УДК 004.056
DOI: 10.31673/2409-7292.2021.030611

Бобровський О.О., Кушнір Д.І., Дзюба Т.М.

МЕТОДИКА ВИБОРУ СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ВПЛИВУ НА СТРУКТУРУ ВІРТУАЛЬНОЇ СПІЛЬНОТИ

У статті проведено дослідження методів протидії негативному інформаційному впливу через віртуальні спільноти соціальних мереж. Запропоновані загальні рекомендації щодо побудови моделі системи моніторингу віртуальних спільнот соціальних мереж, використовуючи вже існуючі наукові дослідження. Досліджено три стратегії впливу на структуру інформаційного середовища віртуальних спільнот та їх недоліки. Проведено аналіз результату використання розглянутих стратегій на вже існуючих дослідженнях. Отримано графіки зміни показника інформаційної загрози процесу функціонування віртуальної спільноти залежно від стратегії впливу на структуру внутрішнього інформаційного середовища. Розглянуто структуру послідовності розроблення методів та алгоритмів оцінки інформаційних загроз віртуальних спільнот в соціальних мережах.

Ключові слова: соціальна мережа, віртуальна спільнота, негативний інформаційний вплив, внутрішнє інформаційне середовище.

Вступ

Віртуальні спільноти все активніше і масштабніше використовують в інтересах інформаційно-психологічного впливу. Вони надають широкі можливості в плані впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації). 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.

Аналіз проблеми протидії інформаційному впливу на структуру віртуальної спільноти. Згідно із законодавством України визначення поняття «інформаційна безпека» таке: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [1]. Відповідно до нормативно-законодавчих актів держави [2] та нормативно-правових документів провідних країн світу об’єктами інформаційних загроз є: особа; суспільство; держава.

У відповідності [3] до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні:

прояви обмеження свободи слова та доступу громадян до інформації;

поширення засобами масової інформації культу насильства, жорстокості, порнографії;

комп'ютерна злочинність та комп'ютерний тероризм;

розголошення таємної та конфіденційної інформації;

намагання маніпулювати суспільною свідомістю.

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.

Метою статті є розробка методики оцінювання ефективності протидії інформаційному впливу на структуру віртуальної спільноти.

Визначення ступеня інформаційної загрози віртуальної спільноти в соціальних мережах. Основи методу визначення ступеня інформаційної загрози лежать показники

інформаційної загрози віртуальної спільноти, які можна обчислити відповідно до виразу за підходами щодо визначення критичної цінності віртуальної спільноти, а саме [4]:

$InfThreat_{CritMembers}(VirtualCommunity)$ – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти заснований 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;

$InfThreat_{InfConfr}(VirtualCommunity)$ – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти заснований 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 .

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* ≤ 0 приймається рішення щодо протидії інформаційним загрозам віртуальної спільноти.

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. В разі збільшення кількості учасників деструктивної віртуальної спільноти збільшується показник *InfThreat CritMembers* (*VirtualCommunity*).

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:

$$InfThreat = 1 - (InfThreat_{InfConfr}(VirtualCommunity) + InfThreat_{CritMembers}(VirtualCommunity))' \quad (2)$$

Враховуючи визначення ступеня інформаційної загрози (2) він буде приймати значення в межах [1,–1]. Зміни значення ступеня інформаційної загрози віртуальної спільноти в залежності від кількості учасників деструктивної та конкуруючої віртуальної спільноти зображено на рис. 1. При значенні *InfThreat* ≤ 0 приймається рішення щодо протидії інформаційним загрозам віртуальної спільноти.

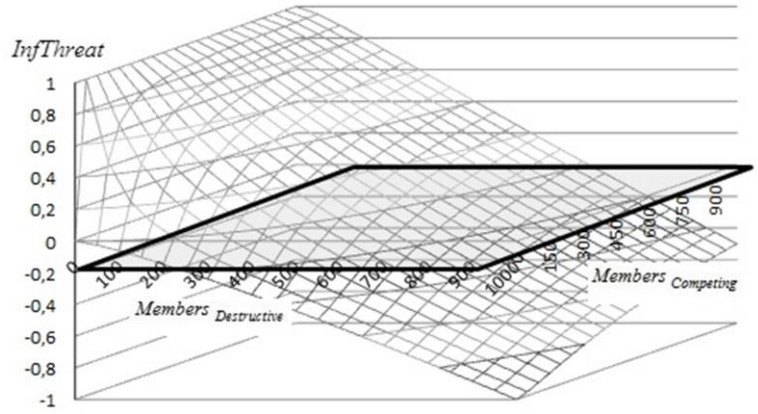

Рис. 1. Зміна *InfThreat* залежно від кількості учасників деструктивної та конкурентної віртуальних спільнот

Стратегії впливу на структуру внутрішнього інформаційного середовища розроблено залежно від правил протидії держави інформаційному впливу віртуальних спільнот, а саме:

Стратегія 1. Блокування дискусій або інформаційно-психологічного впливу на них з метою зміни тематичної спрямованості дискусій та їх переміщення до конкурентної віртуальної спільноти, що пов'язано зі зменшенням кількості дискусій та учасників у віртуальній спільноті.

