УДК 004.056
DOI: 10.31673/2409-7292.2021.020102

Бобровський О.О., Опанасенко М.І., Дзюба Т.М.

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ВІРТУАЛЬНИХ СПІЛЬНОТ В СОЦІАЛЬНИХ МЕРЕЖАХ

Статтю присвячено розгляду актуального питання виявлення інформаційних загроз у віртуальних спільнотах соціальних мереж та механізмам протидії таким загрозам. Досліджено процес організації моніторингу та контент-аналізу віртуальних спільнот у соціальних мережах. Розроблено технологію виявлення інформаційних загроз віртуальних спільнот у соціальних мережах та методи їх оцінки. Запропоновано підхід щодо пошуку сторінок дискусій у соціальних мережах на базі Лувенського методу. Розроблено технологію визначення ступеня інформаційної загрози віртуальної спільноти в соціальних мережах та способи протидії інформаційним загрозам віртуальної спільноти.

Ключові слова: віртуальна спільнота, соціальна мережа, моніторинг, інформаційно-психологічний вплив.

Вступ

В сучасному інформаційному суспільстві відбувається зародження і становлення соціальних формацій – віртуальних спільнот (ВС), з принципово іншими (порівняно з традиційними формами впливу на соціальні структури в індустріальному суспільстві) можливостями з надання впливу на традиційні громадські та державні структури, поява яких пов’язана з програмами створення оперативного доступу через канали відкритих телекомунікаційних мереж до розподілених інтелектуальних і матеріальних ресурсів у будь-якій точці земної кулі. Багато в чому поява таких віртуальних спільнот пов’язана з проведенням телекомунікаційної глобалізації..

Постановка проблеми

Поряд з конструктивними віртуальними спільнотами, які прагнуть активно взаємодіяти з суспільством, маючи на меті поліпшення життя як суспільства загалом, так і окремих соціальних груп та індивідів, соціальні мережі все частіше використовують для створення деструктивних віртуальних спільнот. Деструктивні віртуальні спільноти, на відміну від конструктивних, намагаються з цим співтовариством боротися усілякими, не завжди законними, методами. Вони створюють нові загрози, оскільки держава вже не здатна контролювати їх у повному обсязі через особливості їх функціонування у соціальних мережах. Саме тому, створення технічних та програмних засобів для виявлення та протидії деструктивному впливу інформаційному наповненню віртуальних спільнот у соціальних мережах є найактуальнішим.

Мета дослідження: розроблення методів і засобів виявлення та оцінки інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж.

Для досягнення цієї мети в роботі необхідно вирішити такі **завдання**:

1) проаналізувати віртуальні спільноти у соціальних мережах з точки зору можливих суб’єктів інформаційної безпеки;

2) сформувати технологію виявлення інформаційних загроз віртуальних спільнот у соціальних мережах та методи їх оцінки.

Аналіз віртуальних спільнот в World Wide Web

На сьогоднішній день соціальні мережі та віртуальні спільноти – це середовище з практично миттєвою швидкістю поширення інформації і досить сильним ефектом пам'яті (вміст багатьох соціальних ресурсів індексується пошуковими системами і є доступним матеріалом). Крім того, з кожним роком стрімко зростає індекс довіри до цих джерел інформації. Віртуальні спільноти набирають популярності серед молодих людей віком від 12 до 25 років, але за останні роки вік учасників-користувачів соціальних мереж стає все більшим. Вони виникають і функціонують в електронному просторі з метою сприяння вирішенню своїх професійних, політичних завдань, задоволення своїх потреб у мистецтві, дозвіллі тощо [1, 2].

Процес функціонування віртуальних спільнот у соціальних мережах має певні особливості:

отримати доступ до інформації в дискусіях соціальних мереж може лише зареєстрований користувач соціальних мереж, а в закритих дискусіях – тільки учасник дискусії;

значна частина відвідувачів потрапляє на сайт за безпосередньою рекомендацією інших користувачів;

взаємопов'язаність сторінок дискусій;

анонімність або спотворення даних про себе самими користувачами соціальних мереж.

