Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Department of Electronics, Robotics, Monitoring and IoT Technologies, Professor, National Aviation University.

Ключко Олена Михайлівна, кандидат біологічних наук (біофізика), доцент кафедри електроніки, робототехніки і технологій моніторингу та Інтернету речей Національного авіаційного університету.
E-mail: kelenaXX@ukr.net.
Orcid ID: 0000-0003-4982-7490.
Ключко Елена Михайловна, Кандидат биологических наук (биофизика), доцент кафедры электроники, робототехники и технологий и интенета мониторинга вещей Национального авиационного университета.
Klyuchko Olena, Candidate of Sciences (Biophysics), Associate Professor Department of Electronics,Robotics, Monitoring and IoT Technologies National Aviation University.

Шутко Володимир Миколайович, доктор технічних наук, професор, завідувач кафедри електроніки, робототехніки та технологій моніторингу та Інтернету речей Національного авіаційного університету.
E-mail: vnshutko@ukr.net.
Orcid ID: 0000 0002 9761 5583.
Шутко Владимир Николаевич. Доктор технических наук, Профессор, заведующий кафедры кафедры электроники, робототехники и технологий мониторингу и Интернета вещей Национального авиационного университета.
Shutko Vladimir. Doctor of Sciences (Engineering), Professor, Head of Electronics, Robotics, Monitoring and IoT Technologies of the Software Engineering Department National aviation university.

Колганова Олена Олегівна, кандидат технічних наук, асистент кафедри інженерії програмного забезпечення Національного авіаційного університету.
E-mail: kolganovae79@gmail.com.
Orcid ID: 0000 0002 1301 9611.
Колганова Елена Олеговна, кандидат технических наук, ассистент кафедры инженерии прогаманого обеспечения Национального авиационного университета.
Kolganova Olena, Candidate of Sciences (Engineering), Assistant Professor of the Software Engineering Department National aviation university.

DOI: 10.18372/2410-7840.22.14979
УДК 004.056

МОДЕЛЮВАННЯ ПРОЦЕСІВ ПОШИРЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СЕГМЕНТІ СОЦІАЛЬНОЇ МЕРЕЖІ

Олександр Улічев, Єлизавета Мелешко

У даній роботі проведено дослідження існуючих методів генерації структури соціальних мереж, запропоновано метод генерації сегменту соціальної мережі з можливістю вибору різної кількості та типів кластерів, а також здійснено моделювання процесів поширення та нейтралізації інформаційних впливів в сегменті соціальної мережі з наперед заданими особливостями топології мережі. Проведено серію експериментів для моделювання поширення та нейтралізації інформаційних впливів з застосуванням різних поведінкових стратегій агентами впливу у соціальній мережі з метою виявлення найбільш ефективних дій для поширення таких впливів. Всього було проведено три серії експериментів. Перша серія експериментів проводилася для порівняння ефективності поширення інформаційних впливів при різних структурних положеннях агенту впливу у сегменті соціальної мережі. Друга серія експериментів проводилася з метою порівняння ефективності інформаційних впливів при різній кількості контрагентів, що протидіють ворожому інформаційному впливу. Третя серія експериментів мала на меті порівняння ефективності протидії інформаційному впливу при блокуванні різної кількості соціальних зв'язків ворожого агенту впливу. Встановлено, що ефективність інформаційного впливу та розповсюдження інформації у соціальній мережі залежить не лише від особистих якостей агенту впливу, наприклад, його репутації, але й від структурного положення та характеристик вузлів з околу агенту впливу. Експерименти показують, що навіть при найвигіднішому положенні і високому потенціалі інформаційного впливу, агенту впливу можна протидіяти або ж шляхом залучення контрагентів, або шляхом блокування його соціальних зв'язків.

Ключові слова: *соціальні мережі, моделі генерації мереж, інформаційні впливи, інформаційна безпека, агенти впливу, лідери думок, інформаційне протиборство.*

ВСТУП

З розвитком технологій та розширенням покриття мережі Інтернет суттєво підвищуються можливості застосування соціальних мереж для інформаційного впливу [1]. Соціальні мережі в наш час стали одним з основних джерел інформації для користувачів мережі Інтернет. Вони надають інструменти для міжособової та масової комунікації, пошуку даних, перегляду новин, тощо [2]. У той же час СМ стали зручним середовищем для поширення інформаційно-психологічних впливів та маніпулювання суспільною думкою, що викликає загрози як для окремих користувачів, так і для суспільства і держави в цілому [1, 3].

Мета інформаційних впливів у соціальних мережах може бути досить різною: від реклами товарів і послуг [4] до політичної пропаганди і питань державної безпеки [1, 5]. У сучасному світі однією з головних загроз інформаційній безпеці держави є саме інформаційно-психологічні впливи через засоби масової інформації, соціальні медіа, тощо [1-5]. Вони мають на меті формування певних ідей, поглядів, уявлень, переконань, спонукання до певних дій або бездіяльності. На ефективність та швидкість розповсюдження інформації в соціальній мережі впливає ряд факторів, зокрема, можна виділити наступні: особистісні характеристики агенту впливу, що розповсюджує інформацію, його структурне положення в соціальній мережі, рівень довіри та інформаційного спротиву інших учасників інформаційного обміну – користувачів соціальної мережі [1-4]. Для дослідження, прогнозування перебігу подій та вибудовування стратегій протидії інформаційним впливам у мережі Інтернет можуть бути застосовані моделі генерації соціальних мереж та інформаційних впливів у них [3, 6].

