \dfrac{dI}{dt} = Z_p(\overline{\overline{Z}} + Z) + (C_v + \tilde{N}_K)(\overline{I} + I); \\ \dfrac{dZ}{dt} = \dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}(\tilde{N}_v + C_k)(C_v + C_k) - \\ -(\overline{I} + I)(C_{d2} + C_{d1}). \end{cases} \qquad (15)$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_K)I; \\ \dfrac{dZ}{dt} = -I(C_{d2} + \tilde{N}_k) + \dfrac{1}{n_i} + \dfrac{x_1}{\sum_{i=1}^{n} x_i}(\tilde{N}_v + C_k)_i \times \\ \times (C_v + C_k). \end{cases} \qquad (16)$$

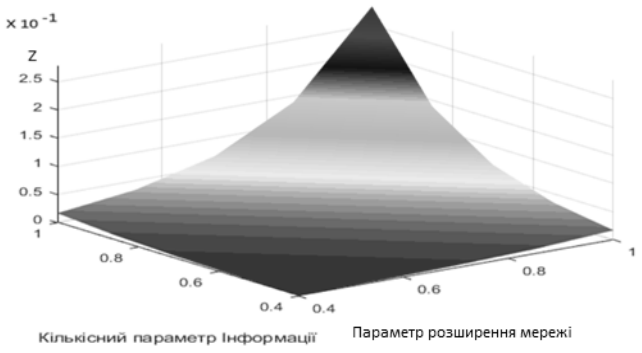


Рис. 6. Залежність захисту персональних даних від складових

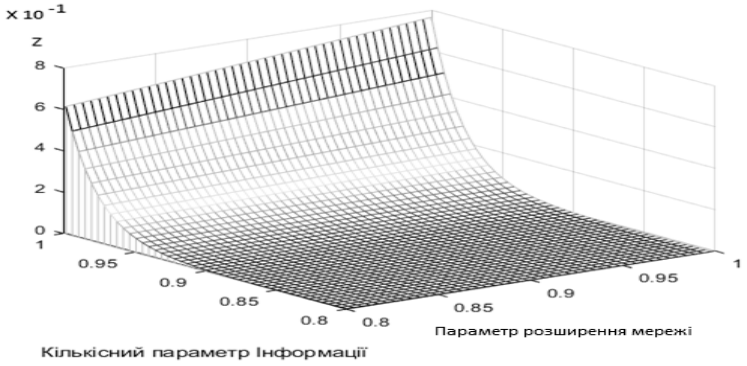


Рис. 7. Залежність захисту персональних даних від складових

Диференціюючи перше рівняння системи (16) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p - n^{-2}{}_i + \frac{2x_1}{(\sum_{i=1}^{n} x_i)} \times \quad (17)$$

$$\times(\tilde{N}_v + C_k)) - (C_v + C_K)\frac{dI}{dt};$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2}) \times$$

$$\times(Z_p - n^{-2}{}_i + \frac{2x_1}{(\sum_{i=1}^{n} x_i)}(\tilde{N}_v + C_k))I = 0. \quad (18)$$

Рівняння (18) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де:

$$\omega_0 = \sqrt{(\tilde{N}_{d1} + C_{d2})\left(Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)}\right)}. \quad (19)$$

$$\omega = \sqrt{(C_{d1} + C_{d2})\left(Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)} - \frac{(C_v + C_K)^2}{4}\right)}. \quad (20)$$

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2})(Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)}(\tilde{N}_v + C_k) - \frac{(C_v + C_K)^2}{4}}}. \quad (21)$$

$$\beta = \frac{(C_v + C_K)}{2} \quad (22)$$

Рішення рівняння гармонічного осцилятора розкладається на три варіанти (рис. 8, 9, 10).

Рис. 8. Залежність захисту персональних за умові (23)

Рис. 9. Залежність захисту персональних за умові (24)

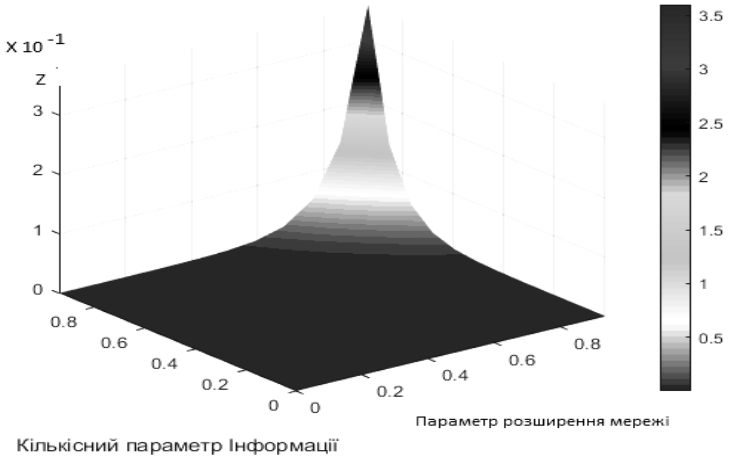


Рис. 10. Залежність захисту персональних за умові (25)

