DOI: 10.25140/2411-5363-2023-2(32)-193-200
УДК 004.738.5:351

Ольга Васильєва
аспірантка
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: olga.vasiljeva37@gmail.com. **ORCID:** https://orcid.org/0000-0001-8263-782X

МОДЕЛІ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ ДИНАМІКИ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ

У статті розглянуто деякі положення проведення інформаційні операції, як одна з головних загроз національній безпеці в інформаційній сфері, продемонстровано використання соціальних мереж як основного поля для їх проведення завдяки новітнім технологіям, проведено аналіз запропонованих моделей інформаційних операцій у соціальних мережах.

Стаття присвячена проблемі комплексного застосування теоретичних моделей, які використовуються для дослідження «вірусного» поширення інформації в соціальних мережах кіберпростору. Проаналізовано формальне моделювання, яке застосовується до вивчення особливостей комунікації в соціальних мережах. Виділено три складові формальних моделей поширення онлайн-повідомлень у соціальних мережах: типологія повідомлень, мережева модель, формальна модель поширення сигналів. Окрема увага приділена можливостям застосування нелінійних моделей поширення інформації.

Ключові слова: *моделювання; інформаційні операції; національна безпека в інформаційній сфері; соціальні мережі; динамічне середовище.*

Рис.: 4. Бібл.: 7.

Актуальність теми дослідження. В умовах сьогодення Україна, прагнучи забезпечити та зберегти державний суверенітет, має приділяти увагу не лише таким складовим державної безпеки, як військова, економічна чи дипломатична, а також значною мірою інформаційній, особливо в контексті організації протидії інформаційній війні, яку веде агресор не лише проти нашої держави, а й в глобальному інформаційному просторі проти світових демократій.

Постановка проблеми. Росія організовує та проводить у межах інформаційної війни масштабні інформаційні кампанії, пропагандистську діяльність, займається поширенням фейків на стратегічному рівні з метою руйнування цінностей та потенціалу інших держав, заміни їх власними та прагне до підпорядкування їхніх ресурсів для використання у своїх інтересах. Цілком очевидно, що інформаційна складова війни є не менш небезпечною для нашої країни, ніж військова.

Можемо стверджувати, що одним з основних полів здійснення інформаційних впливів сьогодні є соціальні мережі в кіберпросторі. І причиною цього став стрімкий розвиток інформаційних технологій, візуалізація та глобалізація медіасистем, виникнення новітніх комунікативних моделей і розширення інтерактивних аудиторних рецепцій. Активізація інформаційних процесів вплинула також на систему стратегічних комунікацій суспільства, у якій провідна роль відводиться комунікативній складовій. Соціальні медіа нині дозволяють аудиторії набувати таких ознак як, мобільність, персоніфікація, інтерактивність. Вони перетворилися на домінуючий канал поширення інформації та комунікації громадян у віртуальному просторі. Саме соціальні мережі надають користувачам засоби для обміну контентом різного типу, утворення зв'язків з іншими користувачами, саморозвитку, об'єднання у віртуальні спільноти за спільними інтересами тощо.

Ці чинники створюють нагальну потребу у вивченні нової медійної реальності як на теоретичному, так і на емпіричному рівнях. Проте більшість наукових досліджень мають дескриптивний характер і спрямовані на вдосконалення нормативно-правового регулювання інформаційного простору мережі Інтернет, призначені для вирішення окремих часткових завдань забезпечення інформаційної безпеки, не враховують особливості процесів соціальної комунікації користувачів у віртуальних спільнотах та функціонування соціальних мереж [1].

Саме для того, щоб діяти на випередження, бути в змозі своєчасно виявляти та нейтралізувати інформаційні операції супротивника, а також ефективно планувати власні, пропонується розглянути такий алгоритм як імітаційне моделювання, яке активно застосовується для динамічних систем та соціальних процесів, до яких можемо віднести й інформаційні операції.

