УДК 004.9

О.С. Улічев, асп.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна, E-mail: askin79@gmail.com

Математична модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі

Метою роботи є опис результатів дослідження в напрямку моделювання процесів розповсюдження інформаційних впливів в сегменті соціальної мережі. В основі дослідження лежить запропонована автором математична модель та підходи до реалізації окремих етапів моделювання. Зокрема виділяється 3 основних етапи: моделювання структури мережі, формальний опис вузла мережі, реалізація процесу розповсюдження інформації.

Метод генерування структури мережі базується на використанні параметризованих кластерів трьох типів: кліка, група, лідерська група. Процес розповсюдження інформації запропоновано представляти ітераційним процесом, в ході якого вузли здійснюють інформаційні впливи на інші вузли, через розповсюдження інформаційних повідомлень. В статті запропоновано поняття поведінкових стратегій, що визначають критерії вибору вузла для атаки. Запропоновано їх формальне представлення.

програмна модель, інформаційний вплив, методи генерування мережі, моделі розповсюдження інформації в мережі, поведінкові стратегії

А.С. Уличев, асп.
Центральноукраинский национальный технический университет, г. Кропивницкий, Украина

Математическая модель распространения информационно-психологических воздействий в сегменте социальной сети

Целью работы является описание результатов исследования в направлении моделирования процессов распространения информационных воздействий в сегменте социальной сети. В основе исследования лежит предложенная автором математическая модель и подходы к реализации отдельных этапов моделирования. В частности выделяется 3 основных этапа: моделирование структуры сети, формальное описание узла сети, реализация процесса распространения информации.

Метод генерирования структуры сегмента сети базируется на использовании параметризованных кластеров трех типов: клика, группа, лидерская группа. Процесс распространения информации предложено представлять итерационным процессом, в ходе которого узлы осуществляют информационные влияния на другие узлы, через распространение информационных сообщений. В статье предложено понятие поведенческих стратегий, определяющих критерии выбора узла для атаки. Предложено их формальное представление.

программная модель, информационное воздействие, методы генерирования сети, модели распространения информации в сети, поведенческие стратегии

Постановка проблеми. Інформаційні впливи завжди були дієвим інструментом для маніпуляцій людьми та навіювання певних ідей. Перші методики інформаційних впливів розроблені досить давно. В останній час підходи набули особливого значення і отримали суттєвий приріст ефективності, це пов’язано з розвитком мережі Інтернет та щільним повсякденним використанням користувачами різноманітних соціальних мережевих сервісів. Реєструючись в соціальних мережах користувач потенційно стає об’єктом інформаційних атак різноманітної направленості. Мета інформаційних атак може бути абсолютно різною: від маркетингових і рекламних кампаній до політичної боротьби та інформаційної війни, як засобу створення відповідного ідейного підґрунтя для реальних бойових дій або військових переворотів. Відтак зростає інтерес до використання існуючих СЦ для інформаційних впливів. Факт використання сервісів для деструктивних інформаційних впливів вимагає вироблення методів та засобів

протистояння таким впливам. Ефективний спротив повинен передбачати: дослідження проблеми та аналіз мети впливу, виявлення зон впливу, прогнозування наслідків, вироблення методів пасивного та активного інформаційного захисту.

Одним з підходів в комплексі спротиву інформаційним впливам та атакам є моделювання поширення інформаційно-психологічних впливів у соціальних мережах з метою прогнозування їх наслідків та розробки рекомендацій для протидії ним.

Аналіз останніх досліджень і публікацій. Сьогодні багато вчених, як вітчизняних так і закордонних розглядають проблему моделювання розповсюдження інформації в мережі. Зокрема існують вже класичні моделі, найбільш відомі з них наступні.