Для генерування структури соціальної мережі за останні десятиліття запропоновано багато різних моделей [3, 7-12]. Кожна з моделей має свої недоліки та переваги. Але їх переважна більшість орієнтована на моделювання великих мереж», відповідно до цих моделей ставляться вимоги забезпечення зв'язності, малого діаметру мережі та інші характеристики, що властиві великим мережам [13-14]. Якщо ж необхідно дослідити поширення інформаційного впливу у певному сегменті соціальної мережі, то доцільним є забезпечення дещо інших характеристик мережі: можливість обрання структури соціальних зв'язків в околі агенту впливу, можливість обрання типів та кількості кластерів у сегменті мережі, моделювання особистісних характеристик користувачів мережі, моделювання різних стратегій поширення інформації виходячи із структури мережі. Відповідно для вирішення проблеми моделювання виділеного сегменту мережі мають бути запропоновані інші підходи.

Генерація структури сегменту соціальної мережі та моделювання поширення у ньому інформаційних впливів є допоміжним інструментом для дослідження та прогнозування процесів інформаційного протиборства у кіберпросторі та дозволить краще вибудовувати стратегії протидії виявленим агентам негативного інформаційного впливу у мережі Інтернет.

Таким чином задача моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі з наперед заданою топологією є важливою науково-практичною задачею, вирішення якої дозволить надати додаткові інструменти для прийняття рішень стосовно захисту від ворожих інформаційних впливів у ході інформаційного протиборства.

ПОСТАНОВКА ЗАДАЧІ

Метою роботи є моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі з наперед заданою топологією для дослідження та прогнозування процесів інформаційного протиборства у соціальних мережах з метою прийняття рішень стосовно обрання стратегій захисту від ворожих інформаційних впливів.

Для вирішення поставленої задачі необхідно розв'язати наступні завдання:

1. Запропонувати метод генерації структури сегменту соціальної мережі, що надавав би можливість генерувати мережу з наперед заданими властивостями з точки зору структури та щільності зв'язків між вузлами мережі.

2. Запропонувати спосіб визначення найбільш вигідного структурного положення агенту впливу у соціальній мережі для розповсюдження інформаційного впливу.

3. Провести серії експериментів на згенерованому сегменті соціальної мережі для дослідження ефективності різних стратегій протидії ворожим агентам впливу:

3.1. Серія експериментів 1: порівняння ефективності інформаційних впливів при різних структурних положеннях агенту впливу у сегменті соціальної мережі.

3.2. Серія експериментів 2: порівняння ефективності інформаційних впливів при різній кількості контрагентів, що протидіють ворожому інформаційному впливу.

3.3. Серія експериментів 3: порівняння ефективності протидії інформаційному впливу при блокуванні різної кількості соціальних зв'язків ворожого агенту впливу.

ВИРІШЕННЯ ПОСТАВЛЕНОЇ ЗАДАЧІ

Було проведено дослідження існуючих моделей генерації структури соціальних мереж (табл.1). Більшість запропонованих підходів орієнтовані на моделювання "великих" соціальних мереж і їх складно застосувати для моделювання окремого сегменту соціальної мережі. Аналіз існуючих моделей показує, що вони дозволяють генерувати соціальні мережі з низьким рівнем кластеризації, а також не передбачають можливості генерування мереж з наперед заданою структурою соціальних зв'язків та задавати конкретну кількість і типи кластерів. В таблиці 1 наведено порівняння найбільш відомих існуючих моделей генерації соціальних мереж з вказанням їх недоліків з точки зору моделювання відокремленого сегменту соціальної мережі.

Як видно з табл. 1, розглянуті методи моделювання не задовольняють ряду вимог, що є важливими при моделюванні "малих" мереж, або відокремленого сегменту соціальної мережі. Зокрема, важливими вимогами для вирішення таких задач є можливість моделювати соціальну мережу з наперед заданою топологією (структура зв'язків), а виокремлений сегмент мережі повинен характеризуватися наявністю певних кластерів – набір вузлів (користувачів) пов'язаних спільними інтересами й такими, що постійно здійснюють інформаційний обмін всередині певної групи. Окрім цього для реальної соціальної мережі характерний нерівномірний розподіл щільності зв'язків, що також бажано мати змогу врахувати при генерації сегменту мережі.

