МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

УЛІЧЕВ ОЛЕКСАНДР СЕРГІЙОВИЧ

УДК 004.773.2+004.942

МОДЕЛЬ ТА МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

21.05.01 – «Інформаційна безпека держави»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана на кафедрі кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
Мелешко Єлизавета Владиславівна,
Центральноукраїнський національний технічний університет,
доцент кафедри кібербезпеки та програмного забезпечення.

Офіційні опоненти: доктор технічних наук, професор
Євсеєв Сергій Петрович,
Харківський національний економічний університет імені Семена Кузнеця,
професор кафедри кібербезпеки та інформаційних технологій.

доктор технічних наук, професор
Молодецька Катерина Валеріївна,
Поліський національний університет,
професор кафедри комп'ютерних технологій і моделювання систем.

Захист відбудеться 13 травня 2021 р. о 15.00 на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, пр. Любомира Гузара 1, ауд. 11.111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Любомира Гузара 1.

Автореферат розісланий «__» квітня 2021 р.

Учений секретар
спеціалізованої вченої ради
к.т.н., професор Є. Іванченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Соціальні мережі (СМ) 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. У той же час СМ стали зручним середовищем для поширення інформаційних впливів (ІВ) та маніпулювання суспільною думкою, що викликає загрози як для окремих користувачів, так і для суспільства і держави в цілому. У сучасному світі однією з головних загроз інформаційній безпеці держави є саме ІВ через засоби масової інформації, соціальні медіа, тощо.

З точки зору стрімкої глобалізації інформаційних процесів, входження України до світового інформаційного простору та інформаційної експансії з боку інших держав важливим є розробка методологічних основ забезпечення інформаційної безпеки держави (ІБД). Одними з найважливіших завдань забезпечення ІБД є запобігання негативним ІВ на індивідуальну, групову та суспільну свідомість, захист від ворожої пропаганди, створення технологій дослідження, захисту та контрзахисту від негативних наслідків ІВ.

Сучасні наукові роботи, спрямовані на дослідження ІВ в умовах інформаційного протиборства (роботи науковців В. Горбулін, А. Пую, О. Додонов, В. Хорошко, Г. Почепцов, С. Розторгуєв, Р. Грищук, К. Молодецька) розглядають два напрямки:

– методи нападу: формування, поширення та використання ІВ.

– методи протидії: виявлення, прогнозування наслідків та захист від ІВ.

Оскільки СМ є одним з каналів поширення ІВ, актуальною є задача дослідження процесу поширення таких впливів в СМ для розробки методів прогнозування наслідків та методів захисту. Дослідження інформаційних атак на СМ шляхом їх моделювання дозволить розробити і реалізувати превентивні та контрзаходи для запобігання негативним ПІВ на індивідуальну, групову та суспільну свідомість, захист від ворожої або недружньої пропаганди. Також, це дозволить розробити науково-методичні засади і технології захисту людини, суспільства й держави від негативних наслідків ІВ.

Для аналізу процесів поширення та наслідків ІВ у соціальних мережах у існуючих наукових роботах пропонуються та досліджуються наступні методи:

– збір та аналіз даних з відкритих частин веб-ресурсів СМ (роботи науковців Д. Ланде, Р. Гумінський, Т. Батура, Є. Князєва Є., Б. Хоган).

– математичне та програмне імітаційне моделювання соціальних мереж (роботи науковців А. Барабаши, Р. Альберт, Б. Боллобаш, О. Ріордан, П. Ердьош, А. Реньї, П. Баклі, Д. Остхус, Дж. Чаес, К. Боргс, М. Грановветер, Д. Губанов, А. Чхартишвили, Д. Горковенко, І. Гончаров, Б. Торопов, Д. Ланде).

Сучасні СМ використовують різні методи протидії парсингу інформації з їх веб-ресурсів, зокрема, зростає об’єм закритої частини інформації, а на збір відкритої інформації створюють значні часові затримки, тому все актуальнішою стає друга група методів. Імітаційні моделі СМ дозволяють проводити дослідження процесів, що у них протікають, без значних часових та фінансових затрат та без доступу до даних, які відкриті тільки власникам веб-ресурсів. Проведений аналіз

показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла СМ (вузол – користувач СМ), а саме стратегію поширення інформації, яку обирає вузол в процесі ІВ тощо. З огляду на зазначене, розроблення методів і засобів моделювання та реалізації різних стратегій поширення ІВ у сегментах СМ є *актуальною науково-технічною задачею*, що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у межах пріоритетних наукових напрямів, які охоплюють актуальні проблеми, відповідно до рішення Ради президентів академій наук України від 30 січня 2019 року «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019-2023 роки», «Інформатика» за темою: «Розроблення обчислювальних алгоритмів і процедур з метою вирішення практичних задач міждисциплінарного характеру для застосувань, що належать до науково-технічної та соціально-економічної сфер діяльності людини», «Наукова інформація» за темою: «Соціальні мережі, формування в Україні інформаційного суспільства». Дисертаційну роботу виконано у межах зареєстрованих НДР Центральноукраїнського національного технічного університету: «Моделювання та аналіз складних мереж та інформаційних систем» (№ д.р. 0119U003587), «Методи використання інформаційних технологій та інтелектуальних систем для аналізу даних та забезпечення інформаційної безпеки суспільства» (№ д.р. 0116U008161) та «Методи підвищення оперативності передачі даних та захисту інформації у телекомунікаційній мережі» (№ д.р. 0112U006631).

Мета і задачі дослідження. Мета дисертаційної роботи – підвищення швидкості поширення інформаційних впливів у соціальних мережах за рахунок оптимального вибору об'єктів впливу.

Мета дисертаційної роботи визначає необхідність розв'язання таких **основних задач:**

1. Дослідити методи генерації мереж і моделі поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства.
2. Розробити математичну модель поширення інформаційних впливів в сегменті соціальної мережі з врахуванням особистісних характеристик вузлів мережі, що дає можливість, на основі аналізу запропонованих характеристик, застосувати різні поведінкові стратегії суб'єктами інформаційного впливу.
3. Удосконалити метод генерації сегменту соціальної мережі з можливістю моделювання різних варіантів структури сегменту мережі за рахунок обрання різної кількості та різних типів кластерів соціальної мережі.
4. Удосконалити метод оптимального вибору цільових вузлів соціальної мережі суб'єктами поширення інформаційного впливу під час інформаційного протиборства, а також метод вибору поведінкових стратегій суб'єктів впливу на основі наявної про мережу інформації.
5. Провести експериментальне дослідження програмної моделі, що підтверджує ефективність запропонованих методів, з точки зору швидкості поширення інформаційних впливів в сегменті соціальної мережі.

Об'єктом дослідження є процес поширення інформаційних впливів у

сегменті соціальної мережі.

Предметом дослідження є методи моделювання соціальних мереж та моделі поширення у них інформаційних впливів в умовах інформаційного протиборства.

Методи дослідження. Для вирішення завдань математичного моделювання структури соціальної мережі та процесів поширення інформаційних впливів використано теорію графів, теорію складних мереж, теорію множин. Для створення програмної моделі на основі розробленої математичної моделі використано методи об'єктно-орієнтованого програмування, методи візуалізації графів та алгоритми роботи з графами. Для моделювання об'єктів та суб'єктів впливу в соціальних мережах, їх характеристик та стратегій поведінки використовувалися основи соціальної психології, теорія інформаційних протиборств.

Наукова новизна одержаних результатів полягає в наступному:

– *вперше розроблено* математичну модель поширення інформаційних впливів у сегменті соціальної мережі, яка за рахунок параметризації особистісних характеристик вузлів мережі, а саме – введення параметрів вузла: активність, репутація, залученість до ідеї, інформаційний спротив, дає можливість застосування різних поведінкових стратегій суб'єктами інформаційного впливу на основі аналізу параметрів атакованих вузлів;

– *удосконалено* метод генерації структури сегменту соціальної мережі, який за рахунок комбінування структури мережі з набору параметризованих кластерів і вибору їх топологічних особливостей, дозволяє генерувати мережу з наперед заданою структурою;

– *набув подальшого розвитку* метод поширення інформаційних впливів у сегменті соціальної мережі під час інформаційного протиборства, який відрізняється від існуючих застосуванням методу аналізу ієрархій для здійснення оптимального вибору цільового вузла мережі, а також застосуванням та вибором різних поведінкових стратегій суб'єктом інформаційного впливу на основі наявної інформації про мережу, що дозволяє за меншу кількість часу поширити інформаційний вплив серед вузлів соціальної мережі за рахунок вибору оптимальних початкового цільового вузла та стратегії поширення інформації.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати дають змогу здійснити програмне імітаційне моделювання процесу поширення інформаційних впливів у сегменті соціальної мережі та вибір поведінкових стратегій суб'єкту впливу під час інформаційного протиборства.