Стратегія 2. Руйнування зв'язків окремої дискусії, щоб зробити її ізольованою дискусією без зменшення загальної кількості дискусій та учасників у віртуальній спільноті.

Стратегія 3. Руйнування зв'язків окремої дискусії задля формування окремих груп дискусій без зменшення загальної кількості дискусій та учасників у віртуальній спільноті.

Розглянемо вже існуюче дослідження з метою аналізу використання стратегій впливу на внутрішнє інформаційне середовище.

Умови дослідження:

Початкова структура внутрішнього інформаційного середовища така:

кількість дискусій – 100;

кількість учасників дискусій $ThreadMembers_i = 100$;

всі дискусії між собою взаємозв'язані гіперпосиланнями, тобто віртуальна спільнота становить одну групу.

Обмеження експерименту:

для вибору стратегії не враховується якість інформаційного наповнення віртуальної спільноти, тобто $Sim(Thread_i) = 1$.

Критична кількість учасників віртуальної спільноти дорівнює загальній кількості учасників дискусій у віртуальній спільноті $Members(InfThreat_i) = 10000$.

Для визначення інформаційної загрози віртуальної спільноти використовуємо показник інформаційної загрози .

Результати розрахунків вибіркових точок наведено в табл. 1.

Графіки зміни показника інформаційної загрози процесу функціонування віртуальної спільноти залежно від стратегії впливу на структуру внутрішнього інформаційного середовища наведено на рис. 2.

Результати використання стратегій:

Стратегія 1. Планомірне зменшення показника інформаційної загрози до нульової позначки, що характеризується не зміною структури внутрішнього інформаційного середовища віртуальної спільноти, а зменшенням кількості дискусій та учасників у віртуальній спільноті. Недоліком цієї стратегії є те, що не завжди існують інструменти

впливу щодо блокування сторінок дискусій у соціальних мережах, що пов'язано з багатьма об'єктивними причинами та особливостями віртуальних спільнот у разі виявлення небезпеки їх функціонування.

Таблиця 1.

Результати вибіркових точок

№ розрахунку	Стратегія 1			Стратегія 2			Стратегія 3		
	К-ть дискусій у групі	К-ть блокованих дискусій	Показник інформаційної загрози	К-ть дискусій у групі	К-ть ізольованих дискусій	Показник інформаційної загрози	К-ть груп	К-ть дискусій у групі	Показник інформаційної загрози
1	100	0	1	100	0	1	1	100	1
2	99	1	0,99	99	1	0,99	2	50	0,92
4	97	3	0,97	97	3	0,98	4	25	0,83
5	96	4	0,96	96	4	0,97	5	20	0,80
10	91	9	0,9	91	9	0,94	10	10	0,72
20	81	19	0,79	81	19	0,87	20	5	0,64
25	76	24	0,73	76	24	0,84	25	4	0,61
50	51	49	0,47	51	49	0,68	50	2	0,52
100	1	99	0	1	99	0,44	100	1	0,44