Аналіз останніх досліджень і публікацій. Дослідження останніх публікацій показало, що проблеми виявлення та організації протидії інформаційним операціям як загрозі інформаційної безпеки держави, а також проблема ефективного планування власних наступальних інформаційних операцій є досить актуальною як у практичному досвіді, так і в наукових колах. Так, до питання вирішення завдання аналізу та виявлення інформаційного впливу в соціальних мережах на основі мультиагентних моделей поширення інформації зверталися такі науковці, як Д. В. Ланде та В. О. Дадонов. До питання моделювання інформаційних операцій зверталися О. С. Улічев, Ю. В. Наконечна, А. Б. Качинський. Науковець К. Молодецька-Гринчук дослідила методи оцінювання ознак загроз інформаційній безпеці держави в соціальних медіа. Методи моделювання інформаційних операцій досліджували також В. П. Горбулін, О. Г. Додонов та Д. В. Ланде.

Якщо ми говоримо про моделювання інформаційних операцій, яке може бути застосоване не стільки для виявлення, Більшість науковців погоджуються, наприклад, із запропонованим Д. В. Ланде лінійно-статистичним методом для виявлення інформаційних операцій на основі кількісного аналізу контенту в інформаційному полі. Цей метод може бути застосований, якщо говорити про інформаційні операції, організовані в класичних електронних ЗМІ. При цьому самі автори погоджуються з тим, що виявлення відбувається вже на пізніх стадіях, коли організація ефективної протидії або нівелювання не є можливими. Запропоновані в роботах деяких науковців методи виявлення інформаційних операцій засновані на семантичному підході до оцінки повідомлень. Вони мають високу повноту і точність виявлення впливів, але виконуються за участю експертів і практично не можуть бути автоматизовані.

скільки для планування та організації власних інформаційних операцій з метою вироблення критеріїв ефективності, запропоновані методі моделювання базуються на кількісних та якісних оцінках саме інформації. Автор даної статті пропонує розглянути моделювання інформаційних операцій в соціальних мережах з точки зору саме механізму розповсюдження контенту.

Виділення недосліджених частин загальної проблеми. Проведений аналіз останніх досліджень і публікацій показав, що попри великий спектр наукових праць, на сьогодні не існує універсального та загальноприйнятого підходу ні до виявлення, ні до моделювання інформаційних операцій.

Метою статті аналіз запропонованих моделей інформаційних операцій, які проводяться в соціальних мережах.

Виклад основного матеріалу. Інформаційні операції не є принципово новим явищем, по суті, вони використовувались протягом історії людства повсякчас. Однак сьогодні це поняття як і його суть стали більш значущими. Що ж змінилось?

Змінилися основні методи та прийоми, вони отримали наукове обґрунтування, на цьому фоні виникають наукові дисципліни про управління поведінкою людини та спільнот – соціологія, психоаналіз, теорія реклами, сугестологія, нейролінгвістичне програмування, контент-аналіз.

Також виникають принципово нові електронні засоби масової інформації. Це не лише традиційні новинні сайти, а також соціальні мережі та мобільні месенджери, які використовують новітні технології поширення та популяризації різних типів контенту, алгоритми видачі контенту та його пріоритезації з урахуванням індивідуальних характеристик користувачів, що сприяє поширенню контенту, який спрямований на визначені аудиторії та активно використовується в інформаційних операціях, а також створює сегрегації суспільства [2].

Усе це є достатньо новим з погляду побудови алгоритмів управління соціумом, а також підтверджує теорію про те, що інформаційна зброя – це насамперед алгоритм.

У соціальних системах, серед багатьох інших характеристик, найбільше чітко проявляється цілісність, тобто наявність таких властивостей, які не притаманні жодному елементу, що складають систему, узятому окремо. Ця властивість, яку називають «емерджентністю», є результатом виникнення між елементами системи особливих синергетичних зв'язків. Під терміном «емерджентність», уперше введеному в науковий ужиток Дж. Г. Льюісом, розуміється те, що у фізичних системах ціле є найчастіше більшим, ніж сума частин, тобто на кожному рівні складності виникають нові, часто непередбачені якості, які не властиві окремим складовим. Емерджентність соціальної системи не дає можливості обмежитися вивченням її елементів і зв'язків між ними, а припускає цілісний аналіз усієї системи [3].