Таблиця 1

Порівняння моделей генерації соціальних мереж

Моделі генерації соціальних мереж	**Малий діаметр графу**	**Рівень асортативності**	**Зв'язність графу**	**Високий рівень кластеризації**	**Можливість неоднорідного розподілу щільності зав'язків**	**Топологія мережі обирається (вручну обирається набір кластерів різних типів)**	**Моделювання околу окремого вузла**
Эрдеша-Реньи [7, 13, 14]	+/-	-	+/-	-	+/-	-	-
Уоттса-Строгатца [8]	+	-	+	+	-	-	-
Барабаши-Альберта [9, 13, 14]	+	+	+	-	+	-	-
Боллобаша-Ріордана [10, 13, 14]	+	+	+	-	+	-	-
Баклі-Остхуса [11, 13]	+	+	+	-	+	-	-
Чаес-Боргса [12]	+	+	+	-	-	-	-

Отже, існуючі моделі та підходи генерування соціальних мереж мають ряд недоліків та не дають можливості генерувати мережу з наперед заданою структурою соціальних зв'язків, тобто вказувати кількість і типи кластерів мережі. Для вирішення даної задачі запропоновано метод генерування соціальної мережі на основі параметризованних кластерів [15, 16]. Для моделювання процесу розповсюдження інформаційних впливів використовується програмна модель [16], що дозволяє зібрати статистику – кількість залучених до розповсюджуваної ідеї вузлів мережі за фіксовану кількість ітерацій процесу розповсюдження інформаційного впливу.

Для генерації структури сегменту соціальної мережі та моделювання поширення у ньому інформаційних впливів запропоновано модель, що описана в статтях [15, 16, 17].

Запропонований метод генерації соціальної мережі базується на побудові мережі з параметризованих кластерів. В якості можливих типів кластерів обрано наступні – група, лідерська група та кліка.

Формально вибрані кластери можуть бути описані формулами (1-3):

$$G_{grupa} = (V_n \mid \forall\, V_i, V_j : i, j, k_i \le n \;\; \exists\, \{E_{i,k1}, E_{k1,k2}, E_{k2,k3} \ldots E_{ki,j}\}), \quad (1)$$

де V_i, V_j – довільно вибрані в кластері вузли, а $E_{i,k1}, E_{k1,k2}, E_{k2,k3} \ldots E_{ki,j}$ – послідовність ребер, що зв'язують V_i, V_j через інші вузли кластера.

В кліці існує зв'язок між будь-якими довільно вибраними вузлами:

$$G_{clica} = (V_n \mid \forall\, V_i, V_j : i, j \le n \;\exists\, E_{i,j}). \quad (2)$$

В лідерській групі існує принаймні один вузол (лідер), що має зв'язки з усіма іншими вузлами кластера:

$$G_{lid\_grupa} = (V_n \mid \exists\, i \le n, \forall\; j \le n \;\exists\, E_{i,j}), \quad (3)$$

де *j* – індекс вузла –лідера групи.

В запропонованій моделі вузол (користувач соціальної мережі) описується наступним чином:

$$V_i = < Av_i, Rv_i, Ov_i, Iv_i, \{Vj_i\} >, \quad (4)$$

де *A* (Active) – рівень активності користувача, кількість активних діалогів (звернень до інших користувачів) за одну ітерацію моделі; *R* (Reputation) – рівень репутації, сила переконання; *O* (Opposite) – рівень інформаційного спротиву, рівень недовіри до нової інформації; *I* (Involvement) – ступінь залученості до поширюваного інформаційного впливу, рівень довіри; $\{Vj_i\}$ – множина контактів, вузлів з якими існує інформаційний обмін, вузла V_i.

У запропонованій моделі можуть бути наступні типи вузлів:

– простий вузол (вузол) – звичайний користувач соціальної мережі;

– агент (генератор ідеї) – користувач, що розповсюджує певний інформаційний вплив;

– контрагент (контргенератор) – користувач, що розповсюджує контрпропаганду до поширюваного інформаційного впливу у соціальній мережі.

Процес інформаційного обміну реалізується за наступною формулою:

$$Iv_j = \sum_{m=1}^{x} \sum_{i=1}^{n} k_{ij} \cdot \alpha_{im}, \quad (5)$$

де Iv_j – рівень залученості *j*-го вузла до α-ідеї (α-ідея – поширюваний інформаційний вплив), x – поточна ітерація моделювання, *n* – кількість контактів *j*-го вузла, α_{im} – повідомлення від *i*-го вузла на ітерації *m*, фіксує наявність повідомлення на ітерації *m*. Значення α_{im} визначається за формулою:

$$\alpha_{\text{im}} = \begin{cases} 1, \alpha - \textit{посил від } V_i \textit{ був} \\ 0, \alpha - \textit{посилу від } V_i \textit{ не було}. \end{cases} \quad (6)$$

У випадку наявності у соціальній мережі контрагентів, що протидіють ворожим інформаційним впливам, необхідно враховувати і їх впливи, тоді формула (6) матиме вигляд:

$$\alpha_{\text{im}} = \begin{cases} 1, \alpha - \textit{посил від } V_i \textit{ був}, (V_i - \textit{агент впливу}) \\ 0, \alpha - \textit{посилу від } V_i \textit{ не було} \\ -1, \alpha - \textit{посил від } V_i \textit{ був}, (V_i - \textit{контрагент}), \end{cases} \quad (7)$$

де k_{ij} – коефіцієнт інформаційного впливу, що визначається співвідношенням:

$$k_{ij} = \frac{Rv_i}{Ov_j}, \quad (8)$$

де Rv_i – рівень репутації вузла V_i, Ov_j – рівень інформаційного супротиву вузла V_j.

Використаємо описану вище модель (її програмну інтерпретацію) для моделювання сегменту соціальної мережі з наперед заданою структурою.

