У даній статті запропонована методика прийняття рішення щодо протидії інформаційним загрозам віртуальної спільноти, яка ґрунтується на визначенні показника інформаційної загрози, що використовує значення цінності віртуальної спільноти. Сформована модель загроз та надані рекомендації щодо прийняття рішення по протидії інформаційним загрозам віртуальної спільноти

Ключові слова: соціальні мережі, віртуальні спільноти, інформаційна загроза, модель загроз, цінність, показник

В данной статье предлагается методика принятия решения по противодействию информационным угрозам виртуального сообщества, основанной на определении показателя информационной угрозы, использующей значение ценности виртуального сообщества. Сформирована модель угроз и даны рекомендации по принятию решения по противодействию информационным угрозам виртуального сообщества

Ключевые слова: социальные сети, виртуальные сообщества, информационная угроза, модель угроз, ценность, показатель

УДК 004.738.5(045)
DOI: 10.15587/1729-4061.2015.38016

МЕТОДИКА ПРИЙНЯТТЯ РІШЕННЯ ЩОДО ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ ВІРТУАЛЬНИХ СПІЛЬНОТ

Р. В. Гумінський
Старший науковий співробітник, підполковник
Науково-дослідний відділ
(моделювання бойових дій)
Науковий центр Сухопутних військ
Академії сухопутних військ
вул. Гвардійська, 32, м. Львів, Україна, 79000
E-mail: gruslan@meta.ua

1. Вступ

З розвитком соціальних мереж та зростанням кількості їх користувачів, що зумовлено постійним вдосконаленням їх інструментарію, вони стали ідеальним майданчиком для утворення віртуальних спільнот.

Користувачі соціальних мереж, відповідно до характеру інформаційного наповнення сторінок (дискусій) віртуальних спільнот, широко використовують їх для обговорення певних тематик, для проведення соціальних досліджень, оцінки ставлення людей до тематик різної спрямованості (політичної, культурної, тощо). Крім того, все частіше їх використовують задля різних інформаційних протиборств, а саме: предвиборних перегонів, просування товарів чи послуг у конкурентному середовищі, впливів на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не відповідають їхнім інтересам та пов'язані з інформаційними загрозами особистості, суспільству, державі [1].

На жаль, поряд з конструктивними віртуальними спільнотами, які прагнуть активно взаємодіяти з суспільством, маючи на меті поліпшення життя як усього суспільства, так і окремих соціальних груп та індивідів, соціальні мережі все частіше використовують для створення деструктивних віртуальних спільнот [2]. Деструктивні віртуальні спільноти, на відміну від конструктивних, намагаються з цим співтовариством боротися усілякими, не завжди законними, методами. Об'єктом агресії деструктивних віртуальних спільнот є суспільство загалом або прихильники тих чи інших соціальних груп, як правило, вороже налаштованих до цієї деструктивної віртуальної спільноти.

Основна особливість і головна небезпека деструктивних віртуальних спільнот пов'язана з тим, що визнати за законом їх діяльність як деструктивну в умовах дії норм свободи слова, друку, віросповідання можливо тільки після реалізації в реальному світі їх учасниками певних заходів, здійснених під дією інформаційного впливу. Тільки тоді, вони можуть бути співвіднесені з нормами чинного законодавства та кваліфіковані відповідним чином.

Одним із основних методів інформаційного протиборства серед віртуальних спільнот та протидії інформаційним загрозам у цих спільнотах є інформаційний вплив [3], здійснюваний з метою інформаційного управління. Під інформаційним управлінням, у цьому випадку, розуміють ситуацію, коли об'єкту управління надається певна інформація, під впливом якої, він формує свою лінію поведінки [4].

Таким чином, виникає необхідність щодо оцінки діяльності віртуальних спільнот, їх інформаційного наповнення, на етапі їх функціонування в соціальних мережах та прийняття рішення щодо протидії їхньому інформаційному впливу, з метою попередження інформаційних загроз та реалізації їх в реальному світі.