Переможцем в інформаційному протистоянні двох інформаційних систем стає та сторона, яка в змозі більш повно промоделювати поведінку супротивника в різних ситуаціях, а також визначити свій власний алгоритм поведінки та реалізувати його.

Саме тому завданням даної публікації є підхід до інформаційних операцій не з точки зору аналізу власне інформації, а з точки зору процесів її поширення (динаміку та топологію розповсюдження контенту) в інформаційному середовищі.

Типова динаміка розповсюдження контенту при інформаційній операції, до якої звертаються більшість наукових праць, виглядає наступним чином: сплеск, хвилі із періодом зростання та затухання. Так Д. Ланде пропонує такий типовий варіант кривої: «фонові публікації» - «затухання» - «артпідготовка» - «затухання» - «атака».

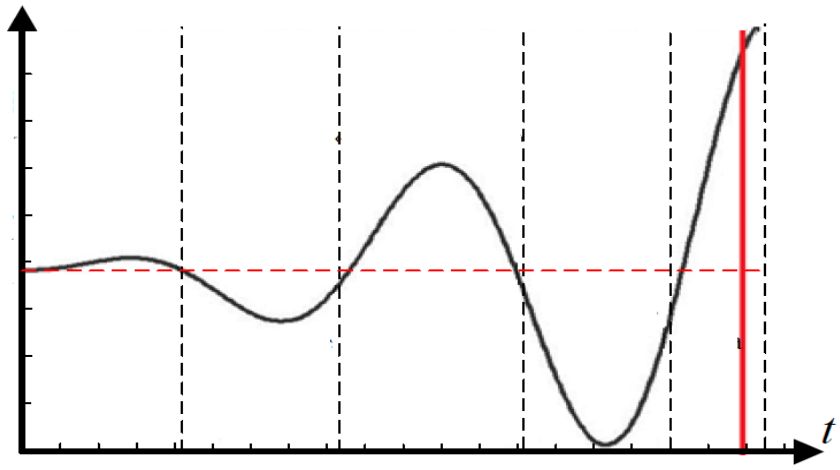

Рис. 1 Типова динаміка інформаційних потоків

При цьому, звичайно, слід брати до уваги тематику інформаційної операції, чи є вона новою в інформаційному полі, чи фігурує постійно, а також враховувати арену, де саме відбувається поширення.

Такий шаблон може використовуватись для виявлення інформаційних операцій як шляхом аналізу ретроспективи інформаційного простору, так і шляхом оперативного моніторингу в режимі реального часу (за наявності високотехнологічних моніторингових систем). Ця модель є простою в реалізації, але при цьому розпізнавання інформаційної операції відбувається вже на кінцевих стадіях її проведення [4].

Так, наприклад, науковці Ю. В. Наконечна, А. Б. Качинський розглядають також SIR-модель, яка є класичною віральною моделлю поширення інфекції в межах популяції залежно від часу. Для процесу поширення інформації застосовують наступне:

S – агенти мережі (користувачі), які не отримали інформаційне повідомлення,

I – отримали повідомлення та вважають надану в ньому інформацію актуальною,

R – забули новину/втратили до неї інтерес.

Так, дану модель було застосовано для моделювання інформаційних впливів на основі даних, отриманих з новинного порталу УНІАН. Аудиторія каналу становить понад 200 тис. Підписників у Facebook, та активну щоденну аудиторію ресурсу близько 9 тис. чоловік, з яких 1428 переглянули новину про відсутність депутатів на своїх робочих місцях 06.04.18. Зважаючи на популярність цієї новини станом на день публікації, було обрано відповідні параметри моделі [5].