Модель SIR детермінована модель епідемії. Модель епідемії була сформульована в роботі [1], основна ідея полягає в розподілі користувачів на групи: уразливі, заражені, не сприймаючі (користувачі з імунітетом). В [1] пропонують розглядати ймовірності потрапляння користувачів в кожну з груп та параметри: частота зараження й швидкість одужання. В цілому модель описується системою диференціальних рівнянь. Пізніше була запропонована розширена модель епідемії, доповнення полягали в тому, що в мережі постійно спостерігається динаміка наявності учасників, якісь користувачі включаються в мережу, інші покидають її. Введення даних параметрів в модель і стало розширеною SIR моделлю. А в 1965 році була сформульована модель Далея-Кендалла [2] для опису поширення чуток. Модель виявилась досить вдалою і до сих пір використовується в деяких симуляторах та програмних моделях. Моделі, що базуються на SIR, націлені на кількісну оцінку розповсюдження і не враховують канали зв'язку та структуру мережі.

Пізніше деякими авторами було запропоновано клітинні автомати, на думку авторів [3, 4] такі моделі більш точно відображають процес, бо враховують стани навколишніх клітин, що досить близько по суті до соціальної мережі.

Більш сучасні ідеї пропонують іноземні вчені, наприклад, Губанов Д.А. в [7], його ідеї полягають в застосуванні у дослідженнях процесів розповсюдження інформації теорії ігор, та вітчизняні вчені, зокрема Ланде Д.В., Грайворонська А.М. [8, 9], які розглядають мультиагентну модель розповсюдження з параметрами впливу лайк/дислайк, репост та іншими. Врахування даних параметрів дозволяє наблизити модель до сучасного поняття соціальної мережі як веб-сервісу.

Серед розглянутих моделей не виявлено прикладів моделей, які б враховували поведінку окремого вузла, стратегію розповсюдження інформації, яку обирає вузол в процесі інформаційного впливу.

Постановка завдання. Метою даної роботи є розробка математичної моделі поширення інформаційно-психологічних впливів у сегменті соціальної мережі, як бази для створення програмної моделі для моделювання та дослідження різноманітних ситуацій та варіативних змін.

Задача моделювання соціальної мережі (сегменту мережі) полягає в дослідженні впливу різноманітних факторів на швидкість розповсюдження інформації та динаміки інформаційного впливу. Використовуючи модель планується досліджувати наступні фактори впливу: структуру сегменту мережі, що моделюється; щільності зв'язків в сегменті мережі; початкове положення вузла – розповсюджувача інформації; поведінкові стратегії, які застосовує активний вузол. При цьому об'єктом дослідження є не лише соціальні мережі в їх електронному варіанті реалізації як веб-сервісів мережі, поняття розглядається в широкому змісті. Соціальна мережа – це структура, що складається з масиву вузлів, які представлені соціальними об'єктами (людьми, групами

або організаціями) та взаємозв'язками між ними. В якості зв’язків розглядаються будь-які засоби комунікацій та інформаційного обміну.

Виклад основного матеріалу. Одним з підходів, в дослідженні соціальних мереж, є моделювання. Зокрема для дослідження можуть використовуватись програмні моделі, в яких моделюють структуру частини соціальної мережі та інформаційні процеси, що протікають в часі. Програмна модель базується на певній математичній моделі та системі допущень і спрощень.

Створення моделі поширення інформаційно-психологічного впливу у сегменті соціальної мережі можна розбити на декілька етапів:

1. Вибір підходу до моделювання структури.
2. Представлення і формальний опис вузла.
3. Математична формалізація інформаційної взаємодії, математичний опис поведінкових стратегій.

Загалом структура мережі, з точки зору інформаційних зв’язків та інформаційного обміну, може розглядатися як граф. В якості вузлів графа виступають суб’єкти інформаційного обміну, а ребрами є наявні інформаційні зв’язки:

$$G(V, E), \tag{1}$$

де V – множина вузлів; E – множина ребер.

Для моделювання конкретних структур фрагменту мережі обрано наступні типи кластерів: група, кліка, лідерська група. Окрім цього варто зауважити, що при моделюванні розглядаємо лише сталі, двосторонні зв’язки. Тобто – якщо вузол $V_i \rightarrow V_j$, то і $V_j \rightarrow V_i$. Далі розглянемо самі кластери, на основі яких моделюється структура.

Група (**Г**) - граф з таким набором зв’язків, що дозволяє встановити зв’язок між будь-якими двома вузлами графу напряму або використовуючи проміжні вузли.