2. Аналіз останніх досліджень та постановка проблеми

У [5, 6] визначено правила протидії Держави інформаційному впливу віртуальних спільнот, а саме:

– силові методи – закриття серверів;

– юридично-правові методи – притягнення до кримінальної відповідальності учасників віртуальної спільноти;

– моніторинг віртуальних спільнот та протидія методами інформаційного впливу.

Визначено, що метод моніторингу віртуальних спільнот та протидія методами інформаційного впливу ефективніші в довгостроковій перспективі щодо інформаційної протидії їм. Використання цього методу дає змогу не тільки припиняти, придушувати діяльність віртуальних спільнот, але й змінювати їхню ідеологію.

У дослідженні [7] розроблено модель інформаційного середовища віртуальної спільноти, яка складається із зовнішнього та внутрішнього інформаційних середовищ.

На основі моделі інформаційного середовища в [8, 9] сформовано показник інформаційної загрози для оцінки рівня інформаційної загрози віртуальної спільноти, в якому відповідно до моделі інформаційного середовища враховано такі складові:

– кількість учасників віртуальної спільноти;

– кількість можливого мобілізаційного ресурсу;

– якість інформаційного наповнення віртуальної спільноти;

– структура зв'язків дискусій у віртуальній спільноті.

В той же час в цих дослідженнях відсутні методики розрахунку показника інформаційної загрози в залежності від визначення критичної цінності віртуальної спільноти.

3. Ціль та задачі дослідження

Метою даної роботи є розробка методики прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот.

Для досягнення поставленої мети вирішувалися наступні задачі:

– визначені підходи щодо розрахунку критичної цінності віртуальної спільноти;

– побудувана модель загроз інформаційної безпеки;

– розроблені рекомендації по прийняттю рішення шодо протидії інформаційним загрозам віртуальних спільнот.

4. Розрахунок показника інформаційної загрози віртуальної спільноти

Використовуючи модель внутрішнього інформаційного середовища, де ***внутрішнє інформаційне середовище віртуальної спільноти*** – це сукупність дискусій, які створюються зареєстрованими учасниками соціальної мережі та об'єднуються за ознакою мети та ідеологією існування, а також зв'язками між ними [7]:

$$\begin{aligned}&\mathrm{InfSpace}(\mathrm{VirtualCommunity}_i)=\\&=\langle \mathrm{Thread}(\mathrm{VirtualCommunity}_i),\\&\mathrm{LinkInternal}(\mathrm{Tread}),\mathrm{Member}(\mathrm{VirtualCommunity}_i),\\&\mathrm{Shadow}(\mathrm{VirtualCommunity}_i)\rangle,\end{aligned}\qquad(1)$$

де $\mathrm{Thread}(\mathrm{VirtualCommunity}_i)$ – сукупність дискусій і-ї віртуальної спільноти; $\mathrm{LinkInternal}(\mathrm{Thread})$ – матриця зв'язків між дискусіями і-ї віртуальної спільноти; $\mathrm{Member}(\mathrm{VirtualCommunity}_i)$ – множина учасників дискусій і-ї віртуальної спільноти, зареєстрованих користувачів соціальних мереж:

$$\begin{aligned}&\mathrm{Member}(\mathrm{VirtualCommunity}_i)=\\&=\bigcup_{j=1}^{N_i}\mathrm{Member}(\mathrm{Thread}_j),\end{aligned}\qquad(2)$$

де $\mathrm{Member}(\mathrm{Thread}_j)$ – множина учасників j-ї дискусії, зареєстрованих користувачів соціальних мереж; N_i– кількість дискусій в і-й віртуальній спільноті; $\mathrm{Shadow}(\mathrm{VirtualCommunity}_i)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) і-ї віртуальної спільноти:

$$\begin{aligned}&\mathrm{Shadow}(\mathrm{VirtualCommunity}_i)=\\&=\bigcup_{j=1}^{N_i}\mathrm{Shadow}(\mathrm{Thread}_j),\end{aligned}\qquad(3)$$

де $\mathrm{Shadow}(\mathrm{Thread}_j)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені тематикою j-ї дискусії та не являються учасниками дискусії; N_i – кількість дискусій у *i*-й віртуальній спільноті.