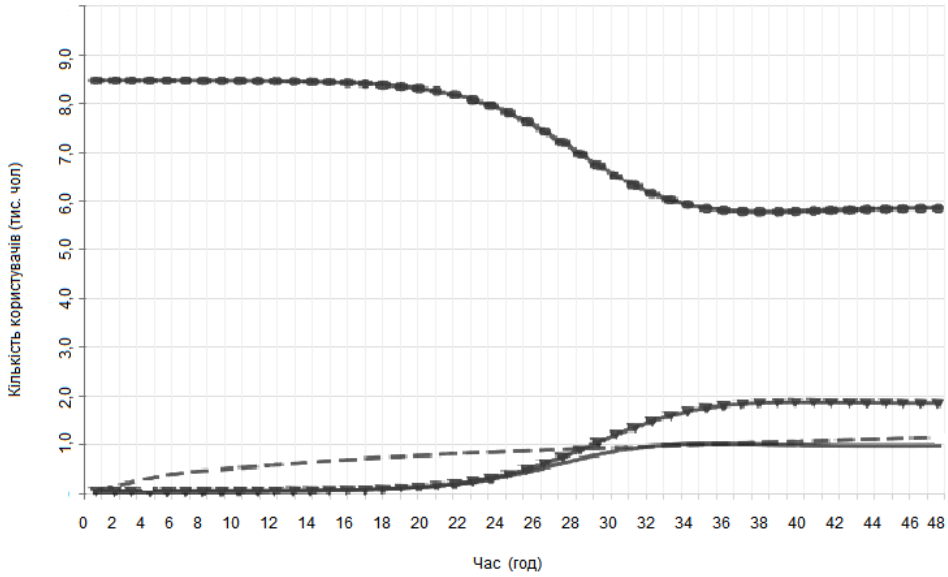

Рис. 2. Приклад структури поширення повідомлення на задану тему

За висновками авторів, розширена модель SIR дає змогу оцінити охват аудиторії, але не відповідає реальності стосовно відображення динаміки поширення новини у часі, а також наявність параметра «забування» робить використання моделі складнішим, адже оцінка швидкості переходу новини у неактуальний стан є комплексним показником та потребує експертної оцінки [5].

Аналізуючи інформаційні операції, які проводить агресор в інформаційному просторі, слід зазначити, що основним середовищем поширення деструктивного контенту стали соціальні медіа, які спираються на новітні цифрові технології, інтерактивність та комбінування різних форм представлення інформації, наприклад текстової, звукової і графічної, анімації та відео. Такі нові медіа як канали месенджера Telegram, соціальні мережі Instagram, Facebook та Twitter мають багатомільйонні цільові аудиторії, швидкість і горизонтальність розповсюдження контенту. Вони, по-перше, дають можливість проводити інформаційні операції за кардинально різними схемами та планами, що ускладнює їх виявлення, а отже, робить неефектним протидію, по-друге, не дають можливості напрацювати чіткі шаблони для організації превентивних заходів.

Власний практичний досвід та досвід зарубіжних партнерів, таких як Трансатлантична комісія з чесних виборів при Альянсі Демократій, які аналізують інформаційні операції в соціальних мережах, показав, що особливо масово при цьому використовується соціальна мережа Twitter, контент якої містить як деструктивний посил, так і маніпулятивні технології для прихованого впливу на суспільну свідомість. Приклади таких втручань зафіксовано під час загальнодержавних виборів в Італії та Мексиці у 2018 році, на референдумі щодо зміни назви в Македонії у 2018, парламентські та президентські вибори в Україні у 2019. На рисунку 3 наведено приклад кластеризації та сегментації акаунтів-ботів в соціальній мережі Twitter, які використовувалися РФ для проведення інформаційних операцій.