Основним інструментом, що використовується у віртуальних спільнотах деструктивного характеру, є інформаційно-психологічний вплив, який передбачає цілеспрямоване розроблення та поширення спеціальної актуальної інформації, здатної справляти безпосередній або непрямий вплив на суспільну свідомість, психологію і поведінку населення. Серед основних завдань, що можна вирішити за допомогою віртуальних спільнот у соціальних мережах виділяють такі [3]:

створення чи посилення опозиційних угруповань чи рухів;

створення атмосфери бездуховності та аморальності, негативного ставлення до культурної спадщини;

маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни задля створення політичної напруженості та хаосу;

дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою розпалювання недовіри, посилення підозрілості, загострення політичної боротьби, провокування конфліктів, репресій проти опозиції, взаємознищення;

провокування соціальних, політичних, національних та релігійних зіткнень;

дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

ініціювання страйків, масових заворушень та інших акцій економічного протесту;

ускладнення прийняття органами управління важливих рішень;

погіршення міжнародного авторитету держави, її співпраці з іншими країнами;

підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу.

Організація моніторингу та контент-аналізу віртуальних спільнот у соціальних мережах

Сьогодні вже розроблена велика кількість спеціального програмного забезпечення щодо моніторингу та контент-аналізу інтернет середовища. Розроблені автоматизовані системи класифікації та аналізу інтернет текстів основані, як правило, на співвіднесенні текстового фрагмента з наперед складеними тональними словниками. За сукупністю виявленої емотивної лексики текст оцінюють як позитивний чи негативний. Однак, інформаційне наповнення сторінок дискусій віртуальних спільнот у соціальних мережах генерується безпосередньо користувачами соціальних мереж з його особливостями:

неусталений порядок слів у реченні;

велика кількість розмовної та ненормативної лексики з найнесподіванішими контекстуальними значеннями;

двозначність гумору, який зрозумілий з аналізу підтекстів і діалогів, але не з фактичного словникового сенсу сказаного, до якого може звернутися автоматизована система.

Отже, можна зробити висновок, що сьогодні доволі адекватної та ефективної автоматизованої системи аналізу інтернет-контенту не існує. Іншим суперечливим питанням щодо аналізу віртуальних спільнот є невизначеність оцінки інформаційної загрози віртуальної спільноти. У дослідженнях показником інформаційної загрози є кількісна динаміка, що характеризується як кількість подій за одиницю часу або кількість повідомлень пов'язаних з їхнім інформаційним наповненням. Це визначення інформаційної загрози

підходить для аналізу інформаційних новинних інтернет ресурсів як оцінка інтенсивності публікацій за відповідною тематикою.

Технологія виявлення інформаційних загроз віртуальних спільнот у соціальних мережах та методи їх оцінки

Відомо [4, 5], що в основу функціонування усіх ВС покладено феномен соціальної мережевої комунікації. При цьому актори в ВС є вузлами зв'язку, а відношення між ними – каналами передачі інформації. Таким чином, віртуальна спільнота акторів у ВС представляє собою систему вузлів, зв'язаних між собою каналами передачі інформації. Можна припустити, що зв'язки між акторами є горизонтальними, тому усі вузли ВС є рівноправними. Оскільки актори можуть встановлювати зв'язки з іншими акторами або віртуальними спільнотами, то можна стверджувати про розподілений характер зв'язків між вузлами. У загальному вигляді взаємодія акторів у ВС подана на рис. 1.

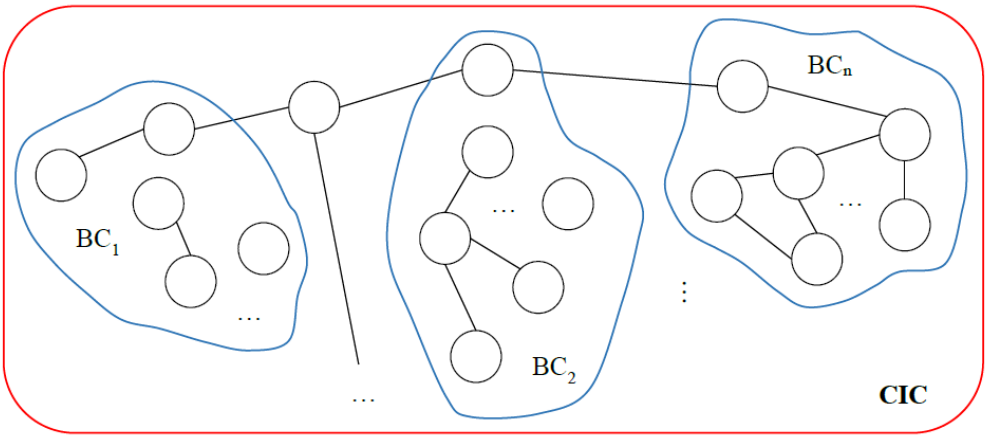

Рис. 1. Принцип організації взаємодії акторів у ВС

На рис. 1 актори позначені кружками, а відповідні взаємозв'язки між ними – лініями. У свою чергу, актори можуть об'єднуватися у віртуальні спільноти $BC_i, i = \overline{1,n}$.

