DOI: 10.18372/2410-7840.23.16767
УДК 004.738.5

МЕТОД РОЗРАХУНКУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНІЙ МЕРЕЖІ

Михайло Дівізінюк, Володимир Ахрамович,
Сергій Лазаренко, Владислав Дудник, Іван Яковів

В сучасному світі відмічається значний вплив соціальних мереж (СМ) на всі сфери життя окремих людей та суспільств в цілому. Основна інформацію, що зберігається в СМ - це самостійно генеровані та підтримувані дані користувачів та їхніх відвідувачів. Всі типи даних складають особисту інформацію, яка надається безпосередньо користувачем СМ. Додаткова інформація про користувача в СМ часто генерується та стає доступною всередині СМ іншим користувачам. Особисті дані про контакт описують, хто є користувачем, надаючи не лише основну інформацію, таку як ім'я користувача, фото, стать, день народження, місце народження та сімейний стан, але й додаткову мета-інформацію стосовно членства в СМ, контактну інформацію окрім платформи СМ, таку як поштові адреси, телефонні номери, ідентифікатори миттєвих повідомлень та особисті веб-сайти. Крім того, вони описують особисту програму користувача та можуть повідомляти про сексуальні, особисті, політичні чи релігійні інтереси та вподобання. Тому проблема захисту інформації, а також персональних даних в соціальних мережах набуває великого значення. Для побудови систем захисту соціальних мереж необхідно мати кількісні показники залежності параметрів захисту від специфічних параметрів мережі, в тому числі, від параметрів поширення інформації. В теперішній час не виявлено досліджень, які б надавали можливість оцінити вказані кількісні показники. Рішення даної проблеми можливе при моделюванні процесів в соціальних мережах за допомогою системи диференціальних рівнянь. Запропонований метод дозволяє дослідити чи лінійна система захисту, надає можливість розраховувати кількісно показник захисту мережі від специфічних параметрів, в тому числі, від параметрів розповсюдження інформації.

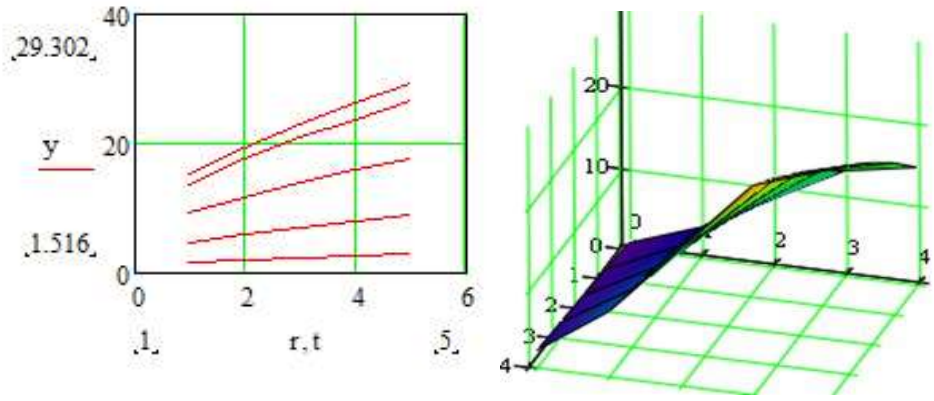
***Ключові слова**: соціальна мережа, система захисту, розповсюдження інформації, система, диференціальні рівняння, нелінійність.*

Постановка проблеми. Інформація яка цікава будь–якого індивідуума в основному залежить від характеристик останнього [4]. Більш того, індивідууми зі схожими характеристиками схильні спілкуватися один з одним. Уявімо епідемічну модель з ймовірністю передачі певної інформації, як функції відстані між джерелом і потенційною метою [2,3,5,8,10]. Далі буде показано, що ця епідемічна модель не має кордонів мережі, має обмежувальний поріг, що має на увазі – поширення інформації обмежено.