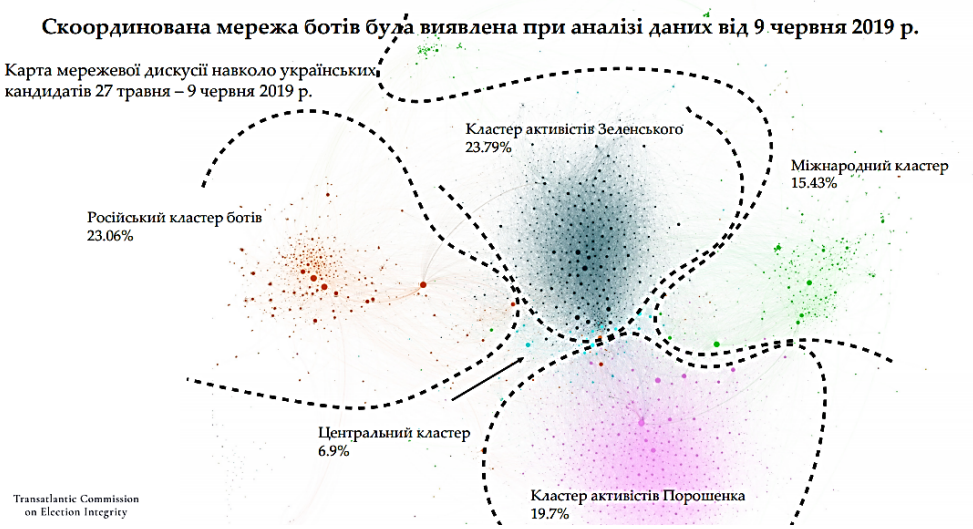

Рис. 3. Приклад кластеризації *та сегментації акаунтів-ботів у соціальній мережі Twitter з подальшим використанням цих кластерів для проведення інформаційних операцій РФ*

Враховуючи динамічне середовище соціальних мереж, а також динамічні соціальні процеси в інформаційній сфері, інформаційні операції неможливо описати аналітичними математичними методами та побудувати модель розповсюдження контенту в часі, яка б була деяким прототипом інформаційної операції. Для цього пропонується розглянути методи імітаційного моделювання.

Незважаючи на те, що аналіз соціальних мереж сам по собі є складною науково-технічною задачею, моделювання поширення інформації дозволяє досліджувати відповідні інформаційні процеси, виявляти закономірності, які можуть використовуватись як при вивченні механізмів передачі інформації у таких мережах, так і рівня її впливу на людей.

Тому для моделювання інформаційних операцій в соціальних мережах пропонується розглянути відносно новий вид імітаційного моделювання – агентне моделювання (agent – based modelingand simulation – ABMS). Саме агентне моделювання дозволяє зімітувати ті соціальні процеси та поведінку користувачів, які відбуваються в цих нових медіа.

Можна виділити основну особливість цього методу, що складається в такому: будуються сценарії можливих варіантів розвитку подій у майбутньому, на підставі чого формуються, а потім відбираються стратегічні альтернативи, які працюють у кожному сценарії та служать підставою для прийняття рішень про вибір інтегрованої стратегії. Агентний підхід дозволяє проводити багатоваріантний ситуаційний аналіз системи, що моделюється. Сутність агентного підходу при побудові сценаріїв полягає в побудові середовища активних агентів, визначення алгоритмів їхнього функціонування та взаємодії, виявлення нових закономірностей, зв'язків, когнітивних зв'язків, а також комплексу математичних моделей формування сценаріїв на комп'ютерному моделюючому комплексі [6].

В імітаційній агентній моделі її складові – агенти – функціонують незалежно один від одного та від системи загалом. Вони діють за своїми законами, на основі яких й формуються загальні правила функціонування системи загалом, тобто побудова моделі «від низу до верху».

Для створення агентної моделі поширення інформації, перш за все, необхідно сформувати близький до реальності віртуальний інформаційний простір, «населений» віртуальними агентами. При побудові агентної моделі однією з основних задач є визначення взаємодії агентів між собою, яким чином дані агенти формуються (виникають), що впливає на передачу інформації від одного агенту до іншого, якою може бути динаміка цієї передачі [6].