Було згенеровано сегмент соціальної мережі з наперед заданою топологією, до якої входить:

– 1 лідерська група (ЛдГ1) з 32 вузлів з високою щільністю вузлів та високим рівнем інформаційного супротиву;

– 1 лідерська група (ЛдГ2) з 32 вузлів з низькою щільністю вузлів та високим рівнем інформаційного супротиву;

– 2 лідерських групи (ЛдГ3, ЛдГ4) з 25 вузлів з випадковим розподілом щільності вузлів та високим рівнем інформаційного супротиву;

– 4 групи (Гп1, Гп2, Гп3, Гп4), в яких кількість вузлів відповідно 24, 24, 24 та 20;

– 1 кліка (Кл1) з 15 вузлів;

– 5 вузлів, що не входять до жодного з кластерів, але мають зв'язки з деякими з них.

Загальна кількість вузлів в сегменті – 226.

Було проведено наступні експерименти на згенерованому сегменті соціальної мережі.

Серія експериментів №1. Виявлення найбільш вигідної структурної позиції у соціальній мережі для агенту впливу, що дозволить йому найбільш швидко та ефективно розповсюдити інформаційний вплив.

Оберемо спосіб визначення найбільш вигідного структурного положення агенту впливу у соціальній мережі. Ряд досліджень проведених в області маркетингу та соціології доводять ефективність застосування для інформаційного впливу (зокрема, розповсюдження вірусної реклами) "лідерів думок" [18, 19]. Термін "лідери думок" (opinion leader) введений соціологом Полом Лазарсфельдом в 1940-х роках. Під час передвиборної кампанії в США він з колегами досліджував, як медіа впливають на громадську думку і голосування. Вчені виділили дві групи людей: ті, хто визначилися з вибором і ті, хто сумнівається. В ході свого дослідження вченні прийшли до висновку, що на другу групу людей більш істотний вплив мали окремі співрозмовники (яких вони і назвали "лідерами думок"), ніж офіційні інформаційні джерела та ЗМІ [20]. Лідери думок (ЛД) відрізняються своїми психологічними особливостями, інтересами і харизмою. Цей набір якостей дозволяє лідерам думок формувати навколо себе певну аудиторію і суттєво впливати на формування думок і суджень з окремих питань.

З точки зору структурного положення та наявних зв'язків "лідер думок" характеризується наявністю великої кількості контактів порівняно з іншими вузлами в його околі.

Дослідження окремих авторів показують, що сьогодні ЛД стають інструментом в руках PR-менеджерів і корпорацій, і думка, яку вони доносять до своєї аудиторії далеко не завжди власна. Зокрема Лазуткіна Є. В. у своїй статті [18], відзначає, що в останні роки проявляється тенденція комерціалізації напрацьованої популярності в мережі і хоча топові блогери лідери думок і дорожать своєю репутацією, вони досить часто використовують свою репутацію та довіру інших учасників мережі для отримання фінансових вигод.

На тлі своєї основної тематики "лідери думок" можуть розповсюджувати інформацію під замовлення: розкручування брендів, реклама товарів, політична реклама чи інші інформаційні впливи. Зокрема, на значиму роль блогерів в процесах просування товарів та реклами вказують автори Санін М.К., Барков Є.І. [19].

В якості ЛД в досліджуваному сегменті соціальної мережі можуть виступати лідери груп. Ці вузли в порівнянні з іншими характеризуються найбільшою кількістю зв'язків та високим рівнем репутації. Порівняємо ефективність розповсюдження інформації через дані вузли. В згенерованій мережі кожен вузол має свій унікальний індекс, будемо використовувати дані індекси для ідентифікації окремого вузла в мережі. Для порівняння окрім лідерів груп візьмемо до уваги й один з вузлів кліки.

Проведемо експеримент з використанням різних стратегій розповсюдження інформаційних впливів у сегменті соціальної мережі.

У розробленій моделі стратегії розповсюдження інформаційних впливів визначають пра-

вило вибору вузла для інформаційної атаки на поточній ітерації.

В ході експерименту застосовувались дві стратегії: стратегія "Дерево" та стратегія "Кущ" [16].

Стратегія "Дерево" обирає вузли для інформаційного впливу на основі певного критерію, у даній серії експериментів на основі критерію вибору вузлів з мінімальним інформаційним супротивом. Така стратегія формально описується наступним чином:

$$P_{tree}=\left\{u_i \in U_g \mid Ou_i \rightarrow \min, |u|=2^{lg}, |u| \le K*Ag, u_i \notin G\right\}. \quad (9)$$

За даною стратегією поведінка жорстко детермінована, тому, з урахуванням незмінної структури соціальної мережі, результат буде однаковим при кожному наступному моделюванні.

Стратегія "Кущ", що формально описується як (10), обирає вузли випадковим чином з доступних контактів агенту впливу:

$$P_{buch}=\left\{u_i \in U_g \mid i=random(|U_g|), |u| \le Ag\right\}. \quad (10)$$

Тому в ході моделювання з використанням даної стратегії будуть отримувані різні результати. Для отримання достовірної оцінки проводились серії експериментів по 30 серій для кожного вузла та брати середнє значення результатів.