Практична цінність роботи полягає у наступному:

– розроблено алгоритми генерації структури сегментів соціальної мережі, що дають можливість моделювати сегмент мережі з наперед заданою структурою зв'язків, розроблено програмну імітаційну модель поширення інформаційних впливів у сегменті соціальної мережі під час інформаційного протиборства та алгоритми моделювання і вибору різних поведінкових стратегій суб'єктів впливу, що дозволяє аналізувати та прогнозувати поширення інформаційних впливів у соціальних мережах з використанням різних поведінкових стратегій;

– застосування поведінкових стратегій суб'єктів інформаційних впливів на

основі аналізу даних про мережу дозволяє підвищити швидкість поширення інформації в середньому на 70% в порівнянні з випадковим вибором вузлів для атаки. Швидкість поширення ІВ через вузли, обрані за запропонованим методом, в середньому на 16% вища, ніж швидкість поширення через інші вузли, що мають виграшні структурні позиції. В порівнянні з запропонованим іншими авторами методом поширення інформаційних впливів через «лідера думок» приріст швидкості поширення інформаційних впливів через вузол вибраний за адаптованим МАІ склав 6%.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження. Результати дисертації впроваджені і використовуються в організації ТОВ «Сайфер БІС», що розробляє програмні системи захисту інформації, а також використано у навчальному процесі Центральноукраїнського національного технічного університету для покращення викладання дисциплін «Інформаційна безпека держави», «Спеціальні розділи математики для інформаційної безпеки» та «Прогнозування та моделювання в соціальній сфері», що підтверджено відповідними актами.

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співавторстві, здобувачеві належать: [1] – дослідження методів поширення інформації у СМ з точки зору інформаційної безпеки держави; [12] – математична модель поширення ІВ у сегменті СМ; [4-6, 11, 10, 13-15] – програмна модель поширення ІВ у сегменті СМ з різними стратегіями поведінки суб'єктів ІВ; [7, 17, 18] – дослідження впливу інформаційних атак на соціально-інформаційні системи; [8] – дослідження різних видів інформаційних атак на соціально-інформаційні системи; [9] – метод вибору цільового вузла суб'єктом ІВ СМ під час інформаційних протиборств; [16] – дослідження моделей складних мереж.

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях: Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» (Кропивницький, 2017-2018 рр.); Міжнародний науково-практичний семінар «Комбінаторні конфігурації та їх застосування» (Кропивницький, 2018 р.); Міжнародна науково-технічна конференція «ITSEC» (Київ, 2018 р.); Міжнародна наукова конференція "Інформація. Комунікація. Суспільство" (Львів, 2018 р.); Всеукраїнська науково-практична конференція «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2018)» (Миколаїв-Коблево, 2018 р.); Міжнародна науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем» (Дніпро, 2019 р.); Всеукраїнська науково-практична Інтернет-конференція «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» (Кропивницький, 2019 р.).

Результати дисертаційних досліджень регулярно доповідалися на наукових семінарах кафедри кібербезпеки та програмного забезпечення

Центральноукраїнського національного технічного університету.

Публікації. Основні положення дисертації опубліковано у 19 наукових працях, у тому числі: 10 наукових статтях (з яких 2 – у закордонних рецензованих наукових виданнях, 2 – у виданнях проіндексованих у Scopus, 6 – у вітчизняних фахових наукових журналах), а також 9 матеріалах та тезах доповідей наукових конференцій.

Структура роботи та її обсяг. Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 143 сторінки основного тексту, 51 рисунків, 14 таблиць, 12 сторінок додатків. Список використаних джерел містить 115 найменувань і займає 13 сторінок. Загальний обсяг роботи 170 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і задачі досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведено аналіз наукової літератури за темою дисертаційної роботи. Показано, що сьогодні СМ стали потужним інструментом ІВ. При цьому ІВ можуть носити як конструктивний так і деструктивний характер. Мета інформаційних атак може бути абсолютно різною: від рекламних кампаній до політичної боротьби та інформаційної війни. Показано актуальність розробки моделей та методів аналізу СМ та процесів поширення ІВ у них.

Аналіз існуючих моделей інформаційного поширення ІВ показує, що вони не враховують ряд важливих показників та критеріїв. Як можна бачити в табл. 1, більшість з розглянутих моделей не враховує таких характеристик як активність користувача і його поведінкову стратегію. У той же час дослідження в реальних СМ, дослідження в області маркетингу та реклами показують, що ефективність істотно залежить від структурного розташування вузла, його поведінки і особистісних характеристик.

Таблиця 1

Порівняння існуючих моделей поширення ІВ

Модель	**К1**	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**	**К8**	**К9**
Модель Грановветера	+	+	+	–	–	+	–	–	–
Модель Торопова	+	+/–	–	+	–	+	–	–	–
Модель Гончарова-Сироти	+	+	+	–	–	+	–	+/–	–
Модель Ланде	+	–	–	+	–	–	–	+	+/–
Модель Губанова	+	+	+/–	+/–	–	+	+/–	–	+/–

У табл. 1 використано наступні позначення: К1 – зміна думки під впливом оточуючих агентів; К2 – вплив структурних особливостей околу агента, і структури мережі в цілому; К3 – різний ступінь схильності агентів до ІС; К4 – наявність імовірнісних параметрів; К5 – врахування активності агента; К6 – оптимізація ІВ; К7 – поведінкові стратегії агентів (ігрова взаємодія); К8 – оцінка ймовірності певного результату і розподіл агентів в певний момент часу; К9 – параметризація особистісних якостей агента.

Проаналізовано ряд запропонованих методів генерації структури мережі, виявлені недоліки представлено в табл. 2.

Таблиця 2

Порівняння існуючих методів генерації структури мережі

Методи	К1	К2	К3	К4	К5	К6	К7
Метод Ердьоша-Реньї	+/–	–	+/–	–	–	–	+/–
Метод Уоттса-Строгатца	+	–	+	+	–	–	–
Метод Барабаши-Альберта	+	+	+	–	–	–	+
Метод Боллобаша-Ріордана	+	+	+	–	–	–	+
Метод Баклі-Остхуса	+	+	+	–	–	–	+
Метод Чаес-Боргса	+	+	+	–	–	–	–

У табл. 2 застосовано позначення: К1 – малий діаметр графу, К2 – рівень ассортативності, К3 – зв'язність графу, К4 – високий рівень кластеризації, К5 – топологія мережі обирається (наперед заданий набір кластерів), К6 – моделювання околу окремого вузла, К7 – можливість неоднорідного розподілу щільності зав'язків

В запропонованих методах виявлено наступні недоліки: низький рівень кластеризації, неможливість наперед визначити структуру мережі. Виходячи з чого, запропоновані методи не можуть бути застосовані в випадку генерації сегменту мережі з наперед заданою структурою зв'язків.

Створення нових та інтеграція вже створених методів і моделей аналізу СМ становить інтерес для дослідження процесів ІВ. Аналіз СМ та процесів поширення інформації у них шляхом програмного моделювання дозволяє проводити оцінку наслідків ІВ на веб-ресурсах. І чим більш наближена модель до реальних процесів у СМ і більш деталізована, тим точніше можна оцінити та спрогнозувати результати ІВ на користувачів реального веб-ресурсу.

Результати програмного імітаційного моделювання ІВ в СМ можна використати як в задачах нападу (пошук вразливості СМ для атаки, підбір оптимальної стратегії поширення ІВ), так і в задачах захисту (пошук вразливості СМ для їх усунення, аналіз можливих наслідків дій супротивника, підбір оптимальної стратегії поширення контрпропаганди).

Таким чином, у першому розділі, на основі проведеного аналізу, визначено і обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення поставленої мети.

Другий розділ присвячений дослідженню структурних властивостей СМ, розробці математичної моделі поширення ІВ у сегменті СМ та розробці методу генерації структури сегменту СМ.