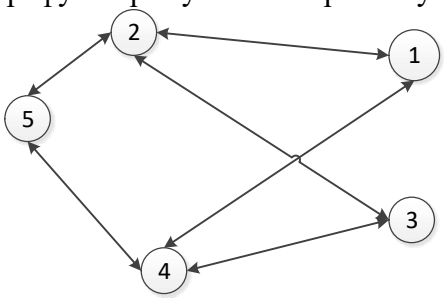

Рисунок 1 – Підмножина типу «Група»

Формальний опис такого кластеру може виглядати так:

$$G_{grupa} = \left(V_n \mid \forall V_i, V_j : i, j, k_i \le n \exists \left\{E_{ik1}, E_{k1,k2}, E_{k2,k3} .. E_{kn,j}\right\}\right), \tag{2}$$

Фактично група є зв’язним графом, матриця суміжності може мати різний вигляд (залежить від щільності зв’язків), а обов’язковою є умова зв’язності – існування шляху між будь-якими вибраними вершинами кластеру.

Кліка (**К**) – граф в якому кожен вузол зв’язаний з кожним, або, іншими словами – всі вершини графа суміжні.

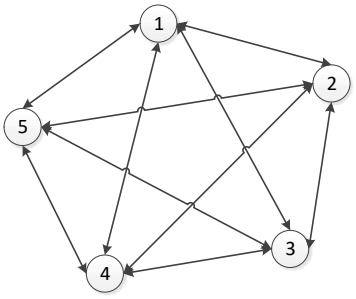

Рисунок 2 – Підмножина типу «Кліка»

Формальний опис кліки:

$$G_{clika} = \left(V_n \mid \forall V_i, V_j : i, j \le n \exists E_{ij}\right), \quad (3)$$

матриця суміжності для кліки буде мати вигляд:

i\j	1	2	3	…	n
1	0	1	1	1	1
2	1	0	1	1	1
3	1	1	0	1	1
…	1	1	1	0	1
n	1	1	1	1	0

Лідерська група (**ЛГ**) – підвид групи з одним або кількома вираженими вузлами, що мають зв'язки з усіма іншими вузлами групи.

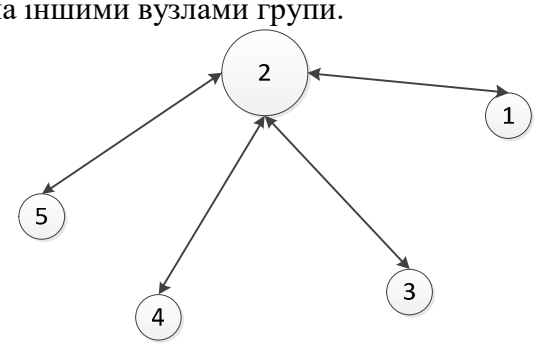

Рисунок 3 – Підмножина типу «Лідерська група»

Формальний опис лідерської групи:

$$G_{lid\_grup} = \left(V_n \mid \exists i \le n, \forall j \le n \exists E_{ij}\right), \quad (4)$$

Матриця суміжності для лідерської групи буде характеризуватись наявністю стовпчика та рядка повністю заповнених 1 (окрім діагонального елементу), матриця матиме вигляд:

i\j	1	**2**	3	…	n
1	0	1	***x***	***x***	***x***
2	1	0	1	1	1
3	***x***	1	0	***x***	***x***
…	***x***	1	***x***	0	***x***
n	***x***	1	***x***	***x***	0

Тут вузол з індексом 2 є лідером, елементи ***x*** в матриці суміжності означає, що інші вузли можуть мати і інші зв'язки, але вони не є обов'язковими для ідентифікації фрагменту мережі як кластера типу «лідерська група»

Задавання структури матрицею суміжності є досить ефективним способом, але для експериментів та візуального сприйняття структури доречним є реалізація в програмній моделі візуального конструктора, що базується на використанні набору базових кластерів з можливістю їх параметризації. Доречною функцією програмної моделі є також можливість внесення «ручних» коректив в структуру: додавання та вилучення вузлів/зв'язків.

Запропонований підхід до генерування структури мережі дозволяє генерувати сегменти мереж з досить різноманітною топологією, а можливість внесення коректив в ручному режимі забезпечує можливість локально змінити структуру та наблизити мережу в моделі до реальної структури мережі, що є об'єктом дослідження.