Аналіз принципів організації взаємодії акторів у ВС (рис. 1) дозволяє зробити такий висновок: актори, об'єднавшись у віртуальні спільноти в ВС суттєво пришвидшують обмін інформацією, яка після її сприйняття свідомістю акторів відображується у вигляді зміни їх поведінки у реальному житті. Встановлено, що відомі підходи до класифікації ВС мають обмежений характер і визначаються можливістю їх практичного застосування в тій чи іншій галузі, роллю у формуванні громадянського суспільства, психологічними аспектами взаємодії акторів тощо.

Результати аналізу різноманіття сучасних ВС показали, що вони динамічно розвиваються і вдосконалюються [6-11]. Використання спільних принципів, покладених в основу їх функціонування, дозволило розробити узагальнену класифікацію ВС із застосуванням ознакового принципу на основі ієрархічного підходу [12]. Перевагами ієрархічної класифікації є простота, логічність побудови і висока інформаційна ємність, а жорсткість її структури забезпечує чітке віднесення окремого ВС до виділених функціональних ознак [13, 14]. За функціональним призначенням розрізняють такі СІС:

1) соціальні пошукові системи (social search) – це сервіси, які дозволяють акторам самостійно визначати пріоритетні напрямки пошуку контенту, задавати ключові слова, обирати джерела контенту і форму подання результатів [9];

2) соціальні закладки (social bookmark) – централізована онлайн-служба, яка дозволяє акторам додавати, анотувати, редагувати і обмінюватися закладками, використовуючи теги [9, 11]. До соціальних закладок відносять Blinklist, Delicious, BlogBookMark, Clipclip, Cloudytags;

3) вікі (Wiki) – інтернет-сервіс, побудований на основі технології створення колекції зв'язаних між собою записів, які можуть створювати і редагувати усі актори. Зміни публікацій зберігаються на сторінці історії для аналізу та управління, встановлення їх авторства. Найбільш популярними є сервіси Wikipedia, PPbworks, SocialText, MediaWiki, Wiki;

4) блоги (blog) використовуються для публікації дискретних повідомлень та їх обговорення. Такі повідомлення з'являються в СІС у зворотному хронологічному напрямку – останні публікації відображаються першими. Зазвичай блоги ведуться актором індивідуально, в окремих випадках – невеликою групою і часто присвячені деякій обраній тематиці. Сьогодні блоги можуть бути багатоавторськими і професійно відредагованими. На ринку сервісів блоги представлені такими СІС – Живой Журнал, Blogger, Wordpress, Edublogger та іншими;

5) соціальні медіа-сховища (social media hubs) призначені для зберігання, класифікації і обміну цифровими фотографіями, аудіо- та відеозаписами, текстовими файлами, презентаціями й обговорення цих ресурсів. Залежно від типу контенту соціальні медіа-сховища поділяють на такі:

для розміщення фотографій, схем, рисунків, а саме Flickr, Flamber, Panoramio, Instagram;

відео, наприклад Youtube, Vimeo, Wistia, Brightcove;

публікації аудіозаписів – iTunes Store, Last.fm, Spotify, SoundCloud;

презентації – Sladeshare, Spresent;

публікація текстових даних, наприклад книжок у Scribd;

6) карти знань (mind map) – це СІС для представлення задач, тезисів, ідей, об'єднаних єдиною концепцією у вигляді діаграм і графіків. Часто використовуються для візуалізації середовища взаємодії акторів. До карт знань відносять FreeMind, MindMeister, Zoho, Bubble, Mindomo.

7) соціальна мережа (social network) – це СІС, який ґрунтується на соціальній структурі, складається з множини соціальних суб'єктів (акторів чи організацій), набору діадних зв'язків та інших соціальних взаємодій між ними. Контент соціальної мережі формується безпосередньо акторами, з можливістю вказати дані про себе для подальшого створення контактів з іншими суб'єктами. До майданчиків на базі соціальних мереж належать Facebook, Vkontakte, LinkedIn, Одноклассники тощо.