В табл. 2 наведено результати моделювання (кількість ітерацій необхідних для захоплення всіх вузлів мережі) з використанням стратегії (9) та усереднені результати серій експериментів з використанням стратегії (10). Одна ітерація моделі умовно імітує 1 день, максимальна кількість ітерацій моделі рівна – 365 (вважаємо, що протягом року актуальність інформаційного впливу проходить).

Найкращі результати (захоплення всіх вузлів сегменту за меншу кількість ітерацій моделі) за обома стратегіями показав вузол V77. Також варто відмітити, що V133 (член кліки) з використанням стратегії "Кущ" показує кращі результати ніж лідер групи V99.

Це пояснюється тим, що в порівнянні з вузлом V99 він має більшу кількість зв'язків (32 проти 25), а в порівнянні з V185 менший рівень інформаційного супротиву. Це пояснюється особливістю стратегії "Кущ" і її ефективністю за умови високої щільності зв'язків у досліджуваному сегменті соціальної мережі.

Таблиця 2

Швидкість захоплення всіх вузлів мережі (кількість ітерацій моделі) для різних структурних позицій агенту впливу та різних стратегій розповсюдження інформаційних впливів

Агент впливу	**Стратегія "Дерево"**	**Стратегія "Кущ"**
V185 – лідер групи ЛдГ1	89	135
V77 – лідер групи ЛдГ2	87	131
V99 – лідер групи ЛдГ3	94	142
V133 – член кліки Кл1	112	140

Отже, в ході експерименту вибрано найбільш вдалий початковий вузол для інформаційного розповсюдження в досліджуваному сегменті мережі це вузол V77.

Серія експериментів №2. Оцінка необхідної кількості контрагентів для інформаційної протидії ефективно вибраному агенту впливу у соціальній мережі. В даній серії експериментів оцінимо ефективність інформаційного впливу за умови наявності агентів, що розповсюджують контрідею. Контрагентів будемо обирати випадковим чином, оцінимо втрати ефективності при різній кількості контрагентів. За умови випадкового вибору контрагентів та застосування стратегії (10) результати експериментів можуть суттєво відрізнятись. Тому для отримання достовірного результату будемо проводити для кожного випадкового набору серію з 30 експериментів та брати середнє значення результатів.

Окрім випадкового вибору контрагентів для порівняння проведемо експерименти, де в якості контрагентів будемо використовувати лідерів груп з табл. 2. Результати даних серій в кінцевій таблиці відмічені жирним шрифтом. Усереднені показники розподілу вузлів залучених до ідеї та контрідеї приведено в табл. 3.

Серія експериментів №3. Оцінка ефективності протидії інформаційному впливу при блокуванні різної кількості соціальних зв'язків ворожого агенту впливу. Даний експеримент полягає в вилучені частини зв'язків лідера групи V77 і оцінці зміни кількості залучених вузлів в залежності

від кількості вилучених зв'язків. Варто враховувати, що при вилучені зв'язків може порушуватись зв'язність графу, тому, аби запобігти втраті зв'язності, випадковий зв'язок з "лідером думок" (вузлом V77) будемо замінювати на зв'язок з випадковим іншим вузлом.

За таких умов ймовірність втрати зв'язності суттєво знижується, але не гарантується повністю. На збереження зв'язності однозначно буде вказувати факт залучення всіх вузлів соціальної мережі. Часткове залучення може бути як результатом втрати ефективності так і результатом втрати зв'язності.

Також необхідно враховувати, що гіпотетично при втраті невеликої кількості малозначущих (з точки зору розповсюдження) зв'язків можуть бути отримані результати кращі, ніж в серії експериментів №1.

Це може бути пояснене тим, що генератор не витрачає зайвий час на залучення незначущих вузлів (що мають мінімальний результуючий вплив), а замість того має можливість впливу на вузли більш значимі для кінцевого результату. Але така ситуація можлива лише при застосуванні стратегій з випадковим вибором вузла. В ході експерименту буде використовуватись детермінована стратегія (9), тому втрата зв'язків не може позитивно позначитись на результаті. Залежність втрат від кількості заблокованих зв'язків у відсотках (усереднені показники серії експериментів) показані на рис. 1.

Рис. 1 Збільшення часу залучення вузлів до інформаційного впливу при блокуванні частини зв'язків агента впливу

З рис. 1 видно, що вже втрата 3-5 зв'язків (при початковій кількості 32 зв'язки) досить суттєво впливають на швидкість залучення вузлів мережі до поширюваного інформаційного впливу.