Запропонований підхід має свої переваги та недоліки.

Переваги:

1. Можливість частково автоматизованого генерування структур з різною топологією:
   - мережі внутрішньо корпоративних зв'язків;
   - мережі міжкорпоративних зв'язків;
   - замкнені мережі організацій;
   - ситуативні утворення (об'єднання людей спільною ідеєю, подією);
   - сегменти соціальних Інтернет мереж.
2. Наявність можливості редагування зв'язків дозволяє суттєво підвищити варіативність.
3. Можливість детального моделювання структури в мережі в околі досліджуваного вузла.

Недоліки:

1. Структура зв'язків і особливості внутрішньої будови кластерів носить випадковий характер.
2. Необхідність ручного регулювання за умови більш точного відтворення наявної структури.

Наявність випадковості в структурі мережі є відносним недоліком, в деяких випадках моделювання певний ступінь стохастичності є обов'язковою умовою. З іншого боку недолік може бути частково компенсований введенням параметрів при генеруванні базових кластерів.

Вузол мережі характеризується певним набором параметрів, що визначають його поведінку і поточній стан. При виборі параметрів – характеристик вузла необхідно намагатись мінімізувати їх кількість при цьому не втративши адекватності моделі, модель має давати наближені до реальності результати.

В моделі вузол описується наступними характеристиками:

$$V_i =< Av_i, Rv_i, O\alpha v_i, \{Vj_i\} >, \quad (5)$$

де (*A*) **Active** – активність користувача, кількість активних діалогів (звернень до інших користувачів) за одну ітерацію моделі.

(*R*) **Reputation** – репутація користувача, вплив інформаційного посилу, сила переконання.

(*O*) **Opposite** – інформаційний спротив, критичність по відношенню до ідеї, що розповсюджується.

(*I*) **Involvement** – ступінь залученості до ідеї, рівень довіри.

$\{Vj_i\}$ - множина контактів, вузлів з якими існує інформаційний обмін, вузла V_i.

Серед вузлів мережі виділимо окремі вузли – генератори ідеї. Дані вузли є активними вузлами і саме вони являються осередками розповсюдження інформаційного посилу. Модель розглядає розповсюдження ідеї конкретного змісту чи спрямування, далі будемо позначати її α-ідея. Модель може передбачати наявність генераторів контрідеї, позначимо її ($-\alpha$), тобто ідея протилежна до α.

Генератор формально описується так:

$$Gen_{\alpha i} =< Vi \mid Av_i \sim 1, I\alpha v_i = Ig >, \quad (6)$$

Тобто, генератори – вузли з високою активністю, ступінь залученості до α-ідеї максимальний. Всі генератори сегменту мережі утворюють множину генераторів - *Gen*

Основна ідея моделі полягає в формалізації поведінкових стратегій активних вузлів сегменту мережі. Вузол починає активну діяльність за умови його залученості до ідеї $I\alpha v_i > 0{,}5Ig$. Тут *Ig*– це залученість до ідеї рівня генератора. Величина даного параметра

визначається особливостями, метою та контекстом інформаційного впливу. Наприклад, існують дослідження (проводились на замовлення радіостанцій), що визначають необхідну кількість прослуховувань пісні аби вона відклалась в пам'яті слухача і стала популярною. Дослідження встановили, що після 8 прослуховувань пісні на протязі короткого періоду пересічний слухач запам'ятовує мелодію і починає підсвідомо підспівувати при перших акордах мелодії. Тобто в даному випадку, підспівуючи пісню, слухач фактично починає поширювати інформацію, а Ig=8.

Кількість інформаційних посилів вузлам з множини доступних вузлів (контакти V_i) за одну ітерацію моделі пропорційна активності вузла - $|\alpha_i| \sim Av_i$.

