ISSN 2076-1546

УДК 004:047:004.912 DOI: 10.46972/2076-1546.2021.20.07

В. С. Савчук

ЗАСТОСУВАННЯ ВЛАСТИВОСТЕЙ ПЕРКОЛЯЦІЇ ДЛЯ ПРОТИДІЇ ПОШИРЕННЮ ДЕСТРУКТИВНОГО ПСИХОЛОГІЧНОГО ВПЛИВУ В СОЦІАЛЬНИХ МЕРЕЖАХ

Сучасне планування психологічних операцій не можливе без використання таких інформаційних технологій, як засоби моделювання, що забезпечують точність спланованих операцій та передбачення їх результатів. У статті запропоновано концепцію протидії поширенню деструктивних інформаційних впливів через персональні акаунти спільнот соціальних мереж, яка, на відміну від відомих, базується на попередньому імітаційному моделюванні конкретної спільноти з метою визначення ключових та найбільш уразливих акторів у ній, що вимагають знешкодження (блокування), а їх видалення призведе до різкого розпаду (перколяції) співтовариства. У роботі наведено результати імітаційних експериментів щодо цілеспрямованого блокування акаунтів соціальних спільнот соціальної мережі «ВКонтакте», що є джерелом поширення деструктивного впливу. Встановлено, що ефект перколяції має місце як для графа всієї мережі, так і для окремих об'єднань (груп) усередині аналізованої спільноти, знайдених із використанням різних відомих методів кластеризації. Як показують результати моделювання, визначення порога перколяції дозволяє встановити частку найбільш вразливих вершин (акторів), що вимагають блокування для протидії поширенню деструктивних впливів у соціальних мережах. Показано, що оцінка порога перколяції коливається в межах 30–50% цілеспрямовано віддалених вершин. При цьому передбачається, що противник володіє аналогічною стратегією і може використовувати її для поширення деструктивного впливу. З іншого боку, якщо виходити з позиції нападника в рамках завдання інформаційного протиборства, то імітаційне моделювання за поточними даними дає можливість розробити оптимальну стратегію протидії певній спільноті, що становить небезпеку. Запропонований підхід сприяє розробці інформаційної технології як для захисту персональних акаунтів соціальних мереж від деструктивних впливів, так і для ефективної протидії в завданнях інформаційного впливу, управління та протиборства.

Ключові слова: *соціальні мережі; безмасштабні графи; деструктивний психологічний вплив; перколяція графа.*

Постановка проблеми в загальному вигляді. У століття розвинених технологій і засобів комунікації традиційні форми інформаційного обміну для основної маси населення відходять на другий план. Навіть телебачення для молодого покоління перестає бути головним джерелом отримання інформації через низьку якість телепродукції та відсутність інтерактивності. З розвитком Інтернету і мобільних пристроїв користувачеві надаються найширші можливості як для вибору джерел і форм отримання інформації на задану тему, так і для обміну інформацією, зокрема фото, аудіо та відео. Практика

показує, що основним засобом комунікації серед населення країн світу, що має доступ до Інтернету, є соціальні мережі. У зв'язку із цим соціальні мережі розглядаються як один з ефективних засобів поширення деструктивного інформаційно-психологічного впливу як у політиці всередині держав, так і в процесі ведення інформаційних війн між ними.

Аналіз останніх досліджень і публікацій. У даний час відома низка міждисциплінарних наукових досліджень, присвячених питанням інформаційного впливу, управління і протиборства в соціальних мережах [1]. Проте розгляд соціальної мережі як комплексної системи, описаної у вигляді графа, дає можливість використовувати істотні наукові напрацювання з іншої міждисциплінарної галузі, присвяченої вивченню таких систем (Complex Systems), у контексті захисту від поширення деструктивних впливів через персональні акаунти. Вагомий внесок у розвиток методів моделювання процесів протидії інформаційним впливам та інформаційній боротьбі в цілому зробили публікації [1–4]. У них обґрунтовано важливість, способи та підходи моделювання інформаційного протиборства. Робота [5] присвячена протидії деструктивним впливам на основі семантичного аналізу текстового контенту для виявлення інформаційних впливів. Питання аналізу поширення інформації в соціальних мережах розглянуто в [6–11], де описано підходи до моделювання безмасштабних мереж та процесів вірусного поширення інформації в них. Але сьогодні найбільш ефективним засобом ведення інформаційного протиборства є соціальні мережі із залученням персональних акаунтів, тому висвітлення потребують підходи до моделювання саме протидії поширенню деструктивних впливів у соціальних мережах, що в подальшому можуть слугувати основою для створення програмного забезпечення.