Для управління взаємодією акторів та їх віртуальних спільнот у СІС використовуються спеціальні засоби управління. Вони надають інструментарій для модерації, підтримки комунікації між акторами, формування контенту і програмування алгоритмів його публікації, планування залучення та утримання учасників віртуальної спільноти, аналізу зв'язків, розробки стратегій досягнення поставлених цілей і задач тощо. До таких соціальних площадок належать Mzinga, Telligent, LifeRay, Jive.

8) соціальні геосервіси (social map) – СІС, які забезпечують акторів засобами ідентифікації, коментування, доповнення фотографіями об'єктів на карті. Для функціонування соціальних геосервісів використовуються реальні дані, отримані за допомогою навколоземних супутників. Прикладами таких СІС є Google Maps, Google Earth, Yahoo!Maps;

9) мешап (mesh up) об'єднує функції декількох СІС і забезпечує інтеграцію їх контенту, в результаті чого утворюється новий унікальний сервіс. Наприклад, об'єднання картографічних даних Google Maps і даних сайту продажу нерухомості. Сьогодні відрізняють такі типи мешапів: користувацькі, даних і бізнес-мешап. Серед популярних сервісів виділяють Serena Business Manager, If This Then That.

Пошук сторінок дискусій у соціальних мережах

Пошук сторінок дискусій здійснюється інструментами соціальних мереж за назвами дискусій або за їх коротким змістом, що не завжди відповідає інформаційному наповненню цих сторінок.

Внаслідок цього виникла проблема, пов'язана з пошуком потрібної інформації на сторінках дискусій у соціальних мережах, яка значно ускладнюється необхідністю проведення пошуку відповідно до тематики інформаційного наповнення та актуальності сторінки дискусії з урахуванням особливостей функціонування сторінок дискусій у соціальних мережах, а саме:

сторінки мають низький ранг в алгоритмах ранжування сторінок;

велику кількість web-сторінок дискусій не ранжують глобальні пошукові системи;

взаємопов'язаність web-сторінок дискусій;

збереження дискусій неактуальної тематичної спрямованості.

Останнім часом робляться численні спроби розробити ефективний алгоритм для виявлення спільнот в соціальних мережах з мільйонів вузлів, які неможливо візуалізувати або аналізувати на рівні окремих вузлів. Бельгійські розробники представили новий алгоритм, який перевершує всі існуючі аналоги по обчислювальної швидкості. Він отримав назву Лувенский метод (Louvain Method, рис. 2).

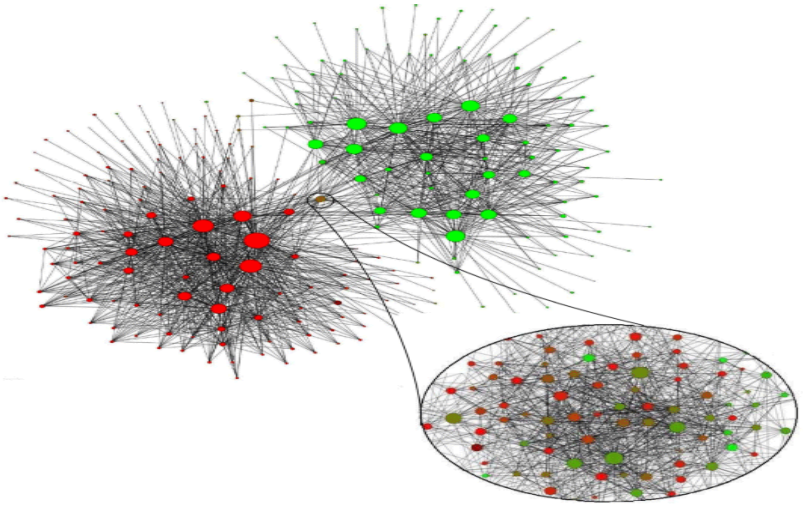

Рис. 2. Результат аналізу бази абонентів в мережі бельгійського оператора стільникового зв'язку. Червоним кольором відзначені спільноти, які розмовляють французькою мовою, зеленим - голандською.

Метод складається з двох стадій (рис. 3). На першій відбувається пошук «малих» спільнот шляхом оптимізації модульності на локальному рівні. На другій стадії вузли одного співтовариства агрегуються і будується нова мережа більшого масштабу, після чого ці стадії повторюються до тих пір, поки не буде досягнутий максимальний рівень модульності. Таким чином, після кожного етапу програма відображає спільноти все більшого масштабу.