Процес інформаційного обміну в моделі можна представляти ітераційним процесом, де кожна окремо взята ітерація відповідає певному часовому дискрету (наприклад: 1 ітерація = 1 уявний день)

Розповсюдження інформаційної ідеї в мережі можна оцінювати за інтегральним критерієм, що визначається як:

$$I\alpha(G) = \sum_{i=1}^{n} I\alpha v_i \,. \tag{7}$$

Залученість до α-ідеї окремого вузла визначається за адитивним принцом. Показник залученості рівний сумі накопичених α-посилів на поточну ітерацію:

$$I\alpha v_j = \sum_{m=1}^{x} \sum_{i=1}^{n} kij * \alpha_i \,, \tag{8}$$

де $I\alpha v_j$ – рівень залученості j-го вузла до α-ідеї,

x – поточна ітерація моделювання,

n – кількість контактів j-го вузла,

α_i – повідомлення від і-го вузла, фіксує наявність повідомлення

$$\alpha_i = \begin{cases} 1, \alpha - \text{посил від } V_i \text{ був} \\ 0, \alpha - \text{посилу від } V_i \text{ не було} \end{cases}, \tag{9}$$

k_{ij} – коефіцієнт інформаційного впливу, що визначається співвідношенням (10):

$$ki_j = \frac{Rv_i}{o\alpha v_j} \tag{10}$$

У випадку наявності в мережі конргенераторів необхідно враховувати їх впливи і тоді формула (8) прийме вигляд:

$$I\alpha v_j = \sum_{m=1}^{x} \left(\sum_{i=1}^{n} kij * \alpha_i + \sum_{i=1}^{n} kij * (-\alpha_i) \right). \tag{11}$$

Більшість існуючих моделей для моделювання розповсюдження інформації та інформаційних впливів не розглядають поведінку окремих вузлів, хоча поведінка може мати суттєвий вплив на кінцевий результат та швидкість розповсюдження.

Перед суб'єктом, що виступає генератором в мережі, виникає задача вибору цілі для інформаційної атаки. Ціль інформаційної атаки обирається на основі поведінкової стратегії. Поведінкова стратегія генератора може бути представлена як:

$$\left\langle F(P_1 P_2 ... P_i) \middle| Vj_g \right\rangle, \tag{12}$$

де $F(P_1P_2…P_i)$ – функція, що визначає поведінкову стратегію;

Vj_g – множина доступних генератору вузлів, тобто – підмножина вузлів всієї мережі, що входить до кола спілкування генератора;

$P_1P_2…P_i$ – набір поведінкових критеріїв.

Серед поведінкових стратегій можна виділити окремі групи:

– стратегії без аналізу, що базуються на масовості інформаційних посилів в околі генератора;

– стратегії на основі аналізу показників доступних вузлів, базуються на виборі найбільш вразливого чи корисного (з точки зору подальшого розповсюдження інформації) вузла з множини доступних (аналіз вузлів в околі генератора);

– стратегії на основі аналізу структури чи положення вузла, базуються на аналізі структури в околі вузла або наявній інформації про ключове значення вузла (аналіз вузлів поза околом генератора).

В найпростішому випадку генератор обирає вузли для атаки випадковим чином. Тоді поведінкова стратегія (умовно назвемо її «кущ») може бути описана як:

$$P_{bush} = \left\{ u_i \in U_g \middle| i = random\left(\left|U_g\right|\right), \left|u\right| \le Act_g \right\}, \quad (13)$$

де $u_i \in U_g$ – доступні генератору користувачі;

$i = random\left(\left|U_g\right|\right)$ – випадковий вибір номера користувача для атаки;

$\left|u\right| \le Act_g$ – кількість обраних користувачів (кількість інформаційних посилів за одну ітерацію моделі) не перевищує показника активності генератора.

На відміну від простих стратегій можуть існувати й більш складні багатокритеріальні поведінкові стратегії. Ймовірним є той факт, що більш складна стратегія, яка використовує певний аналіз і вибір вузлів може показувати кращу ефективність. Але реалізація складних стратегій в реальній мережі вимагає певного аналізу, а відповідно і часу. Однією з цілей моделювання є проведення експерименту залежності ефективності різних поведінкових стратегій від структури сегменту мережі та початкового положення генератора в мережі.