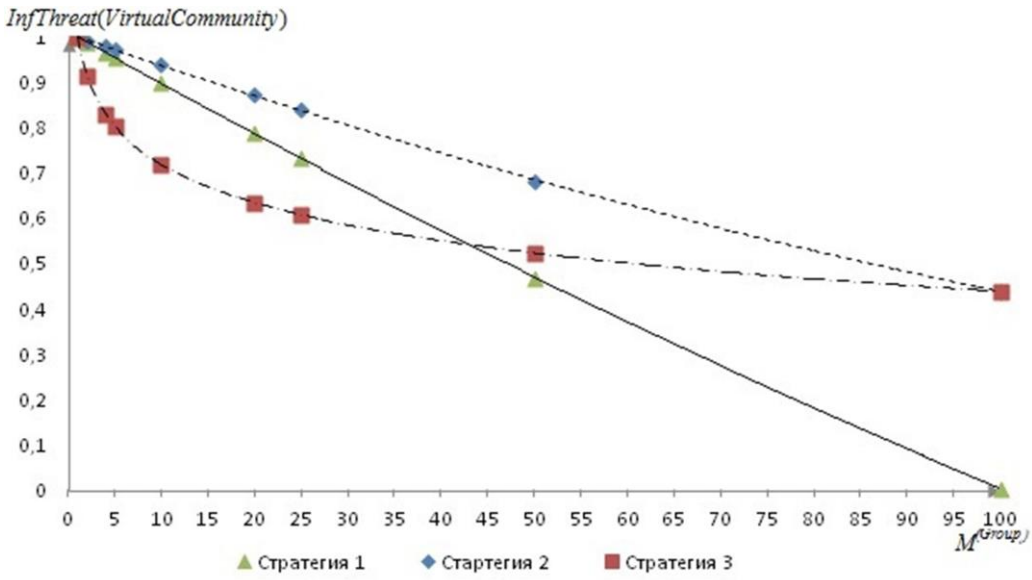

Рис. 2. Зміна показника інформаційної загрози за Стратегіями 1, 2 та 3

Стратегія 2. Планомірне зменшення показника інформаційної загрози до граничного мінімального значення. Зменшення показника залежить від кількості ізольованих дискусій, які утворилися в результаті інформаційно- психологічного впливу на структуру віртуальної спільноти. Недоліки цієї стратегії такі:

практично неможливо за великої кількості дискусій здійснювати інформаційно-психологічний вплив на всі дискусії для зміни структури внутрішнього інформаційного середовища;

обмеженість граничним мінімальним значенням показника інформаційної загрози.

Стратегія 3. Характеризується на перших етапах різким зменшенням показника інформаційної загрози з подальшим планомірним зниженням до граничного мінімального значення. Недоліки цієї стратегії такі:

у загальному випадку, для формування окремих груп дискусій необхідно здійснювати інформаційно-психологічний вплив більш ніж на одну дискусію;

обмеженість граничним мінімальним значенням показника інформаційної загрози.

Рекомендації формулюють після того, як сформовано повний перелік дискусій, видалення яких з віртуальної спільноти забезпечує зменшення показника інформаційної загрози до порогового значення. Метод визначення рекомендацій щодо інформаційного впливу на віртуальні спільноти зображено на рис. 3.