Формулювання завдання дослідження. У статті запропоновано концепцію оптимальної протидії поширенню деструктивних впливів у соціальних інтернет-співтовариствах або пов'язаних із ними спільнотах, в основі якої лежить попереднє моделювання цілеспрямованого блокування акаунтів, що є вагомими для вірусного поширення деструктивного впливу на основі реального графа спільноти станом на поточний момент, для визначення порога перколяції та ключових акаунтів, блокування яких є достатнім для протидії. Отримані результати дають інформацію для розробки стратегії оптимальної протидії.

Мета дослідження – підвищення ефективності протидії поширенню деструктивних впливів у соціальних мережах через акаунти соціальних спільнот за рахунок синтезу оптимальної стратегії їх блокування на основі моделі перколяції графа спільноти як середовища поширення інформації.

Виклад основного матеріалу. Відомо [2–4], що так звані «безмасштабні мережі» (Scale Free Networks), які включають World Wide Web, Інтернет, а також соціальні мережі, відображають високий ступінь надійності до випадково спрямованих атак, що в даному контексті може розглядатися як високий ступінь стійкості до блокування джерел поширення деструктивного впливу. Однак ці ж мережі є надзвичайно уразливими до цілеспрямованого блокування, тобто до вибору й видалення акторів із високим ступенем (рейтингом), які відіграють життєво важливу роль у підтримці зв'язків у мережі. Вразливість характеризується явищем розпаду мережі на частини. У вказаних вище

роботах для асортативних мереж (із позитивним кореляційним зв'язком) це явище називається перколяцією. Це фазовий перехід зі стану, коли мережа характеризується зв'язковим графом, у стан, коли має місце утворення маси окремих фрагментів. У розрізі питань захисту від поширення деструктивних впливів серед акаунтів соціальної мережі виключення певних вузлів, що поширюють деструктивні впливи, має в кінцевому підсумку призвести до ефекту перколяції на інформаційному рівні. У такому контексті слід говорити про моделі поширення інфекцій, які за своєю природою схожі з моделями перколяції [7–11]. При цьому необхідно зазначити, що ефект перколяції має аномалії в разі зростаючих мереж [12]. У зв'язку з викладеним вище питання розробки інформаційних технологій, що дозволяють реалізувати такі моделі в завданнях інформаційного впливу, управління і протиборства на рівні конкретного користувача, є досить актуальними.

У [13] запропоновано описати цільову аудиторію (ЦА) у вигляді неорієнтованого графа. Формально вона подана у вигляді графа G (N, E), у якому $N = \{1, 2, ..., n\}$ – множина вершин (акторів чи акаунтів соціальної мережі); $E = \{1, 2, ..., k\}$ – множина ребер, що відображають зв’язки акторів між собою, під якими розуміємо соціальні зв’язки («дружать», «репостять», мають родинні зв’язки або спільні інтереси тощо). Для дослідження використовувалися дані персональних аканутів користувачів соціальної мережі «ВКонтакте» із м. Волновахи, старші 18 років. Тестовий набір даних містив 8421 актора та 13706 зв’язків між ними. Механізм збору був реалізований за допомогою розробки програмного забезпечення, що взаємодіяло із сервером «ВКонтакте» через надані методи API. Було використано також відкритий онлайн-сервіс https://vk.barkov.net. Для модельного прикладу не враховувалися всі наявні зв’язки акторів. Через відсутність навчальної вибірки використовувалися реальні дані.

Зібрані дані були опрацьовані, на їх основі побудовано базу даних у форматі .csv, що підтримується програмою Gephi, використаною для моделювання. На рис. 1 зображений відповідний ненаправлений граф, кожна вершина якого асоційована з певним персональним акаунтом, а його ребрами описані зв’язки.