Можливі і інші поведінки, коли цілі інформаційної атаки обираються не випадково, а з урахуванням певних характеристик. Найпростішою з точки зору аналізу та доступності характеристикою вузла для атаки є кількість його зв'язків (з точки зору соціальної мережі – кількість друзів). Логічно припустити, що вузли з великою кількістю контактів є більш перспективними для атаки і подальшого розповсюдження ідеї. У випадку вдалої атаки і переконання такого вузла канал передачі значно розширюється. Але в цьому випадку генератору необхідно затрачати певний час для аналізу – вибір вузла для атаки, відповідно кількість активних діалогів має бути зменшена по відношенню до поведінки описаної співвідношенням (13). Обравши перспективний вузол для атаки, генератор намагається залучити його до ідеї першочергово – тому зосереджує увагу саме на цьому вузлі (вузлах). В реальності така стратегія визначається повторюваністю звернень до одного вузла на протязі однієї ітерації. Кількість вузлів обраних для атаки наступними генераторами (залученими до ідеї) може збільшуватись, враховуючи збільшення носіїв ідеї в мережі і сумарний вплив на атакований вузол.

У випадку цієї поведінкової стратегії (назвемо її умовно «дерево»), вона може бути описана наступним чином:

$$P_{tree} = \left\{ u_i \in U_g \middle| \left|U_{ui}\right| \to \max, \left|u\right| = 2^{l\_g}, \left|u\right| \le K * Act_g, u_i \notin Gen \right\}, \quad (14)$$

де $u_i \in U_g$ – доступні генератору користувачі

$\left|U_{ui}\right| \to \max$ – кількість вузлів, доступних атакованому вузлу, обирається за ознакою «максимальна з наявних»

$\left|u\right| = 2^{l\_g}$ – кількість вузлів для атаки залежить від рівня генератора (l_g), починаючи від початкового генератора l_g = 0.

$|u| \le K * Act_g$ – кількість обраних користувачів не перевищує показника активності генератора з деяким коеф., певний час витрачається генератором на аналіз і пошук вузла для атаки.

$u_i \notin Gen$ – атака на вузол продовжується до тих пір поки вузол сам не стане генератором.

Особливості структури сегменту мережі та інші показники можуть вимагати вибору інших поведінкових стратегій. Наприклад – застосування поведінкової стратегії «дерево» з використанням в якості критерію показника кількості контактів потенційної цілі можуть призводити до колізій. Так обраний для атаки вузол може мати найбільшу кількість контактів, але водночас високий рівень інформаційного спротиву. В цьому випадку на залучення до ідеї даного вузла генератором буде витрачено багато часу, що в критичному випадку не призведе до очікуваного результату. Виходом з даної ситуації є зміна критерію вибору вузла, тоді поведінкова стратегія може бути описана як:

$$P_{tree} = \left\{ u_i \in U_g \,\middle|\, Op_{ui} \to \min, |u| = 2^{l-g}, |u| \le K * Act_g, u_i \notin G \right\}. \quad (15)$$

В порівнянні з (14) змінено лише критерій вибору вузла – обираються вузли з мінімальним рівнем спротиву.

Багатокритеріальні поведінкові стратегії природно повинні мати вищу ефективність, але виникає питання про баланс затраченого часу на аналіз критеріїв і приріст ефективності інформаційного впливу.

Висновки. Запропонована математична модель може використовуватись як базис для створення програмної моделі для проведення експериментів та отримання різного роду статистик. Основною перевагою запропонованої моделі є можливість дослідження впливу на розповсюдження інформації поведінки окремого вузла, чого не передбачають інші досліджені моделі. Окрім безпосередньо поведінкової стратегії активного вузла модель дозволяє проводити дослідження залежності розповсюдження інформації від початкового положення вузла та структури найближчого околу активного вузла-генератора.

Модель передбачає варіанти мережі з пасивним інформаційним спротивом, тобто коли в мережі відсутні генератори контр ідеї і мережі з активним інформаційним спротивом – в мережі наявні генератори протилежної за змістом ідеї (конрідея).

Цікаві результати можуть давати експерименти з дослідження протистояння генераторів ідеї та контрідеї, що діють відповідно до різних поведінкових стратегій.

Список літератури

1 Kermack, W.O., McKendrick, A.G. A Contribution to the Mathematical Theory of Epidemics // Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences. 115 (772): 700, 1927.