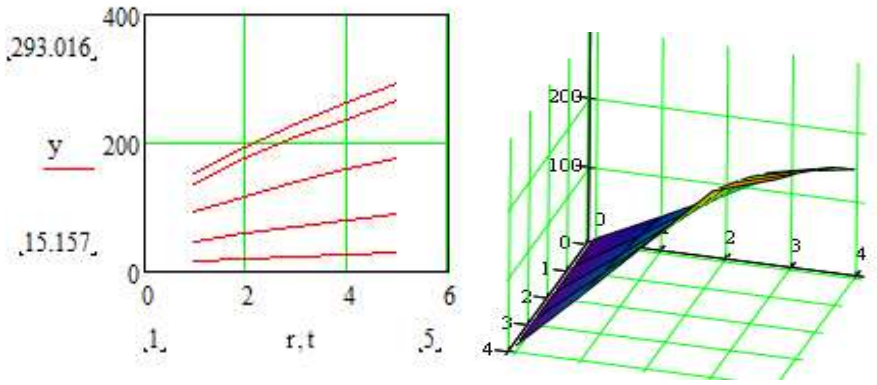
Ймовірність, що *m*–ий сусід передасть цю інформацію особі, з яким він буде контактувати (рис. 1), визначається як [7, 9]:

$$y=t\,(r+1)-f\,, \qquad (1)$$

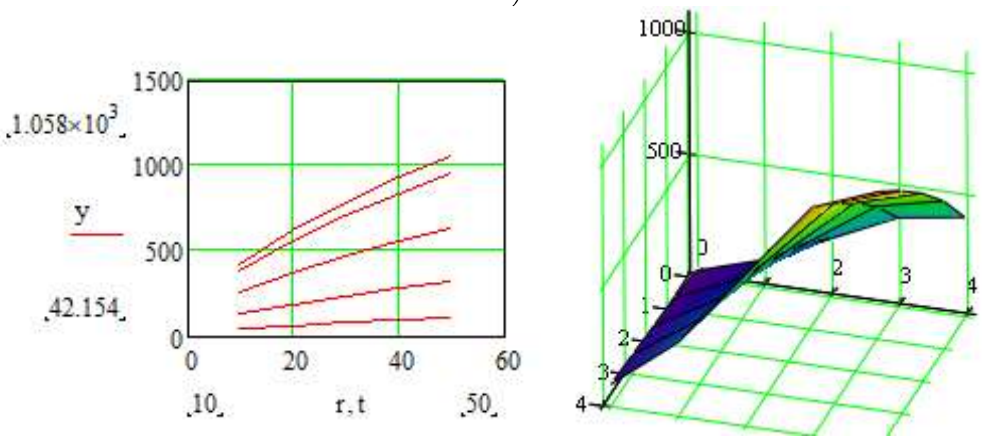
де: f > 0, r –кількість користувачів з якими може поділитися даний користувач інформацією, t – користувач мережі, який знаходиться на визначеному вузлі. При первинному вузлі t (0) = t і при великій віддаленості оточення $t^{(\infty)}$ у зменшується до нуля.



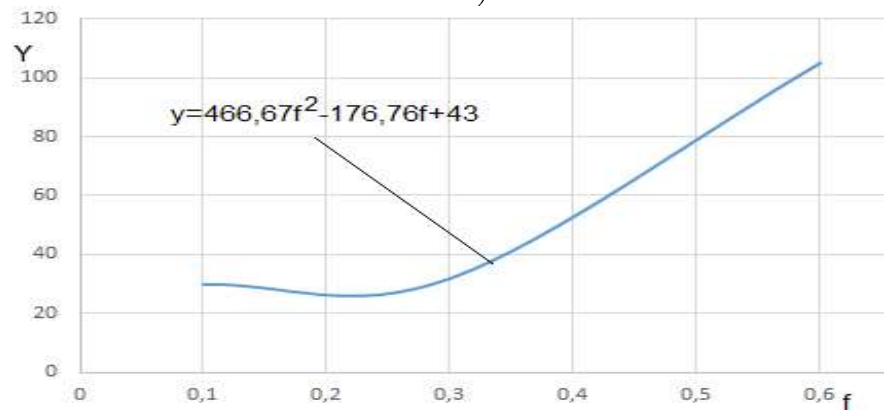
а)