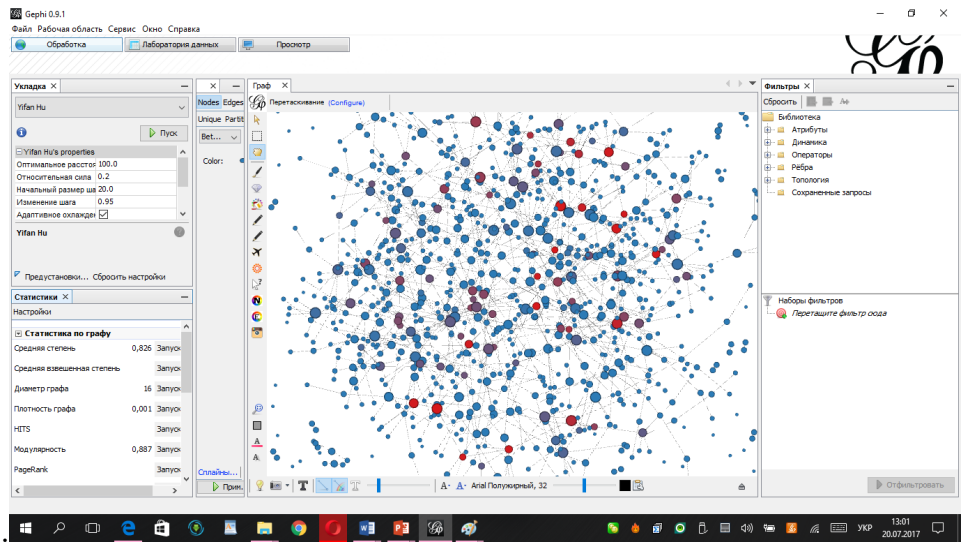

Рис. 1. 3D-візуалізація графа зв’язків персональних акаунтів м. Волновахи

У табл. 1 наведено основні числові характеристики графа. Як видно, мережа має позитивну асортативність ($r \approx 0{,}044 > 0$) із високим коефіцієнтом її кластеризації ($\langle C \rangle \approx 0{,}238$), що підтверджує результати, отримані раніше іншими авторами, щодо безмасштабних графів.

Таблиця 1

Числові характеристики графа

Кількість вершин N	Коефіцієнт асортативності r	Коефіцієнт кластеризації $\langle C \rangle$
5171	+0,0441148073621	+0,238117436772

Ґрунтуючись на експерименті, описаному в роботі [2], був змодельований процес перколяції побудованого графа з відстеженням найбільшого кластера з розміром S (рис. 2а) і середнього кластера з розміром $\langle s \rangle$ (рис. 2б) залежно від частки віддалених вершин. Результати підтверджують властивості перколяції безмасштабного графа, аналогічні тим, що були отримані авторами [2]. Як видно з графіків (рис. 2), для цілеспрямованого блокування акаунтів соціальної мережі чи акторів має місце чітко виражений поріг перколяції (ефект руйнування мережі) при частці віддалених вершин, що дорівнює 0,5. Це означає, що процес поширення інформації стає неможливим за рахунок відсутності зв'язності спільноти.