За практичним аналізом соціальної мережі Twitter на прикладі розповсюдження повідомлень із хештегом #LightOnZelenskyyOff встановлено, що більшість акаунтів, з яких здійснювалося вкидання, є ботами, що підтверджено за рахунок ПЗ Botometer. А модель поширення виглядає таким чином.

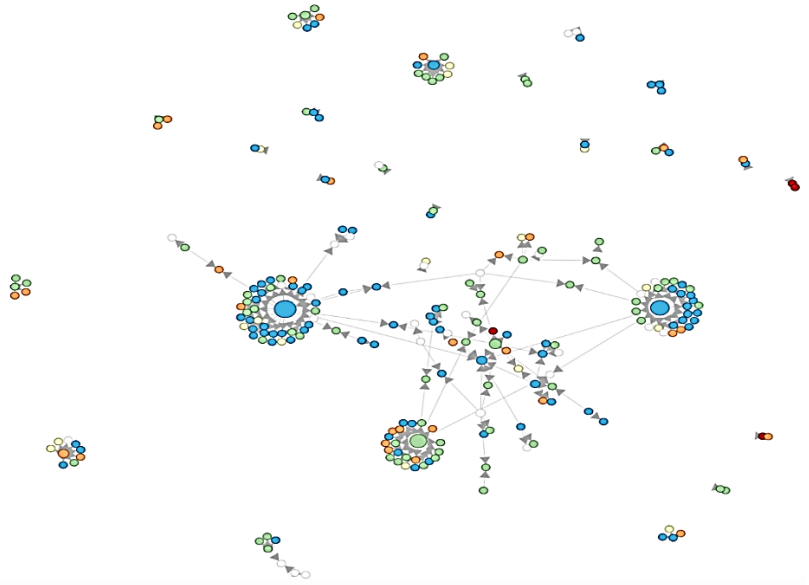

Рис. 4 Приклад моделі поширення вірусного контенту акаунтами-ботів у соціальній мережі Twitter з хештегом #LightOnZelenskyyOff

Аналізуючи типи віртуальних агентів в соціальних мережах в рамках побудови моделі, можна визначити наступні:

– першоджерело – **перший тип агентів**, які публікують контент для подальшої популяризації;

– акаунти–боти – **другий тип агентів** (бот — це спеціальна програма, що виконує автоматично і за заданим розкладом певні дії через ті ж інтерфейси, що й звичайний користувач) – використовуються для штучного нарощування «лайків» чи коментарів з метою підняття рейтингу публікації серед користувачів мережі, дають змогу посилити вплив у інформаційному середовищі шляхом залучення нових цільових аудиторій (бот поширює новину, але майже нічого не змінює, він на відміну від троля є механічним, троль – креативним);

– акаунти-тролі – **третій тип агентів** – звичайна дійова особа, яка надає кольорового забарвлення новинам. Вони оперують великими групами і подають новину з різних ракурсів. За цим типом агентів можуть знаходитись блогери, лідери думок, які репостять «вірусний» контент на власні сторінки, тим самим одразу (в один клік) збільшуючи потенційні цільові аудиторії (перегляди, лайки, репости) в рази;

– **четвертий тип агентів** – реальні люди, які є потенційною цільовою аудиторією інформаційної операції, вони «споживають» контент та сприймають його достовірним, тобто підпадають під інформаційний та психологічний вплив і стають «інфікованими» даним контентом, вірять, що інформація правдива та популяризують її далі в мережі, базуючись на своїй вірі.

Передбачається, що агенти в соціальній мережі можуть

1) самозароджуватися;
2) породжувати нових агентів шляхом репостінгу (repost);
3) «вмирати» — зникати з простору агентів (припинити передавати контент);
4) отримувати лайки (like) від інших агентів.