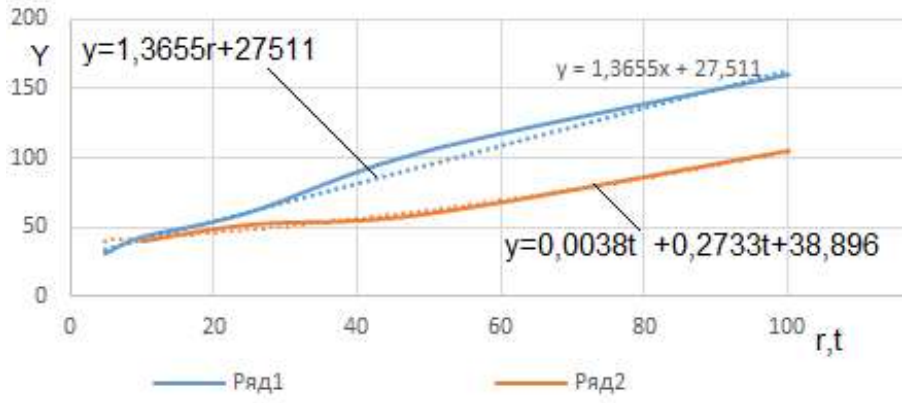
б)



в)



г)



д)

Рис. 1 Залежність передачі інформації іншому користувачеві:
а) f=0,6, r= (1, 2 5), t=(1, 3 10); б) f=0,6, r= (1, 2 5), t=(10, 30 100);
в) f=0,6, r= (10, 20 50), t=(10, 30 100); г) f=0,3, r= (10, 20 50), t=(10, 30 100);
д) залежність передачі інформації іншому користувачеві r= (1, 2 5), t=(10, 30 100); f=0,6.

Лінійне рішення моделі системи захисту. У класичному підході до захисту даних розрізняють:

$$T_i = \left[y_i, y_j \right], \quad (2)$$

де *Ti* – множина загроз від поширення інформації, *yi* - можлива передача інформації між користувачами, *yj* - неможлива передача інформації між користувачами.

Втрата такої якості, як поширення інформації – процес, який має часовий інтервал. Позначимо кількість інформації в системі – I. Потік інформації за межі інформаційної системи через dI–, швидкість зміни цього потоку – dI/dt. Логічно, що якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає:

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

Від чого може залежати витік інформації? Перш за все від захищеності системи – вжитих заходів з нейтралізації загроз безпеки даних [1, 6]. Z – показник захищеності інформаційної системи. Складемо рівняння:

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

де *Zp* – коефіцієнт, що відображає вплив заходів щодо захисту інформації; *Cv* – коефіцієнт, що відображає вплив швидкості витоку даних; *Ck* – коефіцієнт, що відображає вплив кількості даних на їх витік. Інтерпретувати дане рівняння можна наступним чином. Виток інформації залежить:

- від розміру інформаційної системи (отже, в якійсь мірі і від кількості даних);
- від швидкості витоку даних (виток інформації купірується захищенністю системи - заходами щодо нейтралізації загроз безпеки інформації). Далі розглянемо, від чого залежить захищеність системи – Z.

Визначимо захищеність системи як здатність системи протистояти несанкціонованому доступу до конфіденційної даних.

Отже, захищеність системи буде залежати:

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

Складемо рівняння:

$$\frac{dZ}{dt} = t\ (r+1)^{-f} - I(C_{d2} + C_{d1}), \quad (5)$$

де: f>0, r –кількість користувачів з якими може поділитися даний користувач інформацією, t – користувач мережі, який знаходиться на визначеному вузлі. При первинному вузлі t (0) = t і при великій віддаленості оточення $t^{(\infty)}$ *y* зменшується до нуля.

Об'єднаємо рівняння (4) і (5) в систему.

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = t\ (r+1)^{-f} - I(C_{d2} + C_{d1}) \end{cases}. \quad (6)$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (2, 5). Умови стаціонарності $dI = 0;\ dI/dt = 0,$ тоді:

$$\begin{cases} Z_p \bar{Z} + (C_v + C_K) \bar{I} = 0 \\ t\ (r+1)^{-f} - I(C_{d2} + C_{d1}) = 0 \end{cases}. \quad (7)$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{t\ (r+1)^{-f}}{(C_{d2} + C_{d1})}. \quad (8)$$

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

$$Z_p \bar{Z} - \frac{t\ (r+1)^{-f}}{(C_{d2} + C_{d1})} = 0, \quad (9)$$

$$\bar{Z} = \frac{t\ (r+1)^{-f}}{(C_{d2} + C_{d1}) Z_p}. \quad (10)$$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \frac{t\ (r+1)^{-f}}{(C_{d2} + C_{d1})} \\ \bar{Z} = \frac{t\ (r+1)^{-f}}{(C_{d2} + C_{d1}) Z_p} \end{cases}. \quad (11)$$

Вирішимо систему рівнянь (6) методом «малих відхилень» I = Ī + I; Z = $\bar{Z}$ + Z:, отже, система рівнянь прийме вигляд (рис. 2, 3).