При цьому:

$$\begin{aligned}&\mathrm{Member}(\mathrm{VirtualCommunity}_i)\neq\\&\neq\mathrm{Shadow}(\mathrm{VirtualCommunity}_i).\end{aligned}$$

Використовуючи модель внутрішнього інформаційного середовища (1) в [8, 9], сформований показник інформаційної загрози процесу функціонування віртуальної спільноти в загальному має вигляд:

$$\begin{aligned}&\mathrm{InfTreat}(\mathrm{VirtualCommunity})=\\&=\begin{cases}\dfrac{\mathrm{Value}(\mathrm{VirtualCommunity})}{\mathrm{Value}(\mathrm{VirtualCommunity})^*},\\1,\ \text{якщо}\ \dfrac{\mathrm{Value}(\mathrm{VirtualCommunity})}{\mathrm{Value}(\mathrm{VirtualCommunity})^*}>1,\end{cases}\end{aligned}\qquad(4)$$

де $\mathrm{Value}(\mathrm{VirtualCommunity})$ – цінність віртуальної спільноти; $\mathrm{Value}(\mathrm{VirtualCommunity})^*$ – критична цінність віртуальної спільноти, при якій реалізується інформаційна загроза.

Цінність віртуальної спільноти – це потенційна доступність учасників спільноти, з якими любий учасник спільноти може «зв'язатися» в разі необхідності [10].

Цінність віртуальної спільноти [8, 9], визначається, як:

$$\begin{aligned}&\mathrm{Value}(\mathrm{VirtualCommunity})=\\&=\sum_{i=1}^{N}\left(\sum_{j=1}^{M^{(\mathrm{Group}_i)}}\left(\mathrm{Sim}(\mathrm{Thread}_j)\cdot\mathrm{card}(\mathrm{ThreadMembers}_j)\right)\times\right.\\&\times\ln\left(\sum_{j=1}^{M^{(\mathrm{Group}_j)}}\left(\mathrm{Sim}(\mathrm{Thread}_j)\cdot\mathrm{card}(\mathrm{ThreadMembers}_j)\right)\right)-\\&\left.-\sum_{j=1}^{M^{(\mathrm{Group}_j)}}\left(\mathrm{Sim}(\mathrm{Thread}_j)\cdot\mathrm{card}(\mathrm{ThreadMembers}_j)\right)\right),\end{aligned}\qquad(5)$$

де $ThreadMembers_i$ – множина учасників і-ї дискусії; $Sim(Thread_i)$ – міра відповідності тематичного напрямку і-ї дискусії; N – кількість груп у віртуальній спільноті; $M^{(Group_i)}$ – кількість дискусій в і-й групі.

Група віртуальної спільноти – це сукупність дискусій, взаємозв'язаних між собою зв'язками та не зв'язаних з іншими дискусіями віртуальної спільноти.

Міра відповідності тематичного напрямку дописів в дискусії – це ознака, яка залежить від позитивного чи негативного напрямку повідомлень в дискусії, у відповідності до тематичного напрямку віртуальної спільноти.

Для визначення критичної цінності віртуальної спільноти використовуються наступні підходи.

Перший підхід для визначення критичної цінності віртуальної спільноти заснований на визначенні експертами кількості учасників віртуальної спільноти, при якій реалізовується і-та інформаційна загроза, без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті.

Таким чином, виходячи з (5), критична цінність віртуальної спільноти має вигляд:

$$Value(VirtualCommunity)^* = \\ = Memebers(InfTreat_i)\cdot \ln\left(Memebers(InfTreat_i)\right) - \\ - Memebers(InfTreat_i), \quad (6)$$

де $Memebers(InfTreat_i)$ – критична кількість учасників віртуальної спільноти, визначеної експертами, при якій реалізується і-та інформаційна загроза без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті.

Недоліками даного підходу є:

– не завжди точно можна визначити кількість учасників віртуальної спільноти, при якій реалізується інформаційна загроза;

– не відображає загальну картину, щодо інформаційної переваги деструктивної віртуальної спільноти, по відношенню до конкуруючої віртуальної спільноти, які зацікавлені даною тематикою.