Запропоновано наступну математичну модель:

$$\mathrm{INV}\,(\mathrm{G}, \{\mathrm{Gen}\}, \mathrm{F}_{\mathrm{Interaction}}(t), < F(P_1 P_2 P_3 .. P_4) | V_i \epsilon G >) \rightarrow max, \qquad (1)$$

за умов:

$t \leq T$ – час поширення менше часу актуальності інформаційного посилу;

$\{Gen\} \notin \emptyset$ – не порожня множина генераторів ідеї на 1 ітерації процесу;

де G – граф,що описує сегмент мережі;

$\{\mathrm{Gen}\}$ – множина початкових генераторів;

$\mathrm{F}_{\mathrm{Interaction}}(t)$ – функція інформаційної взаємодії;

$< F(P_1P_2P_3..P_4)|V_i \epsilon G >$ – вибір цільових вузлів для інформаційної атаки, на основі поведінкової стратегії генератора;

T – час актуальності інформаційного посилу.

Математична модель поширення ІВ в сегменті СМ реалізується за допомогою таких дій:

1. Представлення вузла (користувача) соціальної мережі в моделі

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

В моделі вузол (користувач СМ) описується наступним кортежом:

$$V_i =< Act_{v_i},\ R_{v_i},\ Op_{v_i},\ I_{v_i}, \{Vj_i\} >, \quad (2)$$

де Act_{v_i} (Active) – активність користувача, кількість активних діалогів (звернень до інших користувачів) за одну ітерацію моделі; R_{v_i} (Reputation) – репутація користувача, вплив інформаційного посилу, сила переконання; Op_{v_i} (Opposite) – інформаційний спротив, критичність по відношенню до ідеї, що поширюється; I_{v_i} (Involvement) – ступінь залученості до ідеї, рівень довіри; $\{Vj_i\}$ – множина контактів, вузли з якими існує інформаційний обмін, вузла V_i.

Серед вузлів мережі виділимо окремі вузли – *генератори ідеї* (суб'єкти атаки). Дані вузли є активними вузлами і саме вони являються осередками поширення інформаційного посилу. Модель розглядає поширення ідеї конкретного змісту, далі будемо позначати її α-ідея.

Генератор ідеї (суб'єкт впливу) формально описується так:

$$Gen_i =< V_i, |\ Act_{v_i} \sim 1,\ I_{v_i} =\ I_g >, \quad (3)$$

де I_g – це залученість до ідеї рівня генератора (суб'єкта впливу).

Генератори (суб'єкти впливу) – вузли з високою активністю, ступінь залученості до α-ідеї максимальний. Всі генератори сегменту СМ (ССМ) утворюють множину генераторів – $\{Gen\}$. Основна ідея моделі полягає в формалізації поведінкових стратегій суб'єктів впливу. Під поведінковою стратегією розуміється набір правил для вибору цільових вузлів - об'єктів атаки. Вузол починає активну діяльність за умови його залученості до ідеї $I_{v_i} > 0{,}5\, I_g$. Кількість інформаційних посилів вузлам з множини доступних вузлів (контакти V_i) за одну ітерацію моделі пропорційна активності вузла - $|\alpha_i| \sim Act_{v_i}$.

2. Імітаційне моделювання процесу інформаційного обміну

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

Поширення ІВ в СМ оцінювався за наступним інтегральним критерієм:

$$I_{\text{ССМ}}(G) = \sum_{i=1}^{n} I_{v_i}. \quad (4)$$

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

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

де I_{v_j} – рівень залученості j-го вузла до α-ідеї, x – поточна ітерація програмного імітаційного моделювання, n – кількість контактів j-го вузла, α_{im} – повідомлення від i-го вузла на ітерації m, фіксує наявність повідомлення значення параметра визначається як:

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

де k_{ij} – коефіцієнт ІВ, що визначається співвідношенням (7):

$$k_{ij} = \frac{Rv_i}{Op_{v_j}}. \quad (7)$$

Поведінка і залученість до ідеї визначається параметром I_{v_j}, при перевищенні певного порогового значення вузол вважається залученим до ідеї.

На кожній ітерації приріст залученості вузла до ідеї визначається коефіцієнтом (7).

Також, у цьому розділі розроблений *метод генерації структури сегменту СМ з заданою кількістю і типами кластерів*, що базується на комбінуванні структури мережі з набору параметризованих кластерів. Під кластерами маються на увазі ділянки СМ з визначеною щільністю зв'язків та певними особливостями їх структури, напр., група, лідерська група, кліка. Група – граф, де є зв'язок між будь-якими двома вузлами напряму або через проміжні вузли. Лідерська група має один або декілька вузлів, що мають зв'язки з усіма іншими вузлами групи. У клікі всі вершини суміжні.

Вхідні параметри методу: кількість кластерів в сегменті, типи кластерів, кількість вузлів в відповідному кластері. Вихідні результати: структура сегменту мережі.

Розроблений метод передбачає декілька етапів:

1 Етап. Створення списку вузлів кластера (визначення їх індивідуальних характеристик) та додавання їх до загального масиву вузлів мережі;

2 Етап. Генерація структури (створення зв'язків між вузлами) відповідно до обраного типу кластеру – ділянок СМ з певною структурою (група, кліка і т.д.);

3 Етап. Внесення змін до матриці суміжності;

4 Етап. Створення масиву точок для візуалізації структури графу соціальної мережі.

Етапи 1-4 повторюються поки структура СМ не буде повністю згенеровано.

Отже, розроблений метод генерації графу сегменту СМ, дозволяє обирати необхідну кількість і типи кластерів соціальної мережі, що дозволяє генерувати мережу заданої структури.

У **третьому розділі** наведено розроблення методу програмного імітаційного моделювання процесу поширення ІВ в сегменті СМ на основі запропонованих базових поведінкових стратегій вузла СМ та методу вибору цільового вузла суб'єктом інформаційних впливів СМ під час інформаційних протиборств на основі методу аналізу ієрархій.

Поведінкові стратегії (ПС) у розроблюваній моделі – набір правил для вибору суб'єктом впливу множини об'єктів впливу на основі їх особистісних характеристик.

Запропонований метод моделювання процесу поширення ІВ реалізується на основі *базових поведінкових стратегій вузла соціальної мережі.*

Поведінкова стратегія генератора (суб'єкта впливу) може бути представлена як:

$$F\left(P_1P_2 \dots P_i, \{Vj_g\}\right) = \{v_1, v_2 \dots v_n\}, \quad (8)$$

де $F(P_1P_2 \dots P_i)$ – функція, що визначає спосіб вибору об'єктів атаки; Vj_g– множина доступних генератору вузлів СМ для інформаційного впливу; $P_1P_2 \dots P_i$ – набір правил вибору об'єктів атаки; $\{v\}$ – множина вибраних для атаки вузлів ($\{v\} \subset \{Vj_g\}$).

Модель передбачає, що у випадку залучення вузла до ідеї він успадковує від суб'єкта впливу і стратегію. Тобто, якщо в мережі наявний генератор α- ідеї, що діє за стратегією $F1\left(P_1P_2 \dots P_i, \{Vj_g\}\right)$, то всі вузли залучені генератором ідеї діятимуть за стратегією $F1\left(P_1P_2 \dots P_i, \{Vj_g\}\right)$.

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

$$P_{bush} = \left\{u_i \in U_g \middle| i = random\left(\left|U_g\right|\right), |u| \le Act_g\right\}, \quad (9)$$

де $u_i \in U_g$ – доступні генератору користувачі; $i = random\left(\left|U_g\right|\right)$ – випадковий вибір номера користувача для атаки; $|u| \le Act_g$ – кількість інформаційних посилів за одну ітерацію моделі не перевищує показника активності генератора.

Така стратегія не вимагає жодного аналізу, і саме в цьому є її перевага – час, що було заощаджений на аналізі, може бути використано для атак. Тобто дана стратегія опирається на масовість атак за одиницю часу. Можливі і інші поведінкові стратегії, коли цільові вузли поширення ІВ обираються з урахуванням аналізу певних характеристик.

Поведінкова стратегія «дерево». Найпростішою з точки зору аналізу та доступності характеристикою вузла для атаки є кількість його зв'язків. Обравши вразливий до атаки вузол, генератор намагається залучити його до ідеї першочергово – тому зосереджує увагу саме на цьому вузлу (вузлах). Кількість вузлів обраних для атаки і кількість впливів на окремий вузол може збільшуватися, враховуючи збільшення суб'єктів впливу в СМ на нових ітераціях програмної моделі після вдалих ІВ. Дана ПС (назвемо її умовно «дерево») може бути описана наступним чином:

$$P_{tree} = \left\{u_i \in U_g \middle| \left|U_{u_i}\right| \to max, |u| = 2^{l\_g}, |u| \le K * Act_g, u_i \notin Gen\right\}, \quad (10)$$

де $u_i \in U_g$ – доступні генератору користувачі; $\left|U_{u_i}\right| \to max$ – кількість вузлів, доступних атакованому вузлу, обирається за ознакою «максимальна з наявних»; $|u| = 2^{l\_g}$ – 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 коефіцієнтом, певний час витрачається генератором на аналіз і пошук вузла для атаки. Для урівноваження стратегій без аналізу, і стратегій, що використовують аналіз, встановимо К=0,5; $u_i \notin Gen$ – атака на вузол продовжується до тих пір поки вузол сам не стане генератором. Фактично дана стратегія орієнтована на побудову

підмережі поширення інформаційного впливу з якомога більш швидким залученням до процесу поширення вузлів з найбільшою кількістю контактів.