$$\begin{cases} \frac{dI}{dt} = Z_p (\bar{Z} + Z) + (C_v + C_{ki})(\bar{I} + I) \\ \frac{dZ}{dt} = t\ (r+1)^{-f} - (\bar{I} + I)(C_{d2} + C_{d1}) \end{cases}, \quad (12)$$

$$\begin{cases} \frac{dI}{dt} = (C_{d1} + C_{d2}) Z - (C_v + C_K) I \\ \frac{dZ}{dt} = -I(C_{d2} + C_k) + t\ (r+1)^{-f} \end{cases}. \quad (13)$$

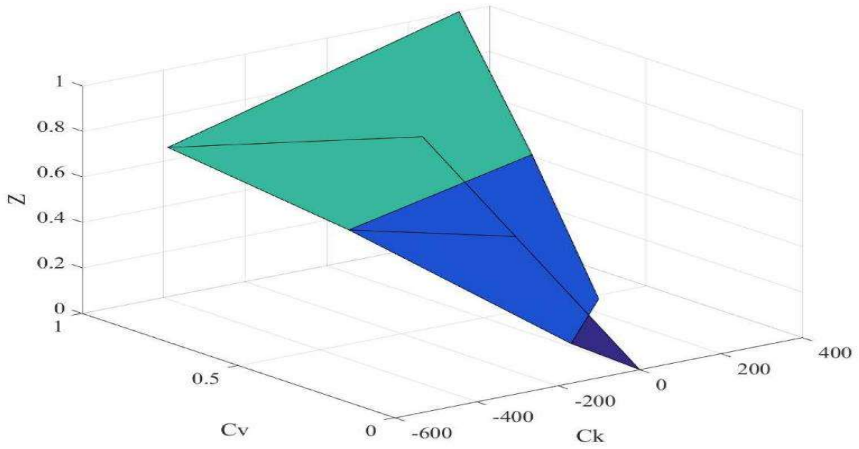


Рис. 2 Залежність захисту даних від складових (за 7, 11)

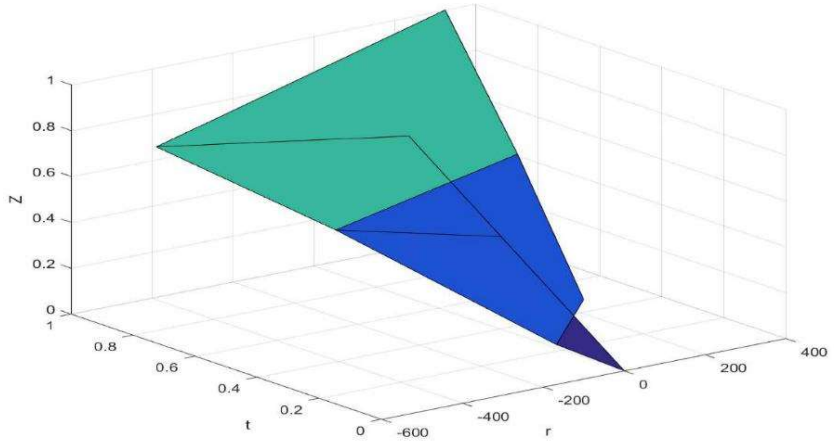


Рис. 3 Залежність захисту даних від складових (за 13)

Диференціюючи перше рівняння системи (13) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + \frac{ft\ (r+1)^{-f}}{r-1} - (C_v + C_k))\frac{dI}{dt}. \quad (14)$$

$$\frac{d^2I}{dt^2} + (C_v + C_k)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + (\frac{ft\ (r+1)^{-f}}{r-1}))I = 0. \quad (15)$$

Рівняння (15) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де (рис. 4, 5):

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})(Z_p + \frac{ft\ (r+1)^{-f}}{r-1})}, \quad (16)$$

$$\omega = \sqrt{(C_{d1} + C_{d2})(Z_p + ft\ \frac{ft\ (r+1)^{-f}}{r-1} - \frac{(C_v + C_k)^2}{4})}. \quad (17)$$