Після появи «вірусного» контенту в акаунті першоджерела, різні типи агентів починають безперервно взаємодіють один з одним, та передавати інформацію (репост) за такими алгоритмами:

- від одного агенту до іншого – взаємодія між четвертим типом агентів;

- від одного агенту до групи агентів – взаємодія між третім та четвертим типом агентів, між першим та четвертим типом агентів та між другим та четвертим типом агентів;

- від однієї групи агентів до іншої – взаємодія між другим типом агентів

Характер зв'язків між агентами може бути як прямим, так і зворотним.

У такій системі рішення задачі можуть формуватися за рахунок взаємодії великої кількості агентів, що безперервно взаємодіють один з одним, а також формується колективна поведінка.

У результаті виділення типових агентів – акаунтів-користувачів – в соціальній мережі, виявлення закономірностей їх взаємодії та притаманних даним агентам характеристик, стає очевидним, що така умовна інформаційна система не належить до формальних моделей, є неоднорідною, а поведінка її елементів – акаунтів користувачів – нераціональною. Саме в таких випадках, коли інформаційна система є децентралізованою та не діє за глобальними правилами й законами, а навпаки, ці глобальні правила і закони є результатом індивідуальної активності членів групи, слід застосовувати агентний підхід.

Висновки. На сьогодні є очевидним, що пошук дієвих механізмів протидії інформаційним операціям є надзвичайно актуальним і важливим завданням. При цьому в своїй більшості запропоновані моделі виявлення націлені не на алгоритми розповсюдження, а на аналіз контенту, та як середовище розглядаються в більшості своїй електронні ЗМІ. Водночас на практиці доведено, що найбільш задіяним середовищем для проведення інформаційних операцій є соціальні мережі. Це нелінійне динамічне середовище, яке не можливо зарегламентувати чи описати чіткими математичними формулами. Для такого середовища запропоновано використання агентної парадигми для моделювання інформаційних операцій.

Особливістю даної парадигми є багаторівнева абстракція опису процесу поширення інформаційних матеріалів у соціальних мережах, а також можливість у подальшому застосувати отримані результати до широкого класу аналогічних інформаційних ресурсів мережі Інтернет.

Застосування цього підходу дозволяє здійснити перехід від реального процесу розгортання інформаційної операції до її формальної моделі, у межах досліджень якої з'являється можливість прогнозувати властивості поведінки інформаційного процесу поширення інформації.

Список використаних джерел

1. Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави в соціальних інтернет сервісах : дис. … д-ра техн. наук / К. Молодецька-Гринчук. – Житомир, 2018. – 368 с.

2. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – Київ : Інтертехнологія, 2009. – 164 с.

3. Якименко Н. М. Важливість дослідження та моделювання інформаційних операцій в умовах інформаційної війни та кібервійни / Н. М. Якименко // Актуальні задачі та досягнення у галузі кібербезпеки : зб. матеріалів Всеукраїнської науково-практичної конференції. – 2016. – С. 207-209.

4. Додонов В. О. Мультиагентний підхід до моделювання інформаційно-аналітичної системи / В. О. Додонов, Д. В. Ланде, В. Г. Путятін // Інформаційно-аналітичні системи обробки даних. – 2016. – Т. 18, № 2. – С. 22- 24.

5. Наконечна Ю. В. Математичні моделі динаміки поширення інформації в соціальних медіа / Ю. В. Наконечна, А. Б. Качинський // Математичні методи комп'ютерного моделювання та кібернетичної безпеки. – Київ, 2018. – С. 37-39.

6. Распознавание информационных операций: мультиагентный подход, Open Semantic Technologies for Intelligent System / А. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук, С. В. Каденко, А. Н. Грайворонская. – Киев : ООО «Инжиниринг», 2017. – 282 с.

References

1. Molodetska-Hrynchuk, K. (2018). *Metodolohiia pobudovy systemy zabezpechennia informatsiinoi bezpeky derzhavy v sotsialnykh internet servisakh [Methodology of building a system for ensuring state information security in social Internet services]*. [Doctor dissertation, Zhytomyr].