2 Daley D.J., Kendall D.G. Stochastic rumors // J. Inst. ath. Appl, 1965, Vol. 142, pp.42-55.

3 John Von Neumann J., Burks A.W. Theory of Self-Reproducing Automata;University of Illinois, Urbana and London, 1966, pp. 297-302.

4 Горковенко Д.К. Сравнительный анализ моделей эпидемии и клеточного автомата при моделировании распространения информации в социальных сетях / Д.К. Горковенко // Научно-технические ведомости СПбГПУ. – 2017. –Т. 10, № 3. – С.103-113. doi: 10.18721/jcstcs.10309

5 Губанов Д.А. Обзор онлайновых систем репутации/доверия [Текст] / Д.А. Губанов // Интернет-конференция по проблемам управления. – М.: ИПУ РАН, 2009. – 25 с.

6 Суслова В.А. Методы моделирования социальных сетей [Электронный ресурс] / В.А. Суслова, А.А. Городов // Решетневские чтения. – 2015. – №19. – С. 133-134. – Режим доступа: http://cyberleninka.ru/article/n/metody-modelirovaniya-sotsialnyh-setey.

7 Губанов Д.А. Модели влияния в социальных сетях [Электронный ресурс] / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили // УБС. – 2009. – №27. 205-281– Режим доступа: http://cyberleninka.ru/article/n/modeli-vliyaniya-v-sotsialnyh-setyah

8 Грайворонська А.М., Ланде Д.В. Дослідження інформаційних потоків як динамічних мультиагентних систем // Системний аналіз та інформаційні технології: матеріали міжнародної науково-технічної конференції SAIT 2015, Київ – К.: УНК «ИПСА» НТУУ «КПИ», 2015. – С. 62-63.

9 Ланде Д.В. Мультиагентна модель розповсюдження інформації в соціальній мережі [Текст] / Д.В. Ланде, А.М. Грайворонська, Б.А. Березін // Реєстрація, зберігання і обробка даних. – 2016. – Т.18, №1. – С. 70-77.

References

1. Kermack, W.O. & McKendrick, A.G. (1927). A Contribution to the Mathematical Theory of Epidemics . Proceed- ings of the Royal Society A*: Mathematical, Physical and Engineering Sciences* (*115 (772): 700)*
2. Daley, D.J. & Kendall, D.G. (1965). Stochastic rumors. *J. Inst. ath. Appl*, *Vol. 142,* 42-55 .
3. John Von Neumann J., Burks A.W. (1966). *Theory of Self-Reproducing Automata*. University of Illinois, Urbana and London.
4. Gorkovenko, D.K. (2017). Sravnitel'nyj analiz modelej jepidemii i kletochnogo avtomata pri modelirovanii rasprostranenija informacii v social'nyh setjah [Comparison of epidemic models and cellular automata in modeling of diffusion of information in socal]. *Nauchno-tehnicheskie vedomosti SPbGPU* – Scientific and technical statements SPbGPU, *Vol.10, 3*, 103-113. doi: 10.18721/jcstcs.10309
5. Gubanov, D.A. (2009). Obzor onlajnovyh sistem reputacii/doverija [Review of online reputation / trust systems]. Management problems: *Internet-konferencija – Internat Conference* (25 p.). Moscow: IPU RAN.
6. Suslova, V.A. & Gorodov, A.A. (2015). Metody modelirovanija social'nyh setej [Methods of modeling social networks]. *Reshetnevskie chtenija – Reshetnev readings*, *19*. 133-134. Retrieved from http://cyberleninka.ru/article/n/metody-modelirovaniya-sotsialnyh-setey.
7. Gubanov, D.A., Novikov, D.A. & Chhartishvili, A.G. (2009). Modeli vlijanija v social'nyh setjah [Models of influence in social networks]. *UBS – UBS*, *27*. 205-281. Retrieved from http://cyberleninka.ru/article/n/modeli-vliyaniya-v-sotsialnyh-setyah
8. Hrajvorons'ka, A.M. & Lande, D.V. (2015). Doslidzhennia informatsijnykh potokiv iak dynamichnykh mul'tyahentnykh system [Investigation of information flows as dynamic multi-agent systems].System analysis and information technology ’15. *Mizhnarodna naukovo-tekhnichna konferentsia – International Scientific and Technical Conference* (pp.62-63). Kyiv: UNK «YPSA» NTUU «KPY».
9. Lande, D.V., Hrajvorons'ka, A.M. & Berezin, B.A. (2016). *Mul'tyahentna model' rozpovsiudzhennia* informatsii v sotsial'nij merezhi [A multi-agent model of information dissemination in social networks]. *Reiestratsiia, zberihannia i obrobka danykh – Registration, storage and processing of data*, Vol.*18*, *1,* 70-77 .