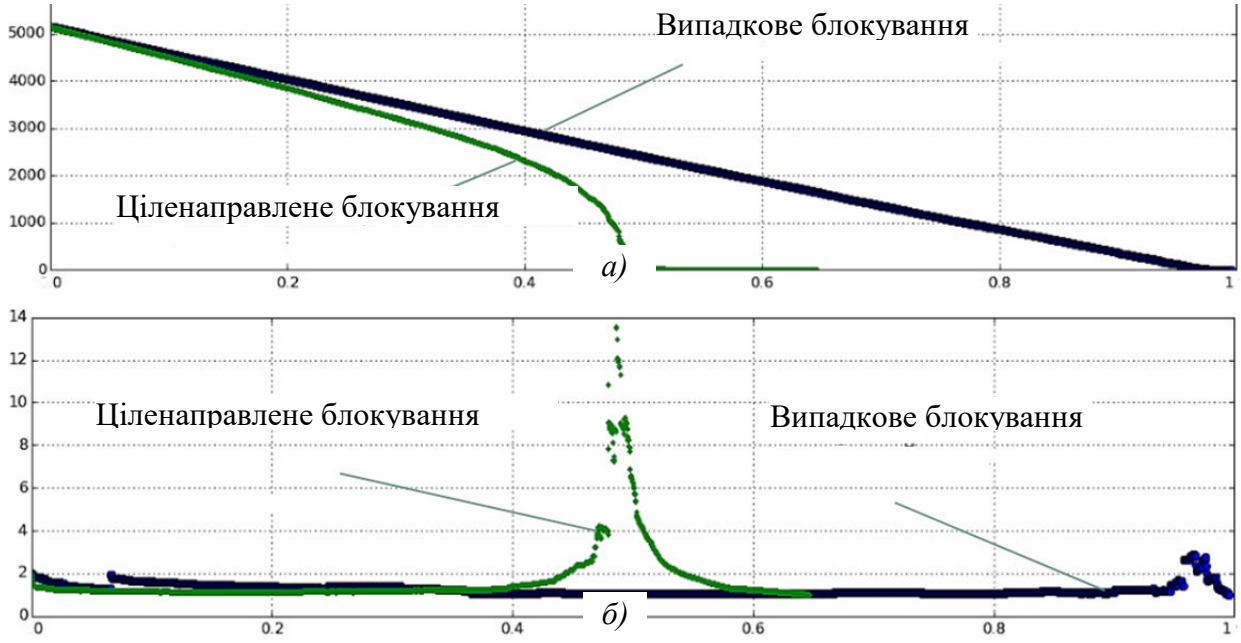

Рис. 2. Фрагментація графа: вісь y – розмір S найбільшого (а) та $\langle s \rangle$ середнього (б) кластерів; вісь x – частка блокованих вершин

На наступному етапі було здійснено пошук і 3D-візуалізацію (рис. 3) спільнот із використанням алгоритму Louvain [12].

Після виділення однієї зі спільнот усередині спільноти акаунтів м. Волновахи (рис. 3) були знайдені її числові характеристики (табл. 2) і застосована модель процесу перколяції з візуалізацією результатів (рис. 4а, б).

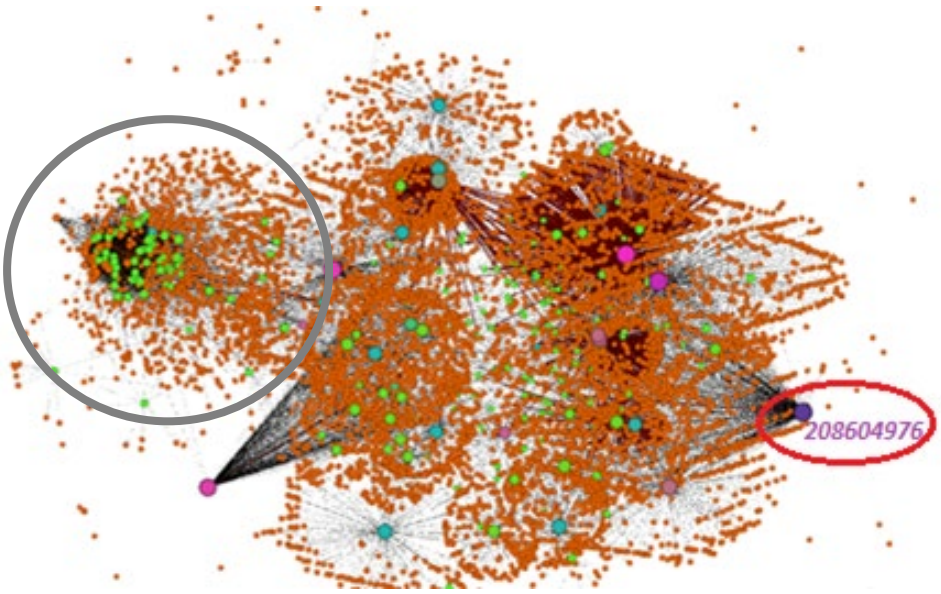

Рис. 3. 3D-візуалізація графа спільнот із виділенням найбільшої з них за кількістю вершин

Таблиця 2

Числові характеристики графа виділеної спільноти (рис. 3)

Кількість нод N	Діаметр d	Коефіцієнт асортативності r	Коефіцієнт кластеризації $\langle C \rangle$
940	7	+0,0609364988023	+0,281535528823