Перевагою даного підходу є те, що для прийняття рішення, щодо протидії інформаційному впливу деструктивної віртуальної спільноти не потрібно враховувати додаткові фактори.

Інший підхід, заснований з урахуванням визначення критичної цінності віртуальної спільноти щодо загальної кількості учасників деструктивної та конкуруючої віртуальних спільнот, які зацікавленні даною тематикою з урахуванням якості інформаційного наповнення та структури зв'язків дискусій в цих віртуальних спільнотах.

Таким чином, критична цінність віртуальної спільноти має вигляд:

$$Value(VirtualCommunity)^* = \\ = \sum_{i=1}^{N} Value(VirtualCommunity_i), \quad (7)$$

де $Value(VirtualCommunity_i)$ – цінність і-тої віртуальної спільноти; N – кількість віртуальних спільнот, зацікавлених даною тематикою (як правило, деструктивна та конкуруюча).

Цінності для деструктивної та конкуруючої віртуальної спільноти розраховуємо використовуючи формулу (5).

Недоліками даного підходу є: в окремих випадках, коли даною тематикою зацікавлена тільки одна деструктивна віртуальна спільнота, до якої входять одна або декілька дискусій, з невеликою кількістю учасників отримуємо максимальне значення показника інформаційної загрози. Таким чином, при прийнятті рішення щодо протидії інформаційному впливу необхідно враховувати додаткові фактори, а саме:

– загальну кількість учасників віртуальних спільнот, зацікавлених даною тематикою;

– середню інтенсивність публікації повідомлень в інформаційному наповненні дискусій віртуальної спільноти.

Перевагою даного підходу є те, що він відображає повну картину інформаційного протиборства між віртуальними спільнотами (деструктивна та конкуруюча), зацікавлених даною тематикою.

5. Методика прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот

Для прийняття щодо протидії інформаційним загрозам віртуальних спільнот в соціальних мережах необхідно проводити вивчення та систематизацію інформаційних загроз віртуальних спільнот [11]. Для цього формуємо модель загроз (зразок моделі загроз табл. 1), яка складається з:

– об'єкту загрози;

– сфери застосування загрози;

– переліку загроз;

– оцінки ризиків загрози.

Об'єкт, сфера застосування та перелік загроз визначається у відповідності до нормативно-правових документів з інформаційної безпеки держави. Аналіз загроз процесу функціонування віртуальних спільнот більш детально проводився в [5, 6].

Перелік загроз, крім того, розподіляється на відповідні тематики щодо інформаційного наповнення віртуальних спільнот.

Оцінка ризиків на відмінності від технічним систем визначається не як ймовірність виникнення загрози, а як критична кількість учасників віртуальної спільноти, при якій реалізується дана загроза.

Вихідними даними для експертного визначення інформаційної загрози, яке несе інформаційне наповнення віртуальної спільноти з моделі загроз є:

– перегляд інформаційного наповнення дискусій віртуальної спільноти;

– оцінювання ключових слів, отриманих центроїдів віртуальних спільнот;

– використання алгоритмів автоматичного реферування [12].

Для визначення ступеня інформаційної загрози використовуємо показники інформаційної загрози віртуальної спільноти, які розраховуються відповідно до виразу (4) за підходами визначення критичної цінності віртуальної спільноти, а саме:

$InfTreat_{CritMembers}$(VirtualCommunity) – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти заснований на визначенні експертами кількості учасників віртуальної спільноти, при якій 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;

$InfTreat_{InfConfr}$(VirtualCommunity) – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти заснований щодо загальної кількості учасників деструктивної та конкуруючої віртуальних спільнот, які зацікавлені даною тематикою з урахуванням якості інформаційного наповнення та структури зв'язків дискусій в цих віртуальних спільнотах.