Ulichev Oleksandr, postgraduate
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Mathematical Model of Dissemination of Informational and Psychological Influences in the Social Network Segment

The purpose of the article is to describe the results of research in the direction of modeling the processes of disseminating information influences in the social network segment. The basis of the research is the proposed mathematical model and approaches to the implementation of individual stages of simulation on the basis of the proposed MM in the programmatic form. In particular, there are 3 main stages: modeling the structure of the network, formal description of the network node, implementation of the process of disseminating information.

The method for generating a network structure is based on the use of parametric clusters of three types: a click, a group, a leader group. This approach allows you to model a wide range of network segments that are diverse in topology. The network node that simulates the state of the subject in the network is proposed to represent as a class with a fixed set of fields, types of fields and their purpose is justified in the text of the article. The process of dissemination of information is proposed to represent an iterative process in which nodes carry out information impacts on other nodes through the dissemination of information messages. The article proposes the concept of behavioral strategies that determine the criteria for selecting a node for an attack. But there are a few examples of possible behavioral strategies. In the text of the article the key points of the program implementation are described, a diagram of the main classes of the program is presented. The series of

experiments were conducted on the program model, the results of which show the adequacy of the model's response to changes in the parameters of individual nodes and network structure.

The article presents the results of experiments: the dependence of the rate of propagation on the density of links, the comparison of selected behavioral strategies, the evaluation of the effectiveness of strategies, depending on the number of nodes-generator links.

software model, information influence, methods of network generation, models of distribution of information in the network, behavioral strategies

Одержано (Received) 07.06.2016

УДК 004.056.5

В.Д. Хох, асп.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна, E-mail: vd.khokh@gmail.com

Автоматизована система проведення аудиту інформаційної безпеки комп'ютерних систем та мереж

У статті розглядається розроблювана в рамках дисертаційного дослідження система для проведення аудиту інформаційної безпеки комп'ютерних систем та мереж. Пропонується вирішення проблем, що виникли під час розробки системи та розглянуто механізми, що було розроблено та інтегровано у розроблювану систему.

інформаційна безпека, аудит, нечітка логіка, експертні системи, автоматизація

В.Д. Хох, асп.
Центральноукраинский национальный технический университет, г. Кропивницкий, Украина

Автоматизированная система проведения аудита информационной безопасности компьютерных систем и сетей

В статье рассматривается разрабатываемая в рамках диссертационного исследования система для проведения аудита информационной безопасности компьютерных систем и сетей. Предлагается решение проблем, возникших при разработке системы и рассмотрены механизмы, которые были разработаны и интегрированы в разрабатываемую систему.

информационная безопасность, аудит, нечеткая логика, экспертные системы, автоматизация

Постановка проблеми. Ситуація, що склалася в нашій країні з початком агресії Російської Федерації, загострює проблему захисту інформаційних систем, оскільки у РФ є великий досвід у проведені різноманітних операцій із залученням спеціалістів з комп'ютерної та інформаційної безпеки. Наприклад, під час загострення відносин Естонії та РФ у 2007 році на фоні конфлікту, спричиненого переносом пам'ятника «Бронзовий Солдат», було виведено з ладу багато урядових сайтів Естонії, а також деяких банківських установ. Експерти, у тому числі і з ООН відмітили, що це була найбільш організована та добре спланована кібератака [1]. І хоча доказів того, що атака була організована саме РФ, Естонія не змогла надати, згодом, того ж року депутат Державної думи Росії Сергій Марков визнав на прес-конференції, що один з його помічників є організатором цієї атаки [1]. Вже через рік РФ продемонструвала