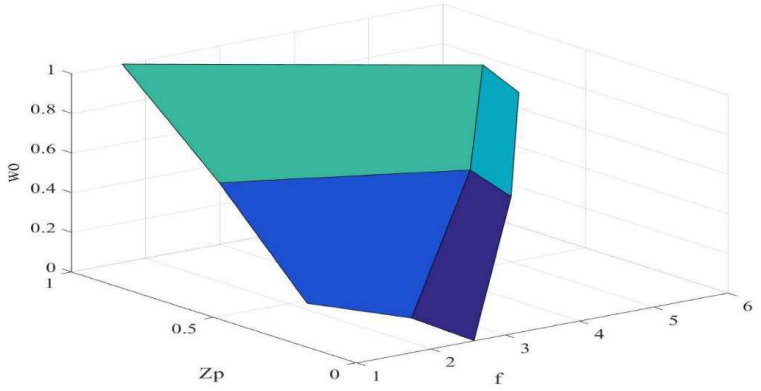


Рис. 4 Особиста частота системи захисту (за 16)

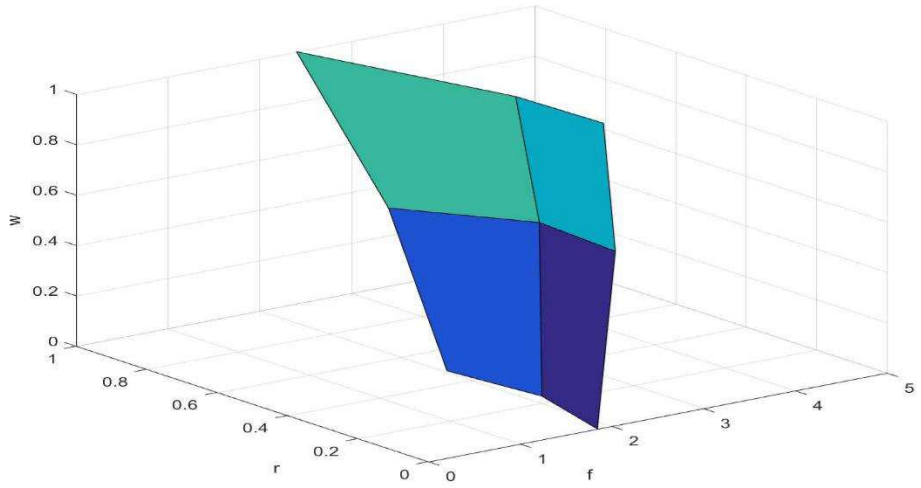


Рис. 5 Частота системи захисту за (17)

Визначимо період коливань та коефіцієнт затухання системи захисту (рис. 6, 7):

$$T = \frac{2\pi}{\sqrt{(C_{d1}+C_{d2})(Z_p + ft\ \frac{ft\ (r+1)^{-f}}{r-1} - \frac{(C_v+C_K)^2}{4}}}, \quad (18)$$

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

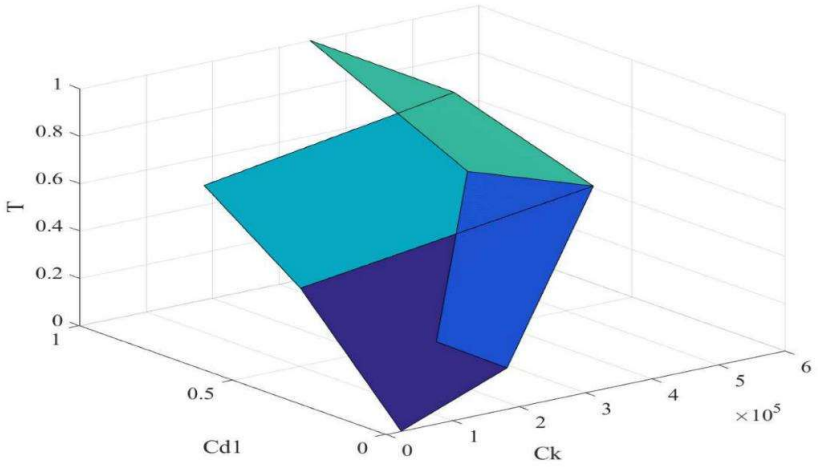


Рис. 6 Період коливань системи захисту (за 18)