2. Horbulin, V.P., Dodonov, O.H., & Lande, D.V. (2009). *Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia [Information operations and social security: threats, countermeasures, modeling]*. Intertekhnolohiia.

3. Yakymenko, N.M. (2016).Vazhlyvist doslidzhennia ta modeliuvannia informatsiinykh operatsii v umovakh informatsiinoi viiny ta kiberviiny [The importance of research and modeling of information operations in the conditions of information warfare and cyber warfare]. *Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky: zb. materialiv Vseukrainskoi naukovo-praktychnoi konferentsii – Actual problems and achievements in the field of cyber security: Collection. materials of the All-Ukrainian Scientific and Practical Conference* (pp. 207-209).

4. Dodonov, V.O., Lande, D.V., & Putiatin, V.H. (2016). Multyahentnyi pidkhid do modeliuvannia informatsiino-analitychnoi systemy [Multi-agent approach to information and analytical system modeling]. *Informatsiino-analitychni systemy obrobky danykh – Information and analytical data processing systems, 18*(2), 22- 24.

5. Nakonechna, Yu.V., Kachynskyi, A.B. (2018). Matematychni modeli dynamiky poshyrennia informatsii v sotsialnykh media [Mathematical models of the dynamics of information dissemination in social media]. Matematychni metody kompiuternoho modeliuvannia ta kibernetychnoi bezpeky – Mathematical methods of computer modeling and cyber security (pp. 37-39).

6. Dodonov, A.H., Lande, D.V., Tsyganok, V.V., Andreichuk, O.V., Kadenko, S.V., & Hraivoronskaia, A.N. (2017). *Raspoznavanie informatsionnykh operatsii: multiagentnyi podkhod, Open Semantic Technologies for Intelligent System [Recognition of information operations: multi-agent approach, Open Semantic Technologies for Intelligent System]*. OOO «Inzhyniryng».

Отримано 30.06.23

UDC 004.738.5:351

Olha Vasylieva
graduate student
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: olga.vasiljeva37@gmail.com. **ORCID:** https://orcid.org/0000-0001-8263-782X

MODELS FOR DETECTING AND FORECASTING THE DYNAMICS OF INFORMATION OPERATIONS IN SOCIAL NETWORKS

The article examines some provisions for conducting information operations as one of the main threats to national security in the information sphere, demonstrates the use of social networks as the main field for conducting them thanks to the latest technologies, and analyzes the proposed models of information operations in social networks.

The article is devoted to the problem of the complex application of theoretical models used in the study of "viral" information dissemination in social networks of cyberspace.

Formal modeling, which is used to study the peculiarities of communication in social networks, is analyzed.

Three components of formal models of online message distribution in social networks are distinguished: typology of messages, network model, formal model of signal distribution.

Special attention is paid to the possibilities of applying non-linear models of information dissemination.

It is proposed to use a relatively new type of simulation modeling - agent-based modeling and simulation (ABMS) for modeling information operations in social networks. It is agent modeling that allows you to simulate those social processes and user behavior that occur in these new media. The main feature of agent modeling is building scenarios of possible options for the development of events in the future, on the basis of which strategic alternatives, which work in each scenario and serve as a basis for making decisions about choosing an integrated strategy are formed and then selected. The agent approach allows for multivariate situational analysis of the modeled system. The essence of the agent approach in building scenarios consists in building an environment of active agents, determining the algorithms of their functioning and interaction, identifying new patterns, connections, cognitive connections, as well as a set of mathematical models for the formation of scenarios on a computer simulation complex.

The types of virtual agents in social networks are distinguished: primary source, bot accounts, troll accounts, real people.

***Keywords**: modeling; information operations; national security in the information sphere; social networks; dynamic environment.*

Fig.: 4. References: 7.

Васильєва О. Моделі виявлення та прогнозування динаміки інформаційних операцій у соціальних мережах. *Технічні науки та технології.* 2023. № 2(32). С. 193-200.