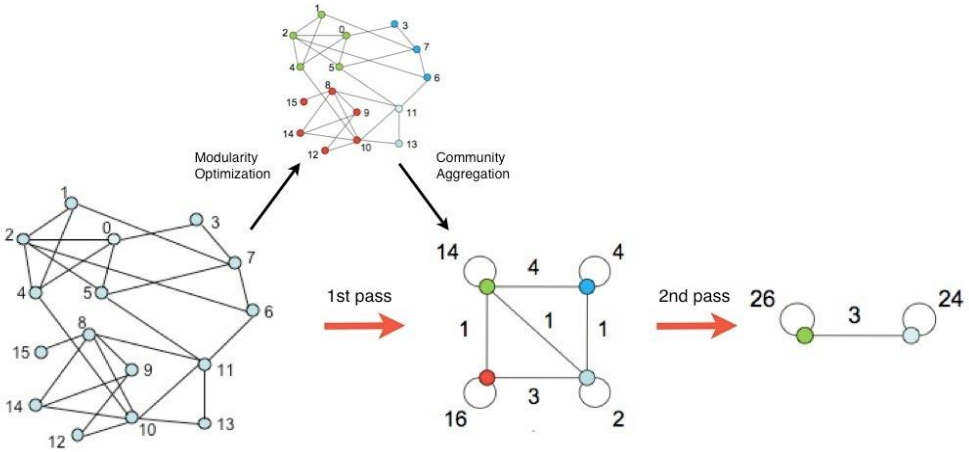

Рис. 3. Дві стадії Лувенського методу

Визначення ступеня інформаційної загрози віртуальної спільноти в соціальних мережах

Для визначення ступеня інформаційної загрози використовуються показники інформаційної загрози віртуальної спільноти, які розраховуються відповідно до виразу за підходами щодо визначення критичної цінності віртуальної спільноти, а саме:

$InfThreat_{CritMembers}(VirtualCommunity)$ – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти основане на встановленні експертами кількості учасників віртуальної спільноти, за якої реалізовується інформаційна загроза, без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті, а саме – умови виникнення загрози з моделі загроз; розраховується показник;

$InfThreat_{InfConfr}(VirtualCommunity)$ – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти основане на загальній кількості учасників деструктивної та конкурентної віртуальних спільнот, які зацікавлені цією тематикою з урахуванням якості інформаційного наповнення та структури зв'язків дискусій у цих віртуальних спільнотах .

Для визначення рекомендацій щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот розглянемо графіки змін показників інформаційної загрози залежно від кількості учасників деструктивної та конкурентної віртуальних спільнот.

На рис. 4 видно, що в разі збільшенні кількості учасників деструктивної віртуальної спільноти збільшується показник *InfThreat CritMember s* (*VirtualCommunity*).

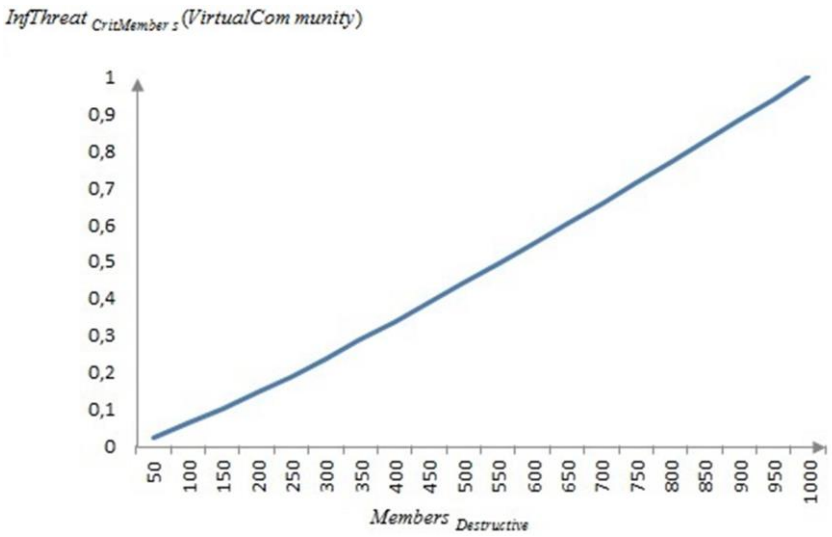

Рис. 4. Зміна *InfThreat CritMember s* (*VirtualCommunity*) залежно від кількості учасників деструктивної віртуальної спільноти

Якщо відсутня конкурентна віртуальна спільнота, то за малої кількості учасників деструктивної віртуальної спільноти *InfThreat InfConfr* (*VirtualCommunity*) = 1, що необхідно врахувати, приймаючи рішення щодо протидії інформаційним загрозам віртуальних спільнот.