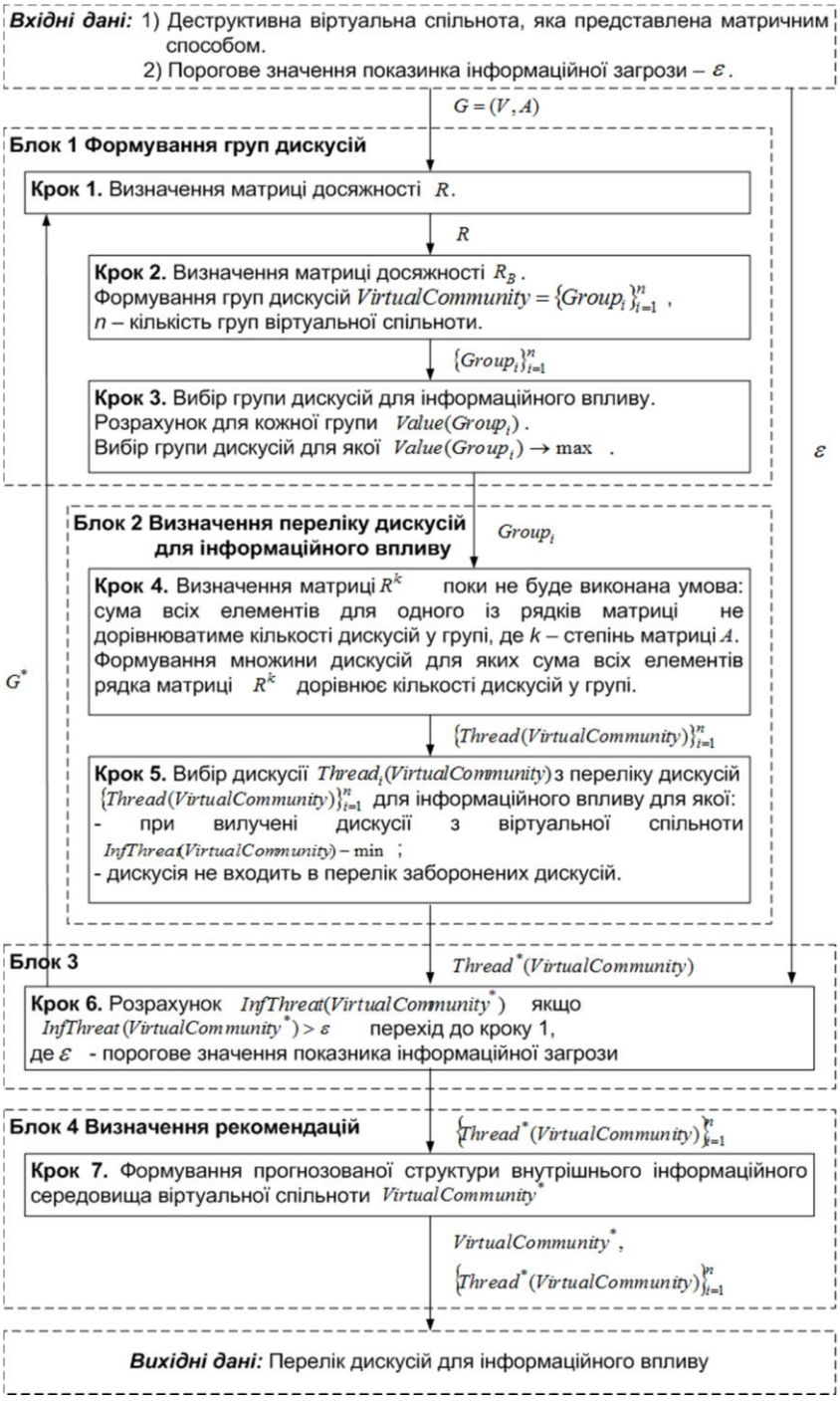

Рис. 3. Схематичне зображення методу визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти

Крім переліку дискусій, формується прогнозована структура внутрішнього та зовнішнього інформаційних середовищ віртуальної спільноти після інформаційного впливу. Для подальшого моніторингу віртуальної спільноти визначають вікно спостереження, яке забезпечить очікування результатів після виконання дій щодо інформаційно-психологічного впливу. Під час повторного моніторингу соціальної мережі здійснюють всі заходи для виявлення та формування віртуальної спільноти за визначеною тематикою інформаційного наповнення. Перед повторним моніторингом соціальної мережі формується перелік заборонених дискусій.

Загальним недоліком стратегій 2 та 3 є те, що практично неможливо методами інформаційно-психологічного впливу руйнувати зв'язки між дискусіями у віртуальній спільноті.

Отже, ефективними стратегіями впливу є змішані стратегії 1&2 та 1&3, у разі використання яких можливі такі варіанти впливу:

руйнування зв'язків між дискусіями групи за допомогою блокування дискусій (силовий метод);

інформаційно-психологічний вплив на дискусії з метою зменшення ступеня відповідності тематичного напряму повідомлень у дискусії та переходу дискусії до конкурентної віртуальної спільноти (моніторинг віртуальних спільнот та протидія методами інформаційно-психологічного впливу).

Висновки.

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. Становлення віртуальних спільнот інструментом руйнівного характеру ставить під загрозу питання інформаційної безпеки не тільки однієї держави, але і суспільства в найбільш серйозних масштабах. Для протидії негативному інформаційно-психологічному впливу віртуальної спільноти найбільш доцільним є реалізація однієї з досліджених стратегій. Вибір стратегії доцільно здійснювати на основі дослідження залежностей змін показників інформаційної загрози залежно від кількості учасників деструктивної та конкурентної віртуальних спільнот. Створення технічних та програмних засобів для виявлення та протидії деструктивному впливу інформаційному наповненню віртуальних спільнот у соціальних мережах є подальшим кроком для реалізації запропонованого підходу.

Перелік посилань

1. Жарков Я.М. Інформаційна безпека особистості, суспільства, держави /Я. М. Жарков, Т. М. Дзюба, І. В. Замаруєва. – К. : Видавничо- поліграфічний центр «Київський університет», 2008. – 274 с.

2. Доктрина інформаційної безпеки України: проект: за станом на 1 квітня 2015 р. / [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025. – Назва з екрана.

3. Закон України «Про основи національної безпеки України» від 19 червня 2003 року: із змінами, внесеними Законом України від 12 лютого 2015 р.: за станом на 1 березня 2015 р. / [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15. – Назва з екрана.

4. Бобровський О.О., Опанасенко М.І., Дзюба Т.М. Технологія виявлення інформаційних загроз віртуальних спільнот в соціальних мережах. Сучасний захист інформації №2(46), 2021. – С. 6–13.

Надійшла: 14.06.2021 Рецензент: д.т.н., професор Вишнівський В.В.