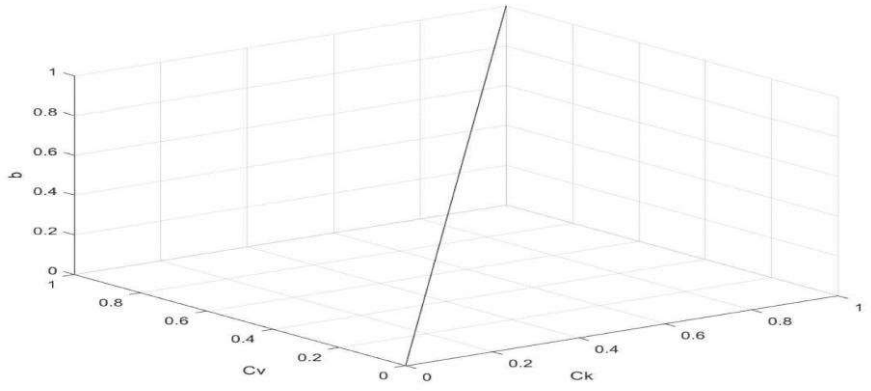


Рис. 7 Коефіцієнт затухання системи захисту (за 19)

Рішення рівняння гармонічного осцилятора розпадається на три випадки.

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

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

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

де

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_k)^2}{4} - (C_{d1} + C_{d2} + Z_p + \frac{ft\ (r+1)^{-f}}{r-1}}). \quad (22)$$

Розглянувши три варіанти вирішення рівняння близько стаціонарного стану системи та виходячи з умов співвідношення диссипації і власної частоти коливань величини можливо прийти до висновку, що 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 (1) до дискретної і промоделювавши деякий інтервал існування системи.

Слідуючи з умови стаціонарної позиції системи, I і Z будуть рівні 0,5 і 1.

Крок моделювання приймемо за 0,1 для всіх ітерацій моделювання, тому в таблиці відображати його не будемо.

Величини *Isp, Zsp* відображають стаціонарні значення параметрів, якщо такі були досягнуті за кінцеве число ітерацій. Далі проведемо моделювання для значень $\beta < \omega_0$, $\beta = \omega_0$, $\beta > \omega_0$ з відхиленням від стаціонарної позиції системи.

Дані представлені в табл. 1. Графічні результати ітераційного обчислення представлені на рис. 8-10. Візуалізація результатів.

Таблиця 1

Параметри моделювання

№ з/п	Z_p	I	Z		C_v	C_{d1}	f	C_{d2}	C_K	r	t	Параметри
1	1	0,5	1		1	1	0,1	0,5	1	1-20	1	$\beta \prec \omega_0$
2	1	0,5	1		2	1	0,1	1	2	1-50	1	$\beta = \omega_0$
3	1	0,5	1		4	1	1	1	5	1-20	1	$\beta \succ \omega_0$

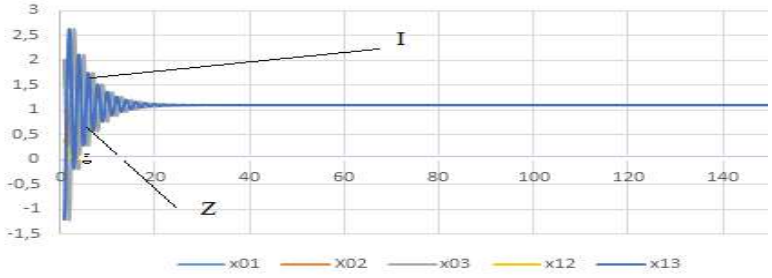


Рис. 8 Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140)

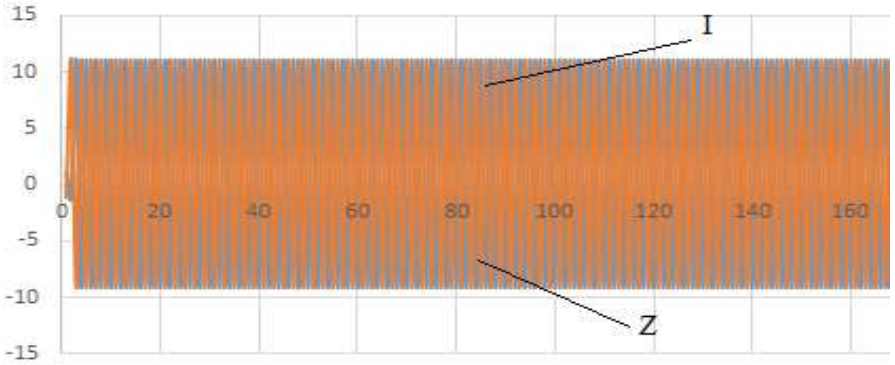


Рис. 9 Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140), $\beta = \omega_0$, *Di* = 0,5