Таблиця 3

Результати моделювання інформаційного протистояння з залученням контрагентів

Кількість контрагентів	**Ідентифікатори вузлів-контрагентів**	**Кількість залучених до ідеї вузлів**	**Кількість залучених до контрідеї вузлів**	**Кількість незалучених вузлів**	**Кількість ітерацій до стабілізації**
2 контрагенти	V33, V196	165	61	0	70
	V160, V29	115	111	0	150
	V16, V219	216	10	0	53
	V185, V220	**113**	**65**	**48**	**40**
3 контрагенти	V160, V29, V12	85	73	68	365
	V160, V29, V107	81	76	69	365
	V155, V29, V107	127	37	62	145
	V185, V29, V107	**72**	**108**	**45**	**130**
4 контрагенти	V159, V38, V119, V15	96	65	65	92
	V138, V80, V215, V135	91	70	65	98
	V185, V29, V107, V133	**68**	**119**	**39**	**120**
5 контрагентів	V51, V48, V22, V127, V173	86	73	67	128
	V99, V133, V185, V205	**68**	**145**	**13**	**135**

Таблиця 4

Результати моделювання інформаційного протистояння
при блокуванні різної кількості соціальних зв'язків ворожого агенту впливу

Кількість вилучених зв'язків	**Ідентифікатори заблокованих вузлів**	**Кількість залучених до ідеї вузлів**	**Кількість ітерацій для захоплення вузлів**	**Середнє значення**
1 зв'язок	V59	226	91	101
	V58	226	116	
	V173	226	97	
	V55	226	99	
3 зв'язки	V52, V60, V70	226	98	112
	V65, V74, V75	226	132	
	V56, V69, V74	226	106	
5 зв'язків	V60, V64, V56, V61, V76	226	117	114
	V48, V56, V66, V67, V68	226	111	
10 зв'язків	V49, V51, V53, V55, V56, V64, V68, V72, V74, V76	226	158	158

ВИСНОВКИ

Досліджено існуючі моделі генерації структури соціальних мереж, визначено їх недоліки з точки зору моделювання "малих" мереж та сегментів соціальної мережі з різними топологіями. Запропоновано метод генерації структури сегменту соціальної мережі з наперед заданими особливостями топології. Запропоновано спосіб визначення найбільш вигідного структурного положення агенту впливу у соціальній мережі для розповсюдження інформаційного впливу. Проведено серію експериментів для моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі.

В серії експериментів №1 модель показує високі показники впливу "лідерів думок", серед запропонованих альтернатив в ході експерименту вибрано вузол з найкращим показником по швидкості захоплення вузлів соціальної мережі в ході інформаційної взаємодії.

В серії експериментів №2 було здійснено оцінку необхідної кількості контрагентів для ефективного інформаційного спротиву. Так при випадковому виборі контрагентів розподіл залучених до ідеї та залучених до контрідеї вузлів складає приблизно 75% до 25%. Але при залучені до контрагентів вузлів з високим потенціалом інформаційного впливу розподіл змінюється: 50% залучених до ідеї, 28% залучених до контрідеї та 22% вузли не визначились, тобто, з'являється досить значима кількість вузлів, що не були залучені ні агентами, ні контрагентами. При збільшені випадкових контрагентів (3 контрагенти) розподіл змінюється наступним чином: 42% залучених до ідеї, 29% залучених до контрідеї та 29% не визначились. При такій кількості контрагентів в серіях експериментів часто спостерігалась ситуація, коли зміни відбувались протягом всіх 365 ітерацій.

При залучені трьох контрагентів з включенням вузлів з високим потенціалом розповсюдження вже спостерігається перевага контрагентів з результатами: 32% до 48% та до 20%. Моделювання показує, що при випадковому виборі контрагентів необхідно залучати не менше чотирьох, при залучені в якості контрагентів вузлів з високим потенціалом впливу перевагу вже має команда з трьох контрагентів.

В той же час варто відмітити, що вдало вибраний агент з високим потенціалом впливу навіть за наявності 5 і більше супротивників встигає переконати біля 25% оточення.

Серія експериментів №3 мала на меті оцінку втрати потенціалу інформаційного впливу при блокуванні (вилучені) певної кількості зв'язків агенту впливу. Усереднені показники даної серії експериментів показують, що вже втрата 3-5 зв'язків (при початковій кількості 32 зв'язки) досить суттєво впливають на швидкість залучення вузлів мережі до поширюваної ідеї.

Проведені експерименти показали, що ефективність інформаційного впливу і розповсюдження інформації у соціальній мережі залежить не лише від особистих якостей агенту впливу (наприклад, його репутації), але й від його структурного положення та оточення (характеристик вузлів з околу агенту).

Експерименти показують, що навіть при найвигіднішому положенні і високому потенціалі інформаційного впливу агента йому можна протидіяти або ж шляхом залучення (вербування) контрагентів, або шляхом блокування його зв'язків.

Конкретний метод протидії залежить від конкретної ситуації та структури сегменту соціальної мережі, може бути застосований і комбінований метод, коли при наявності протидіючих контрагентів є можливість і блокування певної кількості зв'язків.

ЛІТЕРАТУРА

[1] Курбан О. В.Сучасні інформаційні війни в соціальних онлайн-мережах / О. В. Курбан // *Інформаційне суспільство*. - 2016. - Вип. 23. - С. 85-90. -Режим доступу: http://nbuv.gov.ua/ UJRN/ is_2016 _23_15.

[2] Захарченко А.П. Інтернет-медіа: ін терактивний навчальний посібник для курсу "Підтримка сайту" для студентів відділення "Видавнича справа та редагування". – К.: *Видавець Марченко*, 2014. – 198с.

[3] Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. *Социальные сети: модели информационного влияния, управления и противоборства* / Под ред. чл.-корр. РАН Д.А. Новикова. – 2-е изд., стереотипное. – М.: Издательство физико-математической литературы: МЦНМО, 2010. – 228 с.