$$\beta < \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2} \cos(\sqrt{(C_{d1} + C_{d2}) + Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)}(\tilde{N}_v + C_k) - \frac{(C_v + C_K)^2}{4}} (t + \varphi_0); \quad (23)$$

$$\beta = \omega_0 : I = (A_0 + B_0 t \exp\left(-\frac{(C_v + C_K}{2} t \right), \quad (24)$$

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

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)}(\tilde{N}_v + C_k)}. \quad (25)$$

Розглянувши три варіанти вирішення рівняння, наближеного до стаціонарного стану системи, можливо 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 (7), (8) до дискретної і промоделювавши деякий інтервал існування системи, отримаємо:

$$\begin{cases} \frac{I_{n+1} - I_n}{\Delta t} = (C_{d1} + C_{d2}) Z_n - (C_v + C_K) I_n); \\ \frac{Z_{n+1} - Z_n}{\Delta t} = Z_p - (C_{d2} + C_{d1}) I_n - (Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)}(\tilde{N}_v + C_k)(C_v + C_k) I_n). \end{cases} \quad (26)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1} + C_{d2}) Z_n - (C_v + C_K) I_n) \Delta t; \\ Z_{n+1} = Z_n + (Z_n - I_n (C_{d2} + C_{d1} + Z_p - n^{-2}{}_i + \frac{2x_1}{\left(\sum_{i=1}^{n} x_i\right)}(\tilde{N}_v + C_k)(C_v + C_k)) \Delta t. \end{cases} \quad (27)$$

Виходячі з умови стаціонарної позиції системи, I і Z будуть дорівнювати 0,5 та 0,5. Зведемо дані моделювання в таблицю. 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 $\beta < \omega_0, \beta = \omega_0, \beta > \omega_0$ з відхиленням від стаціонарної позиції системи.

Таблиця

Параметри моделювання

№ з/п	Z_p	I	Z	C_v	C_{d1}	C_{d2}	C_K	n	$\sum_{i=1}^{n} x_i$	x_1	Параметри
1	0,8	0,5	1	3	1	0,5	3	100000	1000000	20	$\beta < \omega_0$
2	1	0,5	1	3	1	1	3	100000	1000000	20	$\beta = \omega_0$
3	1	0,5	1	4	1	1	5	100000	1000000	20	$\beta > \omega_0$

Представимо ітерації коливань системи захисту: дорезонансній зоні (рис. 11); резонансній зоні (рис. 12); зарезонансній зоні (рис. 13).