Особливості структури сегменту СМ та інші показники можуть вимагати вибору інших ПС. Напр., 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 вузла до ІВ. В цьому випадку на залучення до ідеї даного вузла суб'єктом впливу буде витрачено багато часу, що в критичному випадку не призведе до очікуваного результату. Виходом з даної ситуації є зміна критерію вибору об'єктів атаки, тоді ПС може бути описана як:

$$P_{tree} = \left\{u_i \in U_g \middle| Op_{u_i} \to min, |u| = 2^{l\_g}, |u| \le K * Act_g, u_i \notin G\right\}. \quad (11)$$

В порівнянні з (10) змінено лише критерій вибору вузла – обираються вузли з мінімальним рівнем спротиву до інформаційних впливів.

Атака за цією стратегією орієнтована на кількість. Дана стратегія гарантує більш швидке залучення вузлів в підмережу, але кінцевий результат (залучення всієї мережі) може бути ускладнений. Напр., за наявності контргенератора, що залучить вибрані вузли з високим рівнем репутації, може настати переломний момент коли якість (вузли з високим рівнем репутації) стануть переважати кількість (кількість залучених вузлів велика, але їх сумарний ІВ досить низький). Багатокритеріальні ПС природно повинні мати вищу ефективність, але виникає питання про баланс затраченого часу на аналіз критеріїв і приріст ефективності ІВ.

Крім того, у цьому розділі дисертації розроблено *метод програмного імітаційного моделювання процесу поширення ІВ в сегменті мережі* з використанням поведінкових стратегій вузла СМ.

Інформаційний вплив зазвичай здійснюється масованим повторювальним донесенням інформації про певний об'єкт, явище, персону і інше до цільової аудиторії. Для досягнення максимального ефекту в реальному житті інформація пропонується в різноманітних видах та способах представлення.

Враховуючи фактор повторюваності та властивість інформаційного накопичення доречно в реалізації методу відобразити поширення інформації як певний ітераційний процес. На кожній ітерації активні вузли здійснюють передачу інформації вузлам в околі доступу з метою ІВ на них. Метод моделює поширення конкретної ідеї (α-ідеї), де рівень впливу визначається співвідношенням характеристик вузлів, що приймають участь в ході інформаційного обміну.

Алгоритм, що реалізується в методі програмного моделювання процесу поширення ІВ, аналітично можна описати наступним чином:

1. Обхід списку всіх вузлів мережі (сегменту мережі).
2. Якщо вузол активний (залученість до ідеї $I_{v_i} > 0{,}5\, I_g$):

2.1 Обрати вузол для інформаційної атаки;

2.2 Здійснити передачу інформації обраному вузлу;

2.3 Зменшити лічильник активності, передаючого вузла;

2.4 Якщо лічильник активності більше 0, перейти до 2.1;

3. Оновити список з визначенням нових активних вузлів.
4. Оновити графічне відображення вузлів сегменту СМ з урахуванням зміни показників залученості на поточній ітерації.

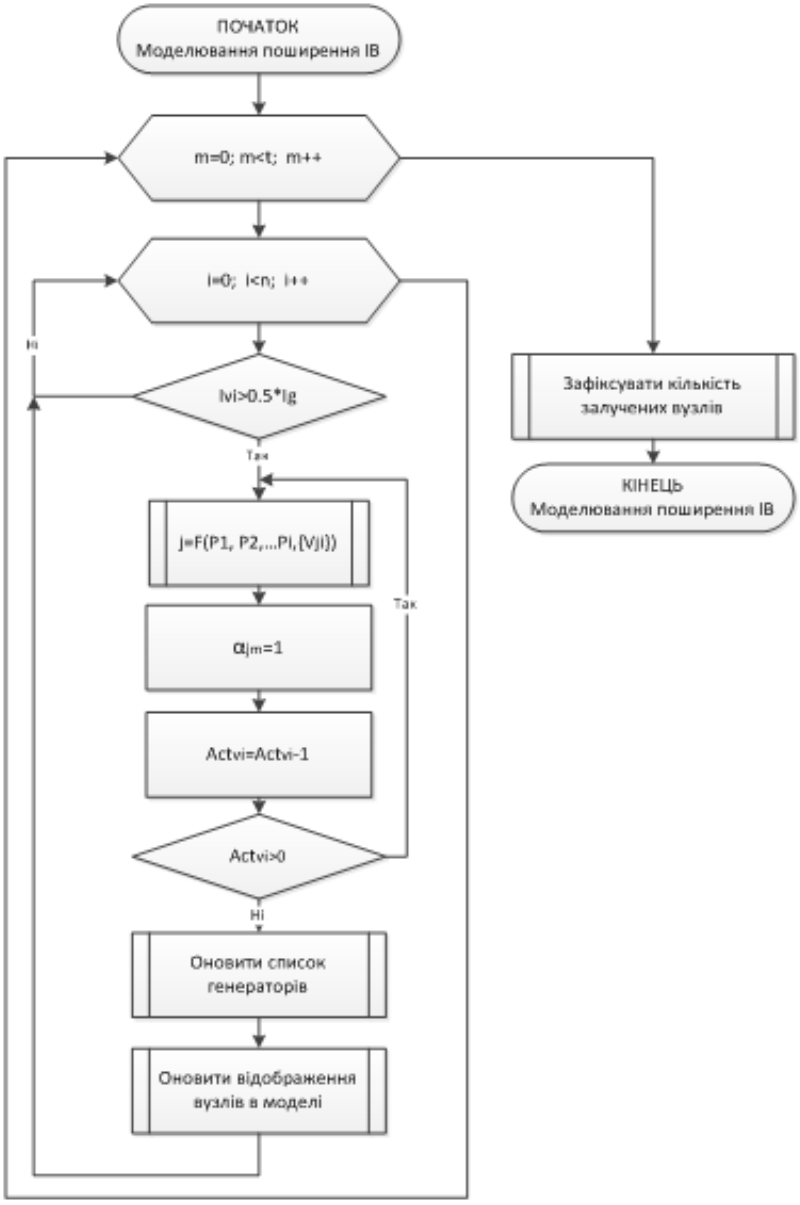


Рис. 1 Блок-схема алгоритму моделювання поширення ІВ

Алгоритм моделювання процесу поширення ІВ представлено на рис. 1 (n- кількість вузлів сегменту мережі, t- час поширення)

Окремо слід зазначити, що в методі програмного імітаційного моделювання процесу поширення ІВ в сегменті СМ, існують обмеження, серед яких варто вказати:

1. На початковому етапі моделі (нульова ітерація) рівень залученості до α-ідеї в усіх вузлів рівний 0, крім вузлів-генераторів.
2. На першій ітерації моделі інформація надсилається лише генераторами.
3. Рівень одиничного ІВ визначається співвідношенням визначеним (7).
4. На подальших ітераціях будь-який з вузлів може почати поширювати ІВ, якщо рівень залученості вузла перевищує половину рівня генератора.
5. Кількість інформаційних повідомлень від конкретного вузла за одну ітерацію визначається рівнем його активності.
6. Вибір цільового вузла для атаки визначається поведінковою стратегією.
7. Модель має графічну інтерпретацію динаміки стану сегменту мережі на поточній ітерації – вузли змінюють колір в залежності від рівня залученості.

Також у розділі набув подальшого розвитку *метод вибору цільового вузла суб'єктом ІВ у СМ під час інформаційних протиборств на основі методу аналізу ієрархій.*

Метод аналізу ієрархій (МАІ) – це математична процедура для ієрархічного зображення елементів з метою визначення суті деякої проблеми. Метод полягає в декомпозиції проблеми на більш прості складові частини, а також в обробці

суджень особи або осіб, що приймають рішення (ОПР) на підставі парних порівнянь пріоритетів (критеріїв) доцільності.

MAI передбачає декілька етапів:

1. Побудова відповідної ієрархії задачі прийняття рішень.
2. Попарне порівняння всіх елементів ієрархії.
3. Математична обробка отриманої від ОПР інформації (пошук власних векторів матриць попарного порівняння альтернатив).
4. Усунення неузгодженості матриць попарних порівнянь (якщо це необхідно).