Таким чином, ступень інформаційної загрози залежить від

$$InfThreat_{CritMembers}(VirtualCommunity) \text{ та } InfThreat_{InfConfr}(VirtualCommunity):$$

$$InfThreat = 1 - f(InfThreat_{CritMembers}(VirtualCommunity), InfThreat_{InfConfr}(VirtualCommunity))$$

Враховуючи, що показники $InfThreat_{CritMembers}(VirtualCommunity)$ та $InfThreat_{InfConfr}(VirtualCommunity)$ мають значення в межах [0, 1] тобто не потребують нормування, ступень інформаційної загрози з урахуванням цих показників визначимо за виразом:

$$InfThreat = 1 - (InfThreat_{InfConfr}(VirtualCommunity) + InfThreat_{CritMembers}(VirtualCommunity)), \quad (1)$$

Враховуючи визначення ступеня інформаційної загрози (1) він буде приймати значення в межах [1, –1]. При значенні $InfThreat \leq 0$ приймається рішення щодо протидії інформаційним загрозам віртуальної спільноти.

Рішення щодо протидії інформаційним загрозам віртуальної спільноти, наведені у табл. 1.

Таблиця 1

Значення показників інформаційної загрози

Значення *InfThreat*	Опис	Результат
InfThreat = 0	Деструктивна віртуальна спільнота має достатню кількість учасників для реалізації інформаційної загрози та перевагу в інформаційному протиборстві з конкурентною віртуальною спільнотою	Необхідно протидіяти інформаційній загрозі.
	Значення показника $InfThreat_{InfConfr}(Virtual\ Community) = 1$ свідчить про відсутність конкурентної віртуальної спільноти щодо тематики інформаційного наповнення деструктивної віртуальної спільноти	Необхідно здійснювати вплив на інформаційне наповнення деструктивної віртуальної спільноти та проводити заходи щодо створення конкурентної.
	Якщо значення показника $InfThreat_{InfConfr}(VirtualCommunity) = 0$ це вказує на відсутність деструктивної віртуальної спільноти.	Ведення постійного моніторингу.
InfThreat > 0	$InfThreat_{CritMembers}(VirtualCommunity) > 1$ та $InfThreat_{InfConfr}(VirtualCommunity) > 1$ кількість учасників деструктивної віртуальної спільноти достатня для реалізації інформаційної загрози та спільнота має рівну перевагу в інформаційному протиборстві.	Необхідно протидіяти інформаційній загрозі.
InfThreat <0	Кількість учасників деструктивної віртуальної спільноти не достатня для реалізації інформаційної загрози, але спільнота має значну перевагу в інформаційному протиборстві з конкурентною віртуальної спільнотою.	Ведення постійного моніторингу щодо збільшення кількості учасників деструктивної віртуальної спільноти.
	Якщо значення показника $InfThreat_{CritMembers}(VirtualCommunity) < 0{,}5$	Ведення постійного моніторингу щодо збільшення кількості учасників деструктивної віртуальної спільноти.
	Якщо значення показника $InfThreat_{InfConfr}(Virtual\ Community) < 1$, це вказує на відсутність конкурентної віртуальної спільноти відносно тематики інформаційного наповнення деструктивної віртуальної спільноти.	Ведення постійного моніторингу щодо збільшення кількості учасників та вживання заходів для створення конкурентної віртуальної спільноти.
	Якщо значення показників $InfThreat_{CritMembers}(VirtualCommunity) < 0$ та $InfThreat_{InfConfr}(Virtual\ Community) < 1$, це свідчить про створення нової або руйнування існуючої деструктивної віртуальної спільноти.	Ведення постійного моніторингу щодо сценарію розвитку деструктивної віртуальної спільноти.

Таким чином запропоновано метод прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот.