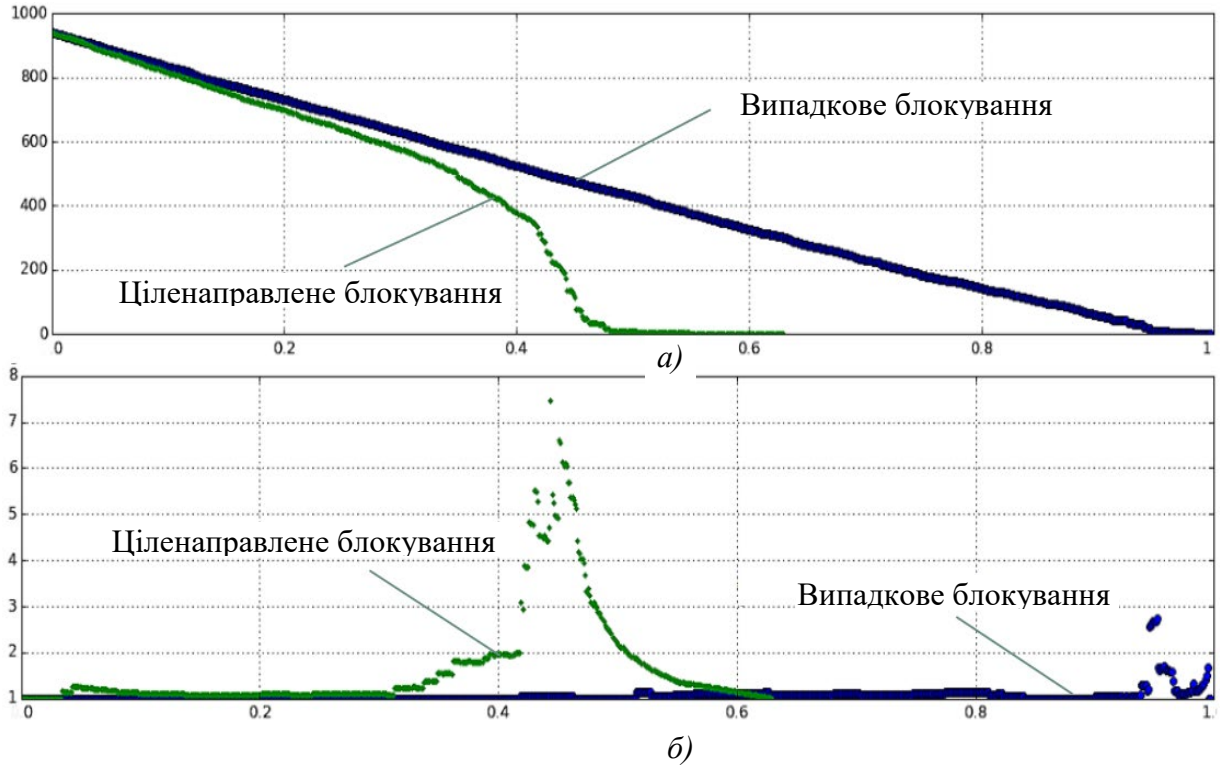

Рис. 4. Фрагментація графа: вісь y – розмір s найбільшого (а) і $\langle s \rangle$ середнього (б) кластерів; вісь x – частка блокованих вершин

Як видно, у разі блокування близько 45% вершин, граф спільноти починає різко руйнуватися. Це означає, що структура цієї спільноти досить стійка, оскільки для її руйнування необхідне блокування майже половини діючих акаунтів. Для оцінювання порога перколяції різних методів сегментації та для різних спільнот була проведена серія послідовних експериментів, суть яких полягала в такому: для графа, наведеного на рис. 1, послідовно були застосовані три відомі алгоритми кластеризації: кращого розбиття (best_partitions), багаторівневих спільнот (community_multilevel) і на основі власних векторів (community_leading_eigenvector). Для кожної виділеної спільноти послідовно проводився імітаційний експеримент із направленого блокування вершин акаунтів соціальних мереж) з подальшим визначенням оцінки порога перколяції. Як видно з результатів (табл. 3), поріг перколяції знаходився в межах 30–50%.

Таблиця 3

Оцінки порога перколяції для різних спільнот, отриманих різними методами кластеризації

№ спільноти	Best_partitions		Community_multilevel		Community_leading_eigenvector	
	Кількість акторів	Поріг перколяції	Кількість акторів	Поріг перколяції	Кількість акторів	Поріг перколяції
1	946	0,41	967	0,43	1312	0,35
2	940	0,45	939	0,42	1209	0,42
3	520	0,40	521	0,41	1010	0,35
4	485	0,39	463	0,39	896	0,38
5	357	0,39	357	0,38	604	0,38
6	328	0,37	324	0,35	7	0,29
7	294	0,29	300	0,35		
8	274	0,26	245	0,39		
9	222	0,38	222	0,30		
10	201	0,39	219	0,37		
11	189	0,36	192	0,35		
12	168	0,34	171	0,31		