[4] Бергер Й. Заразливий. *Психологія вірусного маркетингу* / Пер. з англ. Олени Замойської. – К.: Наш Формат, 2015. – 224 с.

[5] Богуш В.М., Юдін О.К. *Інформаційна безпека держави*. – К.: "МК-Прес", 2005. – 432 с.

[6] Ландэ Д.В., Фурашев В.Н., Брайчевский С.М., Григорьев А.Н. *Основы моделирования и оценки электронных информационных потоков*: Монография. – К.: Инжиниринг, 2006. – 176 с.

[7] Erdös P., Rényi A. On the evolution of random graphs // *Magyar Tudományos Akademia Matematikai Kutato Intezetenek Közlemenyei* [Publications of the Mathematical Institute of the Hungarian Academy of Sciences]. – T. 5., 1960. – pp. 17-61.

[8] Watts D.J.; Strogatz, S. H. Collective dynamics of "small-world" networks // *Nature. 393 (6684)*, 1998. – pp. 440-442.

[9] Barab´asi L.-A., Albert R., Jeong H. Scale-free characteristics of random networks: the topology of the world-wide web. Physica, A281: Macmillan Publishers Ltd, 2000. – pp. 69–77.

[10] Bollobás B., Riordan O. Mathematical results on scale-free random graphs // *Handbook of graphs and networks*. Weinheim: Wiley-VCH, 2003. – pp. 1-34.

[11] Bollobás B., Borgs C., Chayes T., Riordan O.M. Directed scale-free graphs. *ProceedingSODA '03 Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, 2003. – pp. 132–139.

[12] Buckley P.G., Osthus D. Popularity based random graph models leading to a scale-free degree sequence. *Discrete Mathematics: North-Holland*, 2004. – pp. 53-63.

[13] Берновски М.М., Кузюрин Н.Н. Случайные графы, модели и генераторы безмасштабных графов // *Труды Института системного программирования РАН, текст научной статьи по специальности «Математика»*, 2012. – С. 419-432.

[14] Райгородский А.М. Модели случайных графов и их применение // *Труды МФТИ*, 2010. – Т.2, №4. – С. 130-140.

[15] Ulichev O., Meleshko Y., Khokh V. The computer simulation method of a social network structure for the research of dissemination processes of informational influences // *Scientific and Practical Cyber Security Journal (SPCSJ)* 4(3). – Georgia, Tbilisi, 2019. – pp. 34-47.

[16] Ulichev O., Meleshko Ye., Sawicki D., Smailova S. *Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors* // Proc. SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, 2019. – 9 p.

[17] Улічев О.С. Математична модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі // *Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація*, Вип. 31. – Кропивницький: ЦНТУ, 2018. – С. 165-174.

[18] Лазуткина Е. В. Лидеры мнений в информационном пространстве блогосферы рунета//*Вестн. НГУ*. Серия: История, филология, Т. 15, № 6, 2016. – С. 51-59.

[19] Санин М.К., Барков Е.И. Эффективность блоггинга как маркетингового инструмента // *Научный журнал НИУ ИТМО. Серия "Экономика и экологический менеджмент"*. № 2, 2016 – С. 107-112.

[20] Katz E., Lazarsfeld P. *Personal Influence: The Part Played by People in the Flow of Mass Communications* // Publisher: Routledge, 2005. – 434 p.

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ И НЕЙТРАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ В СЕГМЕНТЕ СОЦИАЛЬНОЙ СЕТИ

В данной работе проведено исследование существующих методов генерации структуры социальных сетей, предложен метод генерации сегмента социальной сети с возможностью выбора разного количества и типов кластеров, а также осуществлено моделирование процессов распространения и нейтрализации информационных воздействий в сегменте социальной сети с заранее заданными особенностями топологии сети. Проведена серия экспериментов для моделирования распространения и нейтрализации информационных воздействий с применением различных поведенческих стратегий агентами влияния в социальной сети с целью выявления наиболее эффективных действий для распространения таких воздействий. Всего было проведено три серии экспериментов. Первая серия экспериментов проводилась для сравнения эффективности распространения информационных воздействий при различных структурных положениях агента влияния в сегменте социальной сети. Вторая серия экспериментов проводилась с целью сравнения эффективности информационных воздействий при разном количестве контрагентов, которые противодействуют враждебному информационному влиянию. Третья серия экспериментов имела целью сравнение эффективности противодействия информационному воздействию при блокировании разного количества социальных связей враждебного агента влияния. Установлено, что эффективность информационного воздействия и распространения информации в социальной сети зависит не только от личных качеств агента влияния, например, его репутации, но и от структурного положения и характеристик узлов в окрестности агента влияния. Эксперименты показывают, что даже при самом выгодном положении и высоком потенциале информационного воздействия агенту влияния можно противодействовать или путем привлечения контрагентов, или путем блокирования его социальных связей. Конкретный метод противодействия зависит от конкретной ситуации и структуры сегмента социальной сети. Может быть применен и комбинированный метод, когда одновременно используется и распространение контринформации через контрагентов, и осуществляется блокировка определенного количества социальных связей агента влияния.