Передумовами застосування вищезазначених етапів є:

вибрано скінченну підмножину альтернатив серед всіх можливих варіантів, в якості альтернатив обираються найбільш прийнятні (на думку ОПР) варіанти з точки зору розв'язуваної задачі та очікуваного результату;

встановлено набір критеріїв за якими будуть оцінюватися альтернативи.

Коротко охарактеризуємо зміст етапів MAI.

Перший етап передбачає попереднє ранжування критеріїв, в результаті якого вони розташовуються в порядку спадання важливості (значимості).

На другому етапі відбувається попарне порівняння критеріїв за важливістю за дев'ятибальною шкалою зі складанням відповідної матриці (таблиці) розмірності *n*x*n*, де *n* – кількість вибраних критеріїв. Система парних відомостей призводить до результату, який може бути представлений у вигляді обернено симетричною матриці. Елементом матриці a(*i, j*) є інтенсивність прояву елемента ієрархії ***i*** щодо елемента ієрархії ***j***, індекси ***i, j*** змінюються в діапазоні від 1 до n(де n - кількість критеріїв, за якими оцінюються альтернативи). Інтенсивність оцінюється за шкалою інтенсивності від 1 до 9, де оцінки мають наступний сенс: рівна важливість - 1; помірна перевага - 3; значна перевага - 5; сильна перевага - 7; дуже сильна перевага - 9; в проміжних випадках ставляться парні оцінки: 2, 4, 6, 8.

Матриця парних суджень має вигляд:

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 1/a_{12} & 1 & a_{23} & \dots & a_{2n} \\ 1/a_{13} & 1/a_{23} & 1 & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 1/a_{1n} & 1/a_{2n} & 1/a_{3n} & \dots & 1 \end{pmatrix}, \quad (12)$$

де a_{ij}– міра переваги об'єкта a_i в порівнянні з об'єктом a_j.

В ході аналізу створюється (n + 1) матриця: матриця порівняння критеріїв (попарне порівняння, (12)) і n матриць попарного порівняння альтернатив за обраним критерієм (*A*, *K*1, *K*2, *K*3 ... *Kn*). Розмірність даних матриць *m*x*m*, де *m* – кількість альтернатив, серед яких необхідно обрати найкращий варіант.

На третьому етапі відбувається нормалізація матриці, нормалізована оцінка вектора пріоритетів. Для пошуку власних векторів може використовуватися метод, заснований на наближених оцінках. Можна знаходити власні вектори вирішуючи СЛАР одержувану з рівняння (13).

Нехай число λ і вектор $x \in L$, $x \neq 0$ такі, що:

$$Ax = \lambda x. \quad (13)$$

Тоді число λ називається власним числом лінійного оператора A, а вектор x власним вектором цього оператора, відповідним власному числу λ. У скінченномірному просторі L_n векторна рівність (13) еквівалентна матричній рівності:

$$(A - \lambda E)X = 0, X \neq 0. \quad (14)$$

Звідси випливає, що число λ є власним числом оператора A в тому і тільки тому випадку, коли детермінант det (A-λE) = 0, тобто λ є корінь многочлена $p(\lambda)$ = det (A-λE), який називається характеристичним многочленом оператора A.

Формула пошуку власних векторів буде мати вигляд:

$$w_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}\ , \quad (15)$$

$$v_i = \frac{w_i}{\sum_{i=1}^{n} w_i}. \quad (16)$$

Узагальнені пріоритети розраховуються за допомогою матриці порівняння альтернатив:

Таблиця 3

Матриця порівняння альтернатив

Критерії / Альтернативи	**К1**	**К2**	**К3**	**Узагальнені критерії**
	$\mu 1$	$\mu 2$	$\mu 3$	
А1	v_{11}	v_{12}	v_{13}	λ1
А2	v_{21}	v_{22}	v_{23}	λ2
А3	v_{31}	v_{32}	v_{33}	λ3

Тут v_{ij}– отримуємо за формулою (16), а μ_i – власний вектор матриці порівняння критеріїв. Далі глобальні пріоритети альтернатив (або узагальнені пріоритети) розраховуються за формулою:

$$\lambda_k = \sum_{i=1}^{n} \mu_i a_{ki}, \quad (17)$$

де μ_i – власний вектор матриці порівняння критеріїв.

Так як метод МАІ не може бути повністю формалізований, через необхідність залучати експертів для оцінки альтернатив за критеріями, на результати методу можуть впливати суб'єктивні чинники – неуважність експертів, помилки оцінок і т.п. Для перевірки узгодженості суджень експертів застосована методика, яка заснована на оцінці відношення однорідності (ВО) матриць попарних порівнянь. Для отримання оцінок використані наступні формули:

$$BO = \frac{IO}{M(IO)}, \quad (18)$$

де IO – індекс однорідності, який обчислюється за формулою (19), $M(IO)$ – середнє значення індексу однорідності випадковим чином складеної матриці парних порівнянь, що базується на експериментальних даних, значенням якого є таблична величина, вхідним параметром виступає розмірність матриці (табл. 4).

Таблиця 4

Середнє значення індексу однорідності (визначено експериментальним шляхом)

r	1	2	3	4	5	6	7	8	9	10	11
***M*(*IO*)**	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

$$IO = \frac{\lambda_{max} - r}{r - 1}, \quad (19)$$

де λ_{max} – максимальне власне значення; r – порядок матриці попарних порівнянь (r = n для матриці порівняння критеріїв, r = m для матриці порівняння альтернатив), неузгодженість може виникати при r ≥ 3.

Для розрахунку максимального власного значення матриці існують різні підходи, один з підходів передбачає використання формули (20):

$$\lambda_{max} = e^T AW, \quad (20)$$

де e^T– одиничний вектор розмірності r; A – матриця попарних порівнянь; W – головний (нормалізований) власний вектор матриці A.

Після отримання значення ВО його порівнюють з значенням 0,10, матриця суджень вважається узгодженою якщо ВО <= 0,10. Хоча така оцінка не є однозначною – матриця з оцінкою ВО більше 0,10 насправді може бути узгодженою. Тобто, оцінка ВО це певний маркер, що дозволяє звернути увагу експерта і, можливо, переглянути (перевірити) оцінки. Найкраща альтернатива визначається за максимальним значенням глобального пріоритету.

Адаптація MAI до задачі вибору цільових вузлів СМ суб'єктами впливу

Для застосування MAI до вибору об'єктів впливу у СМ необхідна його певна адаптація, що було проведено у даному розділі. Адаптація наведена нижче.

Альтернативи для MAI: Вузол_1, Вузол_2…Вузол_k. (множина обраних вузлів потенційно корисних з точки зору поширення інформаційного впливу).

Критерії варто розділити на: залежні від оцінки експерта і кількісні – незалежні від суб'єктивної експертної оцінки.

До кількісних (незалежних від експерта) критеріїв можна віднести: кількість контактів вузла мережі; активність (усереднена кількість повідомлень за одиницю часу).

Для ранжування альтернатив за окремим критерієм пропонується використати (21):

$$R(K_{vi}) = \left[9 \cdot \frac{K_{vi}}{Max(K_{vi})}\right], \quad (21)$$

де K_{vi} – оцінка і-ї альтернативи за критерієм K_v; $Max(K_{vi})$ – максимальне значення оцінки за критерієм K_v, серед оцінок всіх альтернатив.

До експертних оцінок варто віднести: схильність до α-ідеї; структурне положення; репутація. Найбільш сприятливий результат очікується у випадку оптимальної збалансованості критеріїв.

Для кореляції балансу пропонується ввести компенсуючі критерії:

– $\frac{R}{Op}$ – відношення критеріїв на основі властивостей вузла репутації та спротиву;

– $\mathrm{Act} \cdot \mathrm{Str}$ – добуток критеріїв на основі властивостей вузла активності та структурного положення.

Таким чином, зазначений метод дозволяє за меншу кількість часу поширити ІВ серед більшої кількості вузлів сегменту СМ за рахунок оптимального вибору об'єктів для ІВ.

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням розроблених методів, моделі та стратегій.