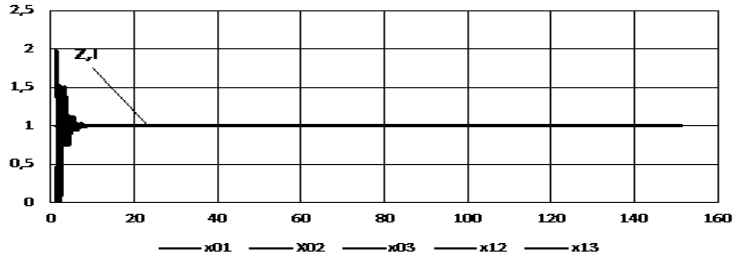


Рис. 11.Коливання системи захисту в дорезонансній зоні

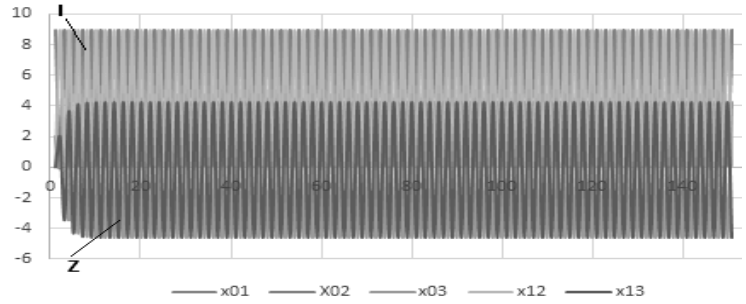


Рис. 12. Коливання системи захисту в резонансній зоні

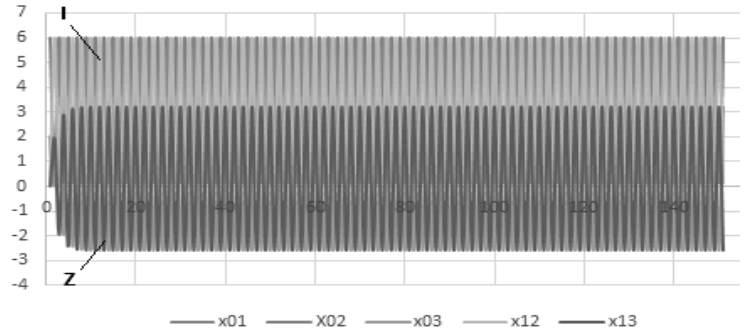


Рис. 13. Коливання системи захисту в за резонансній зоні

Результати, представлені на рис. 13, указують на нелінійність системи захисту [1; 8] в соціальних мережах.

Висновки

Представлена модель росту соціальної мережі з графічною інтерпретацією. Стосовно зростання соціальних мереж це означає, що чим вище валентність, тим швидше вона збільшується. Це цілком логічно, оскільки і при реальному, і при мережевому спілкуванні людина в одиницю часу знайомиться з тим великим числом нових цікавих йому людей, чим більше його контакти. Прискорений розвиток передбачає принципову відкритість системи, тобто постійне приєднання до мережі нових вершин, яка вказує на нелінійний характер розширення СМ.

На відміну до класичного підходу до захисту персональних даних, розроблена система лінійних диференціальних рівнянь, що описують систему захисту СМ з врахуванням специфіки параметрів самої мережі та параметрів розширення, які дозволяють дослідити показник захисту.

Знайдено умови позиції стаціонарності системи, вирішено систему рівнянь методом «малих відхилень», отримані графічні залежності, проведено ітерацію коливань системи захисту. Застосування методу диференціювання функції захисту дозволило дослідити поведінку системи. Дослідження довело залежність захисту даних від величини розширення мережі. Вказана залежність є нелінійною.

Подальше дослідження лінійної моделі захисту в соціальних мережах, показало, що коливання системи захисту СМ описуються диференційним рівнянням другого ступеня та є рівнянням гармонічного осцилятора із затухаючою амплітудою. Також, розглянуті коливання системи захисту СМ в дорезонансній, резонансній та після резонансній зоні.

Отримані власні та вимушені частоти коливань системи, період коливань, коефіцієнт затухання. Результати ітерації коливань указують на нелінійність системи захисту в соціальних мережах. Враховуючи отримані результати необхідне подальше дослідження нелінійної моделі системи захисту.

ЛІТЕРАТУРА

[1] Ахрамович В., Лазаренко С., Мартинюк Г., Баланюк Ю. Модель пошуку співтовариств в соціальній мережі. *Безпека інформації*. К. НАУ. 2020. №1. С. 35–41. DOI: 10.18372/2225-5036.26.14668.

[2] Shchypanskyi P., Savchenko V., Akhramovych V., Muzshanova T., Lehominova S., Chegrenets V. The Model of Secure Social Networks Activity Based on Graph Theory. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*.ISSN: 2278-3075.2020. Vol. 9. Issue4. February 2020. pp. 1803-1810. URL: https://www.ijitee.org/download/volume-9-issue-4 (access date 20.11.2021)

[3] Savchenko V., Akhramovych V., Tushych A., Sribna I., Vlasov I. Analysis of Social Network Parameters and the Likelihood of its Construction. *International Journal of Emerging Trends in Engineering Research*. ISSN 2347 –3983.2020. Vol. 8.No. 2.February2020.pp. 271-276. URL: http://www.warse.org/IJETER/static/pdf/file/ijeter05822020.pdf/(access date 20.11.2021)

[4] Akhramovich V., Hrebennikov A., Tsarenko B., Stefurak O. Methodof-calculating-the-protectionofpersonaldatafromthereputationofusers. *SciencesofEurope*. Praha, Czech-Republic.2021. Vol. 1.No. 80. Pp. 23-31. URL: www.european-science.org (access date 20.11.2021)

[5] Bailey N. The Mathematical Theory of Infectious Diseases and Its Applications. New York: Hafner Press, 1 Applications, Vol. 405, July 2014. pp. 159–170.

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

[7] Rohloff K. Stochastic Behavior of Random Constant Scanning Worms. *The 14th ICCCN*(17-19 Oct. 2005, San Diego, CA, USA). 2005. pp. 339 - 344.

[8] Trubetskov D. Introduction to Synergetics. Chaos and structures. Edition 2 corrected and supplemented. – M. Edytorial. MDFS. 2004. 240p.