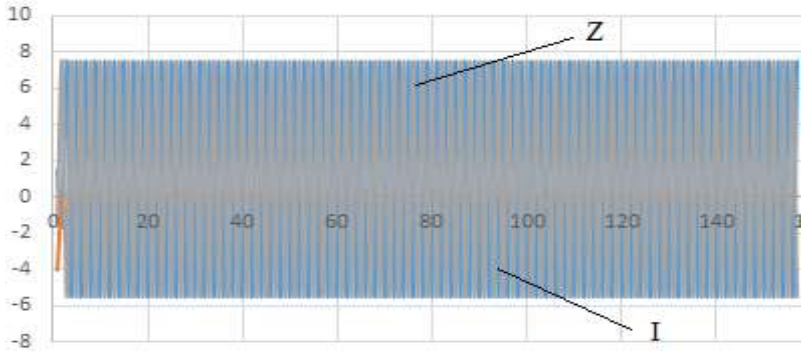


Рис. 10 Залежність інтенсивності та захисту персональних даних від кількості ітерацій (140), $\beta > \omega_0$, $Di = 0{,}1$

Дані складових взяті з табл. 1, $\beta < \omega_0$, через I позначено кількість ітерацій.

ВИСНОВКИ

У ході роботи, розроблена математична модель та проведено дослідження інтенсивності передачі даних та моделі захисту персональних даних від поширення інформації в соціальній мережі. У результаті математичного моделювання доведено, що система захисту соціальної мережі нелінійна [1, 2] на що вказують результати імітаційного моделювання (рис. 10). Враховуючи зазначене, потребує подальше дослідження нелінійної системи захисту персональних даних соціальної мережі для створення якісної системи захисту.

ЛІТЕРАТУРА

[1] Akhramovich V., Hrebennikov A., Tsarenko B., Stefurak O. Method of calculating the protection of personal data from the reputation of users *Sciences of Europe*, Praha, Czech Republic.2021/ VOL 1, No 80 (2021) pp. 23-31.

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

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

[4] Gubanov D., Chkhartishvili A. A conceptual approach to the analysis of online social networks. Upravlenie bol'shimi sistemami – *Large-Scale Systems Control*, No. 45, 2013. pp. 222–236 (In Russian).

[5] Jeffrey Kephart, Steve White, «Directed-Graph Epidemiological Model of Computer Viruses». *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1991. - pp. 343.

[6] Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., , Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS)* 2021. № 1, April 2021. pp. 15-21.

[7] Pavlo Shchypanskyi, Vitalii Savchenko, Volodymyr Akhramovych, Tetiana Muzshanova, Svitlana Lehominova, Volodymyr Chegrenets.The Model of Secure Social Networks Activity Based on Graph Theory/ *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075,Volume-9 Issue-4, February 2020 pp 1803-1810.

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

[9] Vitalii Savchenko, Volodymyr Akhramovych, Alina Tushych, Irina Sribna, Ihor Vlasov. Analysis of Social Network Parameters and the Likelihood of its Construction/*International Journal of Emerging Trends in Engineering Research* ISSN 2347 -3983, Volume 8.No. 2, February 2020. - pp. 271-276.

[10] Williamson, Matthew M.; Laeveillae, Jasmin, 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.

МЕТОД РАСЧЕТА ЗАЩИТЫ ИНФОРМАЦИИ ОТ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНОЙ СЕТИ

В современном мире отмечается значительное влияние социальных сетей (СМ) на все сферы жизни отдельных людей и обществ в целом. Основная информация, хранящаяся в СМ - это самостоятельно генерируемые и поддерживаемые данные пользователей и их посетителей. Все типы данных составляют личную информацию, предоставляемую непосредственно пользователем СМ. Дополнительная информация о пользователе в СМ часто генерируется и становится доступной внутри СМ другим пользователям. Личные данные о контакте описывают, кто является пользователем, предоставляя не только основную информацию, такую как имя пользователя, фото, пол, день рождения, место рождения и семейное положение, но и дополнительную цель о членстве в