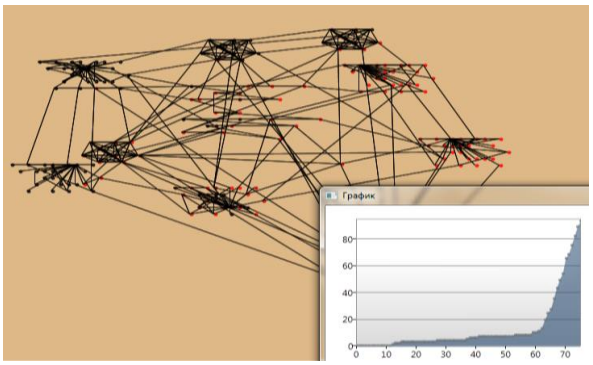


Рис. 2 Сегмент мережі, що згенеровано в програмній моделі, на і-й ітерації моделі

На основі реалізації, запропонованої у другому розділі дисертації математичної моделі поширення ІВ в сегменті СМ, було реалізовано можливість застосування різних ПС суб'єктами ІВ та досліджено залежності поширення інформації від початкового положення та структури найближчого оточення суб'єкта впливу. Після чого було проведено експериментальне дослідження методу генерації структури сегменту СМ з заданою кількістю кластерів.

Приклад сегменту мережі, що згенеровано в програмній моделі відображено на рис. 2. Для графічного відображення динаміки залученості вузлів до ідеї додано можливість отримання динамічного графіка кількості вузлів уражених ІВ на кожній ітерації роботи моделі. Графік дозволяє порівнювати швидкість росту кількості захоплених вузлів для різних ПС та різної структури сегменту СМ.

Програмна модель методу будується з використанням об'єктно-орієнтованого підходу. Всі дії вузла реалізуються як його методи, окремо існує клас, що слідкує за ітераційним процесом. Діаграма базових класів моделі представлена на рис. 3.

Також було проведено експериментальне дослідження методу програмного імітаційного моделювання процесу поширення ІВ в сегменті СМ на основі базових поведінкових стратегій вузла СМ. Крім того було проведено порівняльне дослідження ефективності запропонованих поведінкових стратегій вузлів СМ, приклади результатів програмного імітаційного моделювання наведені на рис. 4.

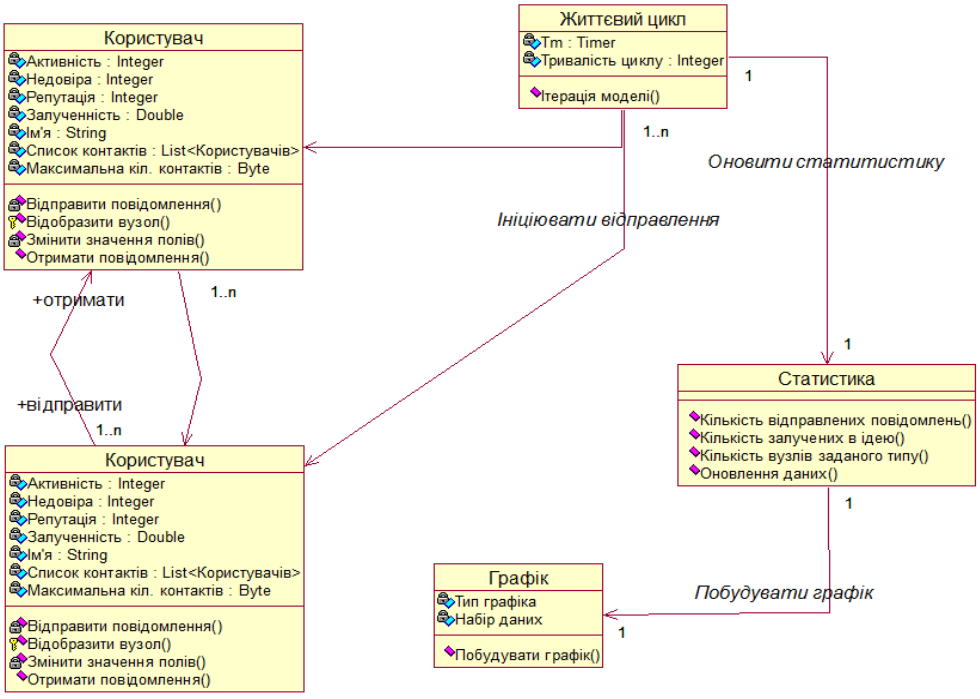
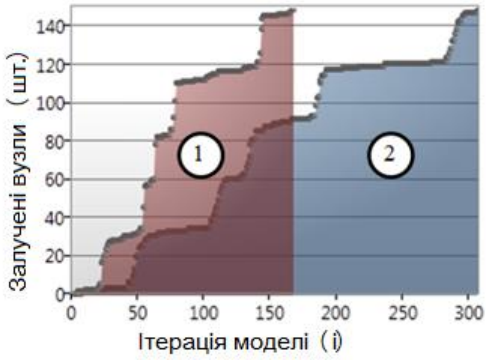
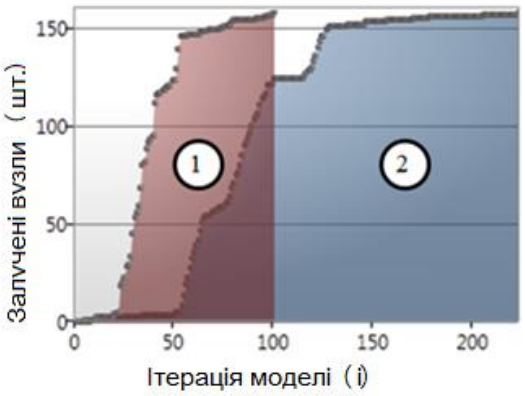


Рис. 3 Діаграма класів моделі



(а) Швидкість поширення ІВ у сегменті з 140 вузлів для стратегій «дерево» – 1 та «кущ» – 2



(б) Швидкість поширення ІВ у сегменті СМ з 160 вузлів для стратегій «дерево» – 1 та «кущ» – 2 при збільшені щільності зв'язків на 40%

Рис. 4 Порівняння ефективності базових стратегій поведінки суб'єктів впливу

Отримані результати показують наступне: реакцію моделі на різні типи поведінкових стратегій; зменшення ефективності стратегії з вибором за критерієм в порівнянні з випадковим вибором при збільшенні щільності зв'язків мережі; графік захоплення вузлів має ступінчасту структуру; різкий ріст кількості захоплених вузлів спостерігається після залученості близько 10-15% від загальної кількості вузлів. А також було визначено, що стратегія «дерево» буде мати суттєву перевагу при середній щільності зв'язків. При низькій щільності стратегія «кущ» з великою ймовірністю може випадково обирати потрібний вузол і за рахунок вищої активності в наслідок заощадження часу на аналіз буде переважати стратегію, що опирається на аналіз навколишніх вузлів. При високій щільності зв'язків значно підвищується кількість альтернативних шляхів ефективної інформаційної атаки і вирішальним фактором є лише активність вузла генератора. Дані результати можна розглядати як доказ адекватності і ефективності запропонованих ПС вузлів СМ.

Проведено експеримент з використанням програмної моделі, в якій створено сегмент СМ, що містить декілька кластерів (рис. 5).

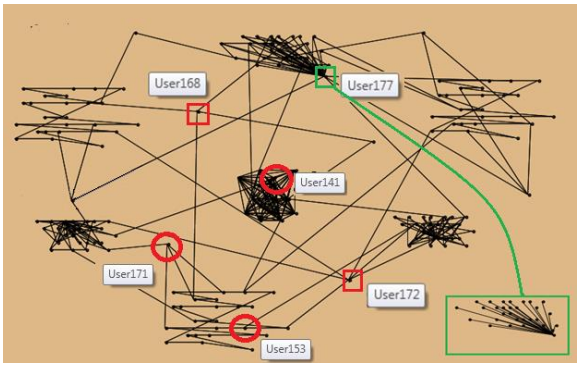


Рис. 5 Сегмент СМ згенерований для тестування запропонованого методу

Були проведені обчислення для вибору вузлів для ІВ на основі методу MAI, та визначені три альтернативи, це вузли: №168, №172, №177. Перспективні альтернативи обрані методом MAI виділено на рис. 5 квадратами, колами виділено вузли, що були обрані випадково та далі будуть розглядатись в експерименті як альтернативи для порівняння.

Проілюструємо приклад розрахунків за методом MAI для порівняння перспективності вузлів №168, №172, №177. Кількісні показники, експертна оцінка положення, та нормалізовані показники наведено в табл. 5.

Таблиця 5

Оцінки альтернатив за критеріями

Критерії	Вузли мережі					
	№ 177	**№ 172**	**№ 168**	**№ 177**	**№ 172**	**№ 168**
	Кількісні показники			***Нормалізовані показники***		
Кількість зв'язків	26	6	4	9	2	2
Активність (Act)	5	3	4	9	5	7
Спротив (Op)	23	20	12	5	5	9
Структурне положення (Str)	6	5	9	6	5	9
Репутація (R)	30	54	67	4	7	9
R/Op	1,3	2,7	5,6	2	4	9
Act · Str	40	18	36	9	4	8

В табл. 6 наведено ранжування критеріїв з табл. 5.