Висновки. Як показують результати моделювання, визначення порога перколяції дозволяє встановити частку найбільш вразливих вершин (акторів), що вимагають блокування для протидії поширенню деструктивних впливів у соціальних мережах. З'ясовано, що ефект перколяції має місце як для графа всієї мережі, так і для окремих спільнот, знайдених із використанням різних відомих методів кластеризації. Показано, що оцінка порога перколяції коливається в межах 30–50% цілеспрямовано віддалених вершин. При цьому передбачається, що противник володіє аналогічною стратегією і може використовувати її для поширення деструктивного впливу. З іншого боку, якщо виходити з позиції нападника в рамках завдання інформаційного протиборства, то імітаційне моделювання за поточними даними дає можливість розробити оптимальну стратегію протидії певній спільноті, що становить небезпеку. Запропонований підхід сприяє розробці інформаційної технології як для захисту персональних акаунтів соціальних мереж від деструктивних впливів, так і для ефективної протидії в завданнях інформаційного впливу, управління та протиборства.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. Москва : Физматлит, 2010. 228 с.
2. Грищук Р. В. Основи кібернетичної безпеки : монографія / За заг. ред. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.
3. Callaway D. S., Newman E. J., Strogatz S. H., Duncan J. Watts Network Robustness and Fragility: Percolation on Random Graphs // Physical Review Letters. 2000. Vol. 85, № 25. P. 5468–5471.
4. Newman E., Girvan M. Finding and Evaluating Community Structure in Networks // Physical Review E. 2004. Vol. 69, Iss. 2. P. 1–15.
5. Молодецька – Гринчук К. В. Семантичний аналіз текстового контенту для виявлення інформаційних впливів на акторів у соціальних інтернет-сервісах // Проблеми і перспективи розвитку IT індустрії : матеріали міжнар. наук.-практ. конф. (м. Харків, листопад, 2017). Харків, 2017. С. 58.
6. Dorogovtsev S. N., Mendes J. F. Evolution of Networks. From Biological Nets to the Internet and WWW. Oxford : Oxford University Press, 2003. 264 p.
7. Pastor-Satorras R., Vespignani A. Epidemic Spreading in Scale-Free Networks // Physical Review Letters. 2001. Vol. 86, № 14. P. 3200–3203.
8. Pastor-Satorras R., Vespignani A. Epidemic Dynamics and Endemic States in Complex Networks // Physical Review E. 2001. Vol. 63, Iss. 6. P. 1–8.
9. Pastor-Satorras R., Vespignani A. Immunization of Complex Networks // Physical Review E. 2002. Vol. 65, Iss. 3. P. 1–9.
10. Moreno Y., Pastor-Satorras R., Vespignani A. Epidemic Outbreaks in Complex Heterogeneous Networks // The European Physical Journal B. 2002. Vol. 26. P. 521–529.
11. Dezső Z., Barabási A. Halting Viruses in Scale-Free Networks // Physical Review E. 2002. Vol. 65, Iss. 5. P. 1–4.
12. Are Randomly Grown Graphs Really Random? / D. S. Callaway, J. E. Hopcroft, J. M. Kleinberg, M. E. J. Newman, S. H. Strogatz // Physical Review E. 2001. Vol. 64, Iss. 4. P. 1–7.
13. De Meo P., Ferrara E., Fiumara G., Provetti A. Generalized Louvain Method for Community Detection in Large Networks // Proceedings of the 11th International Conference On Intelligent Systems Design And Applications (November 22–24, 2011). IEEE, 2001. P. 88–93.
14. Savchuk V. S. Graphic Model of The Target Audience of Psychological Influence in Social Networks // Information & Security: Hybrid Warfare Challenges and Responses: Lessons from Ukraine. Sofia, 2018. Vol. 41. P. 28–36.

Стаття надійшла до редакції 07.05.2021.

REFERENCES

1. Gubanov, D. A., Novikov, D. A., & Chkhartishvili, A. G. (2010). *Sotsial'nye seti: modeli informatsionnogo vliianiia, upravleniia i protivoborstva [Social networks: models of information influence, control and confrontation.]*. Moscow [in Russian].