СМ, контактную информацию кроме платформы СМ, такой как почтовые адреса, телефонные номера, идентификаторы мгновенных сообщений и личные веб-сайты. Кроме того, они описывают личную программу пользователя и могут сообщать о сексуальных, личных, политических или религиозных интересах и предпочтениях. Поэтому проблема защиты информации, а также персональных данных в социальных сетях приобретает большое значение. Для построения систем защиты социальных сетей необходимо иметь количественные показатели зависимости параметров защиты от специфических параметров сети, в том числе от параметров распространения информации. В настоящее время не выявлено исследований, которые предоставляли бы возможность оценить указанные количественные показатели. Решение данной проблемы возможно при моделировании процессов в социальных сетях посредством системы дифференциальных уравнений. Предлагаемый метод позволяет исследовать линейную систему защиты, предоставляет возможность рассчитывать количественно показатель защиты сети от специфических параметров, в том числе, от параметров распространения информации.
Ключевые слова: социальная сеть, система защиты, распространение информации, система, дифференциальные уравнения, нелинейность**.**

METHOD OF CALCULATION OF PROTECTION OF INFORMATION AGAINST DISSEMINATION OF INFORMATION IN THE SOCIAL NETWORK

In the modern world, there is a significant impact of social networks (CM) on all spheres of life of individuals and societies as a whole. The main information stored in the CM is independently generated and maintained data of users and their visitors. All types of data constitute personal information, which is provided directly by the CM user. Additional information about the user in the CM is often generated and becomes available within the CM to other users. Contact personal data describes who the user is, providing not only basic information such as user name, photo, gender, birthday, place of birth, and marital status, but also additional meta information about membership in the CM, contact information other than the CM platform, such as email addresses, phone numbers, instant messaging IDs, and personal websites. In addition, they describe the user's personal agenda and may report sexual, personal, political or religious interests and preferences. Therefore, the problem of protecting information and personal data in social networks is of great importance. To build social network protection systems, it is necessary to have quantitative indicators of the dependence of protection parameters on specific network parameters, including information dissemination parameters. Currently, no studies have been found that would provide an opportunity to evaluate the indicated quantitative indicators. The solution to this problem is possible when modeling processes in social networks using a system of differential equations. The proposed method makes it possible to investigate whether a linear protection system provides an opportunity to quantitatively calculate the indicator of network protection against specific parameters, including information dissemination parameters.
Key words: social network, protection system, information dissemination, system, differential equations, nonlinearity.

Дівізінюк Михайло Михайлович, доктор фізико-математичних наук, професор, головний науковий співробітник ДУ «Інститут геохімії навколишнього середовища НАН України».
E-mail: divizinyuk@ukr.net.
Orcid ID: 0000-0003-1352-042X.

Дивизинюк Михаил Михайлович, доктор физико-математических наук, профессор, главный научный сотрудник ГУ «Институт геохимии окружающей среды НАН Украины».
Divizinyuk Michael, doctor of physical and mathematical sciences, professor, chief researcher GA «Institute of environmental geochemistry NAS of Ukraine».

Ахрамович Володимир Миколайович, д.т.н., с.н.с., професор кафедри Систем інформаційного та кібернетичного захисту Державного університету телекомунікацій.
E-mail: 12z@ukr.net.
Orcid ID: 0000-0003-1352-042X.

Ахрамович Владимир Николаевич, д.т.н., с.н.с., профессор кафедры Систем информационной и кибернетической защиты Государственного университета телекомуникаций.
Akhramovich Volodymyr, Doctor of Technical Sciences, Senior Research Fellow, Professor of the Department of Information and Cyber Defense Systems of the State University of Telecommunications.

Лазаренко Сергій Володимирович, доктор технічних наук, доцент, професор кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: zzi.lazarenko@nau.edu.ua.
Orcid ID: 0000-0003-3529-4806.
Лазаренко Сергей Владимирович, доктор технических наук, доцент, профессор кафедры средств защиты информации Национального авиационного университета.
Lazarenko Serhii, Doctor of Technical Science, Associate professor, professor Department of information security National Aviation University.

Дудник Владислав Басірович, асистент кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: vb.dudnik@gmail.com.
Orcid ID: 0000-0003-1352-042X.

Дудник Владислав Басирович, ассистент кафедры средств защиты информации Национального авиационного университета.
Dudnyk Vladyslav, assistant of the Department of information security, National Aviation University.

Яковів Іван Іванович, асистент кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: theivasyl@gmail.com.
Orcid ID: 0000-0003-1352-042X.
Яковив Иван Иванович, ассистент кафедры средств защиты информации Национального авиационного университета.
Yakoviv Ivan, assistant of the Department of information security, National Aviation University.