Таблиця 6

Ранжування критеріїв

Критерії		**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**
Кількість зв'язків	**K1**	1	0,25	5	0,17	3	2	0,14
Активність (Act)	**K2**	4	1	6	0,33	5	3	0,2
Спротив (Op)	**K3**	0,2	0,17	1	0,17	0,5	0,2	0,13
Структурне положення (Str)	**K4**	6	3	6	1	5	3	0,2
Репутація (R)	**K5**	0,33	0,2	2	0,2	1	0,2	0,17
R/Op	**K6**	0,5	0,33	5	0,33	5	1	0,25
Act · Str	**K7**	7	5	8	5	6	4	1

Найбільший влив на результат поширення ІВ мають активність (особливо в сегментах з щільними зв'язками) та структурне положення вузла. Зазначмо, що структурне положення має в більшості випадків суттєвіший вплив на результат, ніж активність. Відповідно найвпливовішими критеріями (в порядку спадання) є: збалансовуючий критерій: $\mathrm{Act} \cdot \mathrm{Str}$; структурне положення (оцінюється експертом); активність (кількісний незалежний показник).

Приклад порівняння альтернатив за одним з критеріїв наведено в табл.7.

Таблиця 7

Матриця парних порівнянь альтернатив відносно критерію K1

	№ 168	**№ 172**	**№ 177**
№ 168	1	0,333333	1
№ 177	3	1	3
№ 172	1	0,333333	1

Вектори матриці
v_0 = 0,2
v_1 = 0,6
v_2 = 0,2

$\lambda_{max} = 3$, $BO = 2{,}46716227694479\text{E-}16$

Нижче наведено матрицю отримання узагальнених пріоритетів (табл. 8).

Узаг. пріоритети:λ_0 = 0,4799145709407, λ_1 = 0,1454066041997, λ_2 = 0,3746788248594

Отже, MAI серед запропонованих альтернатив визначив найкращим вибором для атаки вузол **№ 168**. Наступною за пріоритетом альтернативою є **№ 177**, а потім – **№ 172.**

Таблиця 8

Матриця порівняння альтернатив

Вузли	Критерії						
	K1	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**
	0,074084	**0,149205**	**0,02413**	**0,216401**	**0,034732**	**0,081467**	**0,419981**
№ 168	0,200000	0,285714	0,625013	0,581552	0,730645	0,739594	0,466470
№ 172	0,200000	0,142857	0,136500	0,109452	0,080961	0,093813	0,100498
№ 177	0,600000	0,571429	0,238487	0,308996	0,188394	0,166593	0,433032

Було проведено експеримент на програмній моделі та порівняння отриманих результатів з оцінками альтернатив по MAI.

В експерименті вибрані альтернативні вузли використовувалися як початкові суб'єкти поширення інформації, для поширення використовуватись ПС «Кущ». Оцінювалась швидкість захоплення 90% вузлів сегменту СМ. Загальна кількість вузлів в згенерованому сегменті – 178, відповідно оцінюється швидкість захоплення 160 вузлів. В табл. 9 наведено результати серії експериментів. Окрім вузлів вибраних серед перспективних альтернатив (вузли №168, №172, №177) проведемо таку ж серію експериментів для трьох випадково вибраних вузлів, що не належать до множини обраних альтернатив через гірші показники власних властивостей і порівняємо результати. А саме, вузли: №153 – вибраний випадковим чином серед вузлів кластеру типу «група»; №141 – вибраний випадковим чином серед вузлів кластеру типу «кліка» з максимальною кількістю зв'язків у сегменті мережі, що розглядається; №171 – вибраний випадково серед вузлів-мостів між декількома кластерами. Розміщення вузлів, що розглядались в експерименті, представлено на рис. 4. Експеримент на моделі показав наступні результати (табл. 9). Як видно з результатів експерименту, вузли обрані на основі методу MAI дозволяють за меншу кількість часу поширити ІВ серед вузлів сегменту СМ.

Таблиця 9

Результати експерименту

Вузол	Номер експерименту										Середнє значення
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
	Кількість ітерацій до захоплення 90% вузлів сегменту мережі										
№168	147	142	151	142	138	152	142	147	152	144	146
№177	152	154	154	158	161	151	160	154	150	152	155
№172	166	168	172	174	168	164	166	168	174	172	169
№153	198	201	205	186	198	200	204	198	190	202	198
№141	169	159	156	162	165	158	162	160	162	151	160
№171	184	192	186	186	190	182	196	182	189	184	187

Серед вибраних альтернатив по MAI було обрано першим за пріоритетом вузол №168, другим – №177 та третім – №172. Експеримент на програмній моделі підтвердив, що вибір вузла №168, з поміж інших альтернатив є найкращим варіантом, з точки зору швидкості поширення ІВ в сегменті СМ. Швидкість захоплення вузлів у випадку атаки через вузол №168 на 6% вища, ніж через вузол №177 («лідер думок»), і на 14% вище ніж з №172. Також вузли, обрані методом MAI, показали в середньому на 16% кращі результати, ніж вузли обрані випадковим чином серед виграшних структурних позицій СМ.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв’язання актуальної та важливої науково-технічної задачі підвищення швидкості поширення інформаційних впливів в сегменті мережі.

У процесі виконання дисертаційної роботи отримані такі наукові та практичні результати:

1. Проаналізовано методи та моделі поширення інформаційних впливів у соціальній мережі в умовах інформаційного протиборства, аналіз дозволив виявити як комбіновані комплексні моделі, що мають підвищити адекватність і відповідність програмного моделювання реальним процесам, так і моделі, орієнтовані на дослідження конкретних характеристик. Аналіз показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла та поведінку суб’ктів при пошерені інформації, стратегію поширення інформації, яку обирає вузол в процесі інформаційних впливів.

2. Вперше розроблено математичну модель поширення інформаційних впливів в сегменті соц. мережі, яка дає можливість застосування різних поведінкових стратегій суб’єктами ІВ на основі аналізу особистісних характеристик вузлів, що обираються для атаки. В ході розробки моделі вперше формалізовано поняття «поведінкова стратегія» та запропоновано приклади базових поведінкових стратегій суб’єктів інформаційних впливів у соціальних мережах, що дозволяють ефективно моделювати різні підходи до вибору цільових вузлів суб’єктами інформаційного впливу.

3. Удосконалено метод генерації структури сегменту соціальної мережі, що дозволяє обирати кількість і типи кластерів сегменту соціальної мережі. Запропонований підхід дає можливість генерувати сегменти мереж з наперед заданою структурою зв’язків та наявними сталими підмножинами вузлів (групи, лідерські групи, кліки)

4. Набув подальшого розвитку метод оптимального вибору цільового вузла для атаки в ході поширення впливів суб’єктом мережі на основі методу аналізу ієрархій та застосування поведінкових стратегій на основі наявних даних про мережу під час інформаційних протиборств. Застосування поведінкових стратегій суб’єктів інформаційних впливів на основі аналізу даних про мережу дозволяє підвищити швидкість поширення інформації в середньому на 70% в порівнянні з випадковим вибором вузлів для атаки. Вибір оптимального цільового вузла дозволяє підвищити швидкість поширення ІВ. Швидкість поширення ІВ через вузли, обрані за запропонованим методом, в експериментах на моделі, в середньому на 16% вища, ніж швидкість через вузли, обрані випадковим чином серед виграшних структурних позицій СМ. В порівнянні з запропонованим іншими авторами методом поширення ІВ через «лідера думок» приріст швидкості поширення ІВ через вузол вибраний по методу МАІ склав 6%.

5. Проведене експериментальне дослідження програмної моделі підтверджує адекватність застосування запропонованих методів з точки зору підвищенні швидкості поширення ІВ.

Результати дисертації впроваджені і використовуються у діяльності ТОВ «Сайфер БІС» та ЦНТУ, що підтверджено відповідними актами впровадження.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Мелешко Є.В., Константинова Л.В., Улічев О.С. Дослідження властивостей інформації та методів її поширення з точки зору інформаційної безпеки в соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 3(35). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2015. – С. 98-106.

2. Улічев О.С. Дослідження моделей розповсюдження інформації та інформаційних впливів в соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 4(50). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2018. – С. 147-151.

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

4. Улічев О.С., Мелешко Є.В. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах // Збірник наукових праць " Сучасні інформаційні системи". Випуск 2(2). – Харків: ХПІ. – 2018. – С. 35-39.