Ключевые слова: социальные сети, модели генерации сетей, информационные воздействия, информационная безопасность, агенты влияния, лидеры мнений, информационное противоборство.

MODELING THE DISTRIBUTION AND NEUTRALIZATION PROCESSES OF INFORMATION INFLUENCES IN A SOCIAL NETWORK SEGMENT

In this paper, the research of existing social network generation models was conducted, the social network segment generation method was proposed with the possibility of choosing a different number and types of clusters, and distribution and neutralization processes of information influences in a social network segment with preselected network topology was simulated. The series of experiments to simulate the distribution and neutralization of information influences using various behavioral strategies by influence agents in a social network in order to identify the most effective actions for the dissemination of such influences was carried out. In total, three series of experiments were carried out. The first series of experiments to compare the effectiveness of the dissemination of information influences at various structural positions of influence agent in the social network segment was carried out. The second series of experiments in order to compare the effectiveness of informational influences with a different number of counteragents that counteract hostile informational influence was carried out. The third series of experiments at comparing the effectiveness of countering informational influence when blocking a different number of social connections of a hostile influence agent was carried out. It has been established that the effectiveness of information influences and information dissemination in a social network depends not only on the personal qualities of the influence agent, for example, his reputation, but also on the structural position and characteristics of nodes near influence agent. Experiments show that even with the most advantageous position and high potential of information impact, influence agent can be counteracted either by attracting counterparties or by blocking his social connections. The specific method of counteraction depends on the specific situation and the structure of the social network segment. A combined method can also be applied, when the spread of counter-information through counteragents is simultaneously used, and a certain number of social connections of influence agents are blocked.

Keywords: social networks, network generation models, informational influences, information security, influence agents, opinion leaders, informational confrontation.

Улічев Олександр Сергійович, аспірант кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.
E-mail: askin79@gmail.com.
Orcid ID: 0000-0003-3736-9613.
Уличев Александр Сергеевич, аспирант кафедры кибербезопасности и программного обеспечения Центральноукраинского национального технического университета, Кропивницкий, Украина.
Ulichev Oleksandr, graduate student of Cybersecurity and Software Academic Department, Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.

Мелешко Єлизавета Владиславівна, кандидат технічних наук, доцент, докторант кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.
E-mail: elismeleshko@gmail.com.
Orcid ID: 0000-0001-8791-0063.
Мелешко Елизавета Владиславовна, кандидат технических наук, доцент, докторант кафедры кибербезопасности и программного обеспечения Центральноукраинского национального технического университета, Кропивницкий, Украина.
Meleshko Yelyzaveta, Candidate of Technical Sciences, Associate Professor, Doctoral Student of Cybersecurity and Software Academic Department, Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.

DOI: 10.18372/2410-7840.22.14980
УДК: 004.491.4

ПРОГРАМНИЙ ПРОДУКТ ТИПУ SPYWARE ТА АНАЛІЗ ЙОГО СТІЙКОСТІ ДО ВИЯВЛЕННЯ ЗАСОБАМИ ЗАХИСТУ

Олександр Ковальов, Олександр Чобаль, Василь Різак

В період активного розвитку інформаційних технологій проблема збереження конфіденційності є надзвичайно актуальною. На сьогоднішній день існують декілька тисяч різновидів шкідливих програм, які працюють за різними алгоритмами. Однак їх всіх об'єднує факт того, що вони створюються спеціалізовано для несанкціонованого користувачем модифікування, знищення, блокування та копіювання інформації, порушуючи роботу комп'ютера та комп'ютерних мереж. Існує вид шкідливих програм, які здатні нанести значної шкоди конфіденційності інформації і при цьому вони залишаються не помітними навіть для спеціалізованих програм. Мова йде про програмних шпигунів (spyware). Для виявлення в системі програмного шпигуна слід використовувати спеціалізоване програмне забезпечення, яке спрямоване на виявлення саме цього виду загроз. Однак навіть вони не можуть гарантувати повної безпеки. У даній роботі описано основні типи програмних шпигунів та розроблено Spyware типу "системний монітор", завданням якого є збір користувацької інформації з можливістю подальшої її обробки та передачі. Ефективність роботи розробленої програми продемонстровано на основі зібраних даних та від'ємних результатів сканування системи спеціалізованими програмними засобами. Розглянуто особливості роботи програмних шпигунів та проведено аналіз їх поведінки, результати якого можуть бути використані при розробці імовірнісних методів пошуку програм досліджуваного типу.

Ключові слова: Spyware, malware, програмний шпигун, кейлогер, Windows.

ВСТУП

Важливою загрозою безпеці, яка сьогодні зачіпає багатьох користувачів Інтернету є шпигунське програмне забезпечення [7, 8]. Шпигунське ПЗ - це шкідливе програмне забезпечення, яке намагається непомітно відстежувати поведінку користувачів, записувати їх звички під час вебсерфінгу або красти їх конфіденційні дані, такі як логіни та паролі. Як правило, зібрана інформація відправляється назад розповсюджувачу шпигунських програм, де вона використовується для цільової реклами або в маркетингових дослідженнях. Це відрізняє їх від інших типів шкідливих програм, таких як віруси та хробаки, які зазвичай прагнуть поширитися на інші системи та завдати їм шкоди [6].