Висновки

Незважаючи на ті переваги, які надають віртуальні спільноти, пов'язані, перш за все, з можливістю оперативної дистанційної взаємодії між людьми, є значна кількість проблем, які потребують негайного вирішення. Основною проблемою є відсутність чіткого правового регулювання відносин у віртуальному просторі нашої держави, відсутність єдиного і завершеного механізму протидії деструктивному інформаційно-психологічному впливу Інтернету в цілому та соціальних мереж зокрема на масову свідомість з боку державних органів. Використання віртуальних спільнот іноземними державами, терористичними і екстремістськими організаціями з метою реалізації операцій інформаційної війни є незаперечним фактом і становить серйозну загрозу для національної безпеки, що в черговий раз підтверджує актуальність розглянутої теми і викликає необхідність проведення подальших досліджень в даній області.

Розроблена технологія виявлення інформаційних загроз віртуальних спільнот у соціальних мережах дає можливість визначати потенційно-небезпечні угруповання у мережі та реалізовувати доцільні сценарії протидії таким впливам.

Перелік посилань

1. Иванов Д. В. Виртуализация общества. Версия 2.0 / Д. В. Иванов. – С-Пб.:Петербургское востоковедение, 2002. – 224 с.

2. Пелещишин А. М. Веб 2.0 – другий шанс для Уанету [Електронний ресурс] / А. М. Пелещишин // Онлайн-журнал Наукового товариства ім. Т. Шевченка. – 2006. – Режим доступу: WWW/URL: http://ntsh.org/uaweb2 07.06.2007.

3. Петрик В. М. Сутність інформаційної безпеки держави, суспільства та особи / В. М. Петрик // Юридичний журнал. – 2009. – № 5. [Електронний ресурс]. – Режим доступу до журналу: http://www.journal.iitta.gov.ua.

4. К. В. Молодецька, "Соціальні інтернет-сервіси як інструмент масової комунікації", на *Міжнар. наук.-практ. конф. Інформаційні технології та комп'ютерне моделювання*, Івано-Франківськ, 2016, с. 60–61.

5. К. М. Коган, "Соціальні мережі як елемент нового соціального середовища", *Міжнародний науковий форум: соціологія, психологія, педагогіка, менеджмент*, вип. 16, с. 61–71, 2014.

6. О. Якимчук, "Онлайнові соціальні мережі: перспективи розвитку", *Релігія та соціум*, № 2(6), с. 199–205, 2011.

7. L. Longo et al. "Enhancing Social Search: A Computational Collective Intelligence Model of Behavioural Traits, Trust and Time", *Transactions on Computational Collective Intelligence II: Lecture Notes in Computer Science*, vol. 6450, Berlin: Springer Berlin Heidelberg, 2010.

8. G. Michael, and Chr. Meinel, "Web Search Personalization Via Social Bookmarking and Tagging", *Lecture Notes in Computer Science*, pp. 367–380, 2007.

9. T. Aichner, and F. Jacob, "Measuring the Degree of Corporate Social Media Use", *International Journal of Market Research*, 57(2), pp. 257–275, 2015.

10. О. Г. Корченко, С. В. Казмірчук, Є. В. Паціра, С. О. Гнатюк, та В. М. Кінзерявий, "Ознаковий принцип формування класифікацій кібератак", *Вісник СНУ ім. В. Даля*, № 4, т. 1, с. 184–193, 2010.

11. К. В. Молодецька, "Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави", *Information Technology and Security*, vol. 4, № 1(6), с. 13–20, 2016.

12. К. В. Молодецька, "Соціальні інтернет-сервіси як суб'єкт інформаційного простору держави", на *VIII Міжнар. наук.-техн. конф. Інформаційно-комп'ютерні технології*, Житомир, 2016, с. 43–44.

13. Р. В. Грищук, та Ю. Г. Даник, *Основи кібернетичної безпеки. Монографія*, Житомир: ЖНАЕУ, 2016.

14. Т. Сазонов, "Социальная сеть микроблоггинга Twitter как инструмент "цветных революций", *Relga.ru*. [Электронный ресурс]. Доступно: http://www.relga.ru/Environ/WebObjects/tgu-www.woa/wa/Main?level1=main& level2=articles&textid=2608. Дата обращения: Нояб. 08, 2017.

15. Р. В. Грищук, та К. В. Молодецька-Гринчук, "Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах", *Сучасний захист інформації*, № 3(31), с. 86–96, 2017.

Надійшла: 14.03.2021 Рецензент: д.т.н., професор Вишнівський В.В.