5. 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, Wilga, Poland (ISSN: 0277-786X). – 2019. – Number article: 111761T. **(SCOPUS)**.

6. 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. – P. 34-47.

7. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження робастності рекомендаційних систем з колаборативною фільтрацією до інформаційних атак // Наукове видання Кібербезпека: освіта, наука, техніка.– Київ: КУБГ, 2019. Т.1 № 5. – С. 95-104.

8. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження відомих моделей атак на рекомендаційні системи з колаборативною фільтрацією // Збірник наукових праць Системи управління, навігації та зв'язку. – Полтава: ПНТУ, 2019. – № 5 (57). – С. 67-71.

9. Ulichev O., Meleshko Ye., Smirnov O., Khokh V., Goncharenko Iu. The method of choosing objects for informational influence in social networks during information campaign based on the analytic hierarchy process // CEUR-WS, Vol. 2588, Lviv, Ukraine (ISSN: 1613-0073). – 2019. – P. 215-227 **(SCOPUS)**.

10. Улічев О.С., Мелешко Є.В. Моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі // Науковий журнал «Захист інформації». – Київ: НАУ, 2020. – Т. 22, № 3. – С. 166-176.

11. Улічев О.С. Генерування моделі соціальної мережі для дослідження впливу її структури на розповсюдження інформаційних впливів // Збірник тез II Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». м. Кропивницький. 20-22 квітня 2017 р. –

Кропивницький: ЦНТУ. – 2017. – С. 103-104.

12. Улічев О.С., Мелешко Є.В. Програмна модель соціальної мережі та стратегій поширення інформаційно-психологічних впливів // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». м. Кропивницький. 19-20 квітня 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 136-220.

13. Улічев О.С., Мелешко Є.В. Математична модель розповсюдження інформації в сегменті соціальної мережі // Матеріали Двадцятого Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 13-14 квітня 2018 р. – Кропивницький: КЛА НАУ. – 2018. – С. 68-72.

14. Улічев О.С., Мелешко Є.В. Програмна модель розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Матеріали VIII Міжнародної науково-технічної конференції «ITSEC», м. Київ, 16-18 травня 2018 р. – Київ: НАУ. – 2018. – С. 34-35.

15. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез Сьомої міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 17-19 травня 2018 р. – Львів: Національний університет "Львівська політехніка". – 2018. – С. 29-30.

16. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Збірник тез X Всеукраїнської науково-практичної конференції «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем(SITS'2018)»,21-23 червня 2018 року. – Миколаїв-Коблево: НАУ та МІПРО. – 2018. – С. 77–79.

17. Мелешко Є.В., Шингалов Д.В., Улічев О.С. Дослідження Баєсових мереж довіри як засобів для моделювання динамічних процесів у складних мережах // Матеріали XVII Міжнародної науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем», 20-22 листопада 2019 р. – Дніпро: ДНУ. – 2019. – С. 284-285.

18. Мелешко Є.В., Хох В.Д., Улічев О.С. Методи тестування робастності рекомендаційних систем з колаборативною фільтрацією // Матеріали Всеукраїнської науково-практичної Інтернет-конференції «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» 13-14 листопада 2019 р. – м. Кропивницький: ЦНТУ. – 2019. С. 88-89.

19. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження методів підвищення робастності рекомендаційних систем до інформаційних атак // Матеріали VI Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», 19-22 лютого 2020 р. – м. Київ: Вид-во Європейського університету, 2020. – С. 65-70.

АНОТАЦІЯ

Улічев О.С. Модель і методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 «Інформаційна безпека держави». – Національний авіаційний університет, Київ, 2021.

Дисертаційна робота присвячена розв'язанню актуальної науково-технічної задачі розроблення методів і засобів програмного моделювання та реалізації різних стратегій поширення інформаційних впливів у сегментах соціальних мереж.

У роботі проведено аналіз сучасних методів і моделей поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства, який показав, що переважна більшість моделей і методів не враховує індивідуальних характеристик вузла, а саме поведінку окремого вузла, стратегію поширення інформації, яку обирає вузол в процесі інформаційного впливу. Розроблено математичну модель поширення інформаційних впливів в сегменті соціальної мережі, яка дає можливість застосування різних поведінкових стратегій суб'єктами впливу. Крім того, на базі запропонованої моделі розроблено алгоритми програмного імітаційного моделювання процесу поширення інформаційних впливів у сегментах соціальної мережі, а також алгоритми генерації структури сегментів соціальної мережі. Розроблено базові поведінкові стратегії суб'єктів впливу у соціальній мережі під час інформаційних протиборств, що дозволяють ефективно моделювати різні підходи до вибору цільових вузлів суб'єктами впливу та процес поширення ІВ. Удосконалено методи генерації структури сегменту соціальної мережі та програмного імітаційного моделювання процесу поширення інформаційних впливів у соціальній мережі, що дозволяють обирати кількість і типи кластерів у мережі та моделювати різні поведінкові стратегії суб'єктів впливу. Запропоновано метод вибору поведінкових стратегій суб'єкту впливу у соціальній мережі під час інформаційних протиборств, який дозволяє за меншу кількість часу поширити інформаційний вплив серед вузлів сегменту соціальної мережі.

Ключові слова: інформаційна безпека, інформаційне протиборство, соціальні мережі, інформаційні впливи, імітаційне моделювання

ABSTRACT

Ulichev O. Model and Methods Dissemination of Information Influences on Social Networks in Conditions of Information Confrontation - Manuscript.

The dissertation on competition of scientific degree of the technical sciences candidate on specialty 21.05.01 "State information security". - National Aviation University, Kyiv, 2021.

The dissertation to the solution of the actual scientific and technical problem of development of methods and means of software modeling and realization of various strategies of distribution of information influences in segments of social networks is devoted.

The relevance of the topic is determined by the increasing role of social networks in the processes of information and psychological influences, which may have economic, political and other motives. In particular, one of the aspects that determine the relevance of the study is countering the propaganda of enemy states in social networks.

The analysis of modern methods and models of information influences dissemination in social networks in the conditions of information confrontation is carried out, which showed that the vast majority of models and methods do not take into account individual node characteristics, namely behavior of separate node and strategy of dissemination information influences.

The mathematical model of information influence distribution in the social network segment has been developed, which allows the application of different behavioral strategies by the subjects of influence. In addition, on the basis of the proposed model developed algorithms for software simulation of the process of dissemination of information influences in the segments of the social network, as well as algorithms for generating the structure of segments of the social network. Basic behavioral strategies of subjects of influence in a social network during information confrontations are developed, which allow to effectively model different approaches to the choice of target nodes by subjects of influence and the process of dissemination of information-psychological influences. Algorithms for software simulation of various behavioral strategies of the subjects of influence in social networks have been developed and their effectiveness has been compared. Examples of basic behavioral strategies of subjects of influence in a social network during information confrontations are offered.

As a result of considering a number of proposed methods for generating the network structure, their disadvantages were revealed: a low level of clustering, the inability to generate a network with a given structure.

The method of generating the structure of the social network segment has been improved, which by choosing the structure of the social network from a set of parameterized subsets of clusters and choosing their structural features, allows you to choose the number and types of clusters in the network. The method of software simulation modeling of information influence distribution in the social network has been improved, which due to the application of the proposed mathematical model of information influence distribution in the social network segment makes it possible to model different behavioral strategies of information influence subjects. The method of choosing the behavioral strategies of the subject of influence in the social network based on analytic hierarchy process during information conflicts, which allows for less time to spread informational influence among the nodes of the social network segment.

The method of optimal selection of the target node for the attack during the spread of

influences by the network entity based on the method of analysis of hierarchies and the application of behavioral strategies based on available data about the network during information conflicts has been further developed. Applying the behavioral strategies of the subjects of information influences based on the analysis of network data can significantly increase the speed of information dissemination by an average of 70% compared to the random selection of nodes to attack. Selecting the optimal target node allows for less time to spread informational influences among the nodes of the network segment.

The software simulation model of the social network and the processes of dissemination of information and psychological influences in it was developed using an object-oriented approach. All actions of network nodes are implemented as their methods, there is a separate class that monitors the iterative process, counts iterations and initiates the action of nodes. To simplify the perception of simulation results, as well as their analysis, the software simulation model contains a graphical display of the social network graph and shows changes in it over time, in particular, the state of network nodes in relation to information and psychological influences, as well as a dynamic graph involved in the influence of nodes on each iteration of the model.

Keywords: information security, information confrontation, social networks, information influences, dissemination strategies, simulation modeling