[9] Matthew M.,Laeveillae J. Epidemiological model of virus spread and cleanup. Hewlett-Packard Laboratories Bristol (February 27th, 2003). URL: http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf (access date 20.11.2021)

[10] Zan Y., Wu J., Li P., Yu Q. SICR rumor spreading model in complex networks: Counterattack and self-resistance. *Physica A: Statistical Mechanics and its Applications*.2014. Vol. 405. July 2014. pp. 159–170.

[11] Zhang Y., Zhu J. Stability analysis of I2S2R rumor spreading model in complex networks. *Physica A: Statistical Mechanics and its Applications*.2018. Vol. 503, August 2018. pp. 862–881.

[12] Zhao N., Cheng X. Impact of information spread and investment behavior on the diffusion of internet investment products. *Physica A: Statistical Mechanics and its Applications*. 2018. Vol. 512, December 2018. pp. 427–436.

Ахрамович В. М., **Лазаренко С. В.**, **НімченкоТ. В., РябоваЛ. В.**

МЕТОД РОЗРАХУНКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД РОЗШИРЕННЯСОЦІАЛЬНИХ МЕРЕЖ

Обчислення або оцінка величини розширення мережі може дати уявлення про вплив та поширення несанкціонованої інформації зловмисними користувачами. Після того, як шкідливий вузол додається до списку контактів, він може отримати доступ до чутливих даних і розкривати їх, використовуючи засоби соціальної мережі, такі як розміщення об'яв, публікація зображень тощо.

Такий вплив можливо виміряти, обчисливши середнє співвідношеннядрузів, яке може отримати конфіденційну інформацію, розкриту зловмисником.

Виконане дослідження лінійної моделі захисту від розширення мережі дозволило отримати систему лінійних рівнянь захисту інформації в соціальних мережах (СМ) залежно від типу та параметрів розширення мережі. Знайдено умови позиції стаціонарності системи, вирішено систему рівнянь методом «малих відхилень», отримані графічні залежності, проведено ітерацію коливань системи захисту. Застосування методу диференціювання функції захисту дозволило дослідити поведінку системи.

Рівняння захисту інформації є рівнянням гармонічного осцилятора з затухаючою амплітудою, яке розкладається на три випадки: до резонансної зони, резонансної та зарезонансної.

Отримані власні та вимушені частоти коливань системи, період коливань, коефіцієнт затухання.

У дорезонансній зоні коливання системи захисту носять лінійний характер (крім перехідного процесу), показник захисту найбільший, в резонансній зоні коливання системи захисту нелінійні, захист відсутній, в зарезонансній зоні коливання системи захисту нелінійні, захист мінімальний. Отримані результати вказують на нелінійність системи захисту в соціальних мережах.

Ключові слова: розширення мережі; функція; залежність; модель; система; захист; загроза; соціальна мережа; лінійність; не лінійність.

Akhramovych V., Lazarenko S., Nimchenko T., Ryabova L.

METHOD OF CALCULATION OF PROTECTION OF PERSONAL DATA FROM EXPANSION OF SOCIAL NETWORKS

Calculating or estimation of the size of network expansion can give an idea of the impact of the spread of unauthorized information by malicious users. Once a malicious node is added to your contact list, it can access sensitive data and disclose it indiscriminately using social media tools such as placing ad boards, publishing images, etc. Such an impact can be measured by calculating the average ratio of friends, which can get confidential information disclosed by an intruder.

The completed study of the linear model of protection against network expansion allowed to obtain a system of linear equations of information protection in social networks (SN) depending on the type and parameters of network expansion. The conditions of the system stationary position were found, the system of equations by the method of "small deviations" was solved, graphical dependencies were obtained, and the fluctuations of the protection system were iteration. The use of the method of differentiation of the protection function allowed to investigate the behavior of the system.

The equation of information protection is an equation of a harmonic oscillator with a suffocation amplitude and breaks down into three cases: pre-resonant zone, resonant and after resonance.

Obtained own and forced frequencies of oscillations of the system, period of oscillations, attenuation factor.

In the pre-resonance zone, the oscillation zone of the protection system is linear (except for the transition process), the protection indicator is the largest, in the resonance zone of the oscillation of the protection system is nonlinear, there is no protection, there is no protection in the resonant zone, the fluctuations in the protection system are nonlinear, the protection is minimal.

Keywords: networkexpansion; function; addiction; model; system; protection; a threat; socialnetwork; linearity; nonlinearity.

Стаття надійшла до редакції 28.11.2021 р.
Прийнято до друку 13.04.2022 р.