2. Hryshchuk, R. V. (2016*). Osnovy kibernetychnoi bezpeky [Fundamentals of cyber security]*. Yu. H. Danyk (Ed.). Zhytomyr [in Ukrainian].
3. Callaway, D. S., Newman, E. J., Strogatz, S. H., & Duncan, J. (2000). Watts Network Robustness and Fragility: Percolation on Random Graphs. *Physical Review Letters, Vol. 85,* № 25, 5468–5471.
4. Newman, E., & Girvan, M. (2004). Finding and Evaluating Community Structure in Networks. *Physical Review E, Vol. 69,* Iss. 2, 1–15.
5. Molodetska – Hrynchuk, K. V. (2017). Semantychnyi analiz tekstovoho kontentu dlia vyiavlennia informatsiinykh vplyviv na aktoriv u sotsialnykh internet-servisakh [Semantic analysis of textual content for identifying informational influences on actors in social Internet services]. In *Problemy i perspektyvy rozvytku IT industrii : materialy mizhnar. nauk.-prakt. konf.[Problems and prospects of IT industry development: materials intern. scientific-practical conf.]*. Kharkiv, November, 2017. (p. 58). Kharkiv [in Ukrainian].
6. Dorogovtsev, S. N., & Mendes, J. F. (2003). *Evolution of Networks. From Biological Nets to the Internet and WWW.* Oxford: Oxford University Press.
7. Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic Spreading in Scale-Free Networks. *Physical Review Letters, Vol. 86,* № 14, 3200–3203.
8. Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic Dynamics and Endemic States in Complex Networks. *Physical Review E, Vol. 63,* Iss. 6, 1–8.
9. Pastor-Satorras, R., & Vespignani, A. (2002). Immunization of Complex Networks. *Physical Review E, Vol. 65,* Iss. 3, 1–9.
10. Moreno, Y., Pastor-Satorras, R., & Vespignani, A. (2002). Epidemic Outbreaks in Complex Heterogeneous Networks. *The European Physical Journal B, Vol. 26*, 521–529.
11. Dezső, Z., & Barabási, A. (2002). Halting Viruses in Scale-Free Networks. *Physical Review E, Vol. 65,* Iss. 5, 1–4.
12. Callaway, D. S., Hopcroft, J. E., Kleinberg, J. M., Newman, M. E. J., & Strogatz, S. H. (2001). Are Randomly Grown Graphs Really Random? *Physical Review E, Vol. 64,* Iss. 4, 1–7.
13. De Meo, P., Ferrara, E., Fiumara, G., & Provetti, A. (2001). Generalized Louvain Method for Community Detection in Large Networks. In *Proceedings of the 11th International Conference On Intelligent Systems Design And Applications. IEEE*. November 22–24, 2011. (pp. 88–93).
14. Savchuk, V. S. (2018). Graphic Model of The Target Audience of Psychological Influence in Social Networks. In *Information & Security: Hybrid Warfare Challenges and Responses: Lessons from Ukraine, Vol. 41,* 28–36. Sofia.

V. S. Savchuk

APPLICATION OF PERCOLATION PROPERTIES TO COUNTER THE SPREAD OF DESTRUCTIVE PSYCHOLOGICAL INFLUENCE IN SOCIAL NETWORKS

Modern planning of psychological operations is not possible without the use of information technology, such as modeling tools that ensure the accuracy of planned operations and predict their results. The article proposes the concept of counteracting the spread of destructive information influences through personal accounts of social networking communities, which, unlike the known ones, is based on preliminary simulation of a particular community to identify

key and most vulnerable actors in it that require neutralization (blocking). removal will lead to a sharp disintegration (percolation) of the community. The paper presents the results of simulation experiments on the purposeful blocking of accounts of social communities of the social network "VKontakte", which is a source of destructive influence. It is established that the percolation effect occurs both for the graph of the whole network and for individual communities in the middle of the analyzed community, found using various known clustering methods. As the simulation results show, determining the percolation threshold allows to establish the share of the most vulnerable vertices (actors) that require blocking to counteract the spread of destructive influences on social networks. It is shown that the estimate of the percolation threshold varies within 30–50% of purposefully distant vertices. It is assumed that the enemy has a similar strategy and can use it to spread destructive influence. On the other hand, if we proceed from the position of the attacker in the task of information confrontation, then simulation based on current data makes it possible to develop an optimal strategy to counter a particular community that poses a danger. The proposed approach contributes to the development of information technology as protection of personal accounts of social networks from destructive influences, and effective counteraction in the tasks of information influence, management and confrontation.

Keywords: *social networks; scaleless graphs; destructive psychological influence; percolation of the graph.*