Таблиця 1

Модель загроз інформаційної безпеки

Об'єкт	Сфера	Перелік загроз		Оцінка ризиків загроз
		Загрози	Тематика ІН	
1. Держава	1.1 зовнішньо-політична	1.1.1 поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації	...	...
			...	...
		1.1.2 зовнішні негативні інформаційні впливи на суспільну свідомість	...	...
			...	...
		1.1.3 ...	...	...
	1.2 державна безпеки	1.2.1 негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів	...	...
			...	...
		1.2.2 ...	...	...
	1.3 ...	1.3.1 ...	...	...
2. Суспільство	2.1 соціальна та гуманітарна	2.1.1 створення атмосфери бездуховності та аморальності	...	...
3. Особистість	3.1 ...	...	...	...

В табл. 2. наведенні значення показників інформаційної загрози.

Таким чином, прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот проводиться на підставі значень показників інформаційної загрози.

Таблиця 2

Значення показників інформаційної загрози

Значення показників	Опис значень показників	Результат
$InfTreat_{CritMembers} > 0,5$, $InfTreat_{InfConfr} > 0,5$	Деструктивна віртуальна спільнота має достатню кількість учасників щодо реалізації інформаційної загрози та має перевагу в інформаційному протиборстві з конкуруючою віртуальною спільнотою.	Необхідно протидіяти інформаційній загрозі.
	Якщо значення показника $InfTreat_{InfConfr} \to 1$ показує відсутність конкуруючої віртуальної спільноти по відношенню до тематики інформаційного наповнення деструктивної віртуальної спільноти.	Необхідно проводити вплив на інформаційне наповнення деструктивної віртуальної спільноти та проводити заходи щодо створення конкуруючої віртуальної спільноти.
$InfTreat_{CritMembers} > 0,5$, $InfTreat_{InfConfr} < 0,5$	Деструктивна віртуальна спільнота має достатню кількість учасників щодо реалізації інформаційної загрози. При цьому, перевагу в інформаційному протиборстві на боці конкуруючої віртуальної спільноти.	Необхідно протидіяти інформаційній загрозі щодо зменшення кількості учасників деструктивної віртуальної спільноти.
	Якщо значення показника $InfTreat_{InfConfr} \to 0$ показує відсутність деструктивної віртуальної спільноти.	Ведення постійного моніторингу.
$InfTreat_{CritMembers} < 0,5$, $InfTreat_{InfConfr} > 0,5$	Кількість учасників деструктивної віртуальної спільноти не має достатньої кількості учасників щодо реалізації інформаційної загрози, але має значну перевагу в інформаційному протиборстві з конкуруючою віртуальною спільнотою.	Ведення постійного моніторингу щодо збільшення кількості учасників.
	Якщо значення показника $InfTreat_{CritMembers} \approx 0,5$	Необхідно протидіяти інформаційній загрозі.
	Якщо значення показника $InfTreat_{InfConfr} \to 1$ показує відсутність конкуруючої віртуальної спільноти по відношенню до тематики інформаційного наповнення деструктивної віртуальної спільноти.	Необхідно протидіяти інформаційній загрозі з метою проведення заходів щодо створення конкуруючої віртуальної спільноти.
	Якщо значення показників $InfTreat_{CritMembers} \to 0$ та $InfTreat_{InfConfr} \to 1$ показує про створення нової або «вмирання» існуючої деструктивної спільноти.	Ведення постійного моніторингу щодо сценарію розвитку віртуальної спільноти.
$InfTreat_{CritMembers} < 0,5$, $InfTreat_{InfConfr} < 0,5$	Кількість учасників деструктивної віртуальної спільноти не має достатньої кількості учасників щодо реалізації інформаційної загрози При цьому перевагу в інформаційному протиборстві на боці конкуруючої віртуальної спільноти.	Ведення постійного моніторингу.

6. Висновки

У роботі розроблена методика прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот, яка використовує показник інформаційної загрози, що використовує значення цінності віртуальної спільноти. Запропоновано підходи щодо визначення критичної цінності віртуальної спільноти, а саме:

– визначення експертами кількості учасників віртуальної спільноти при якій реалізовується інформаційна загроза, без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті;

– визначення загальної кількості учасників деструктивної та конкуруючої віртуальних спільнот, які зацікавлені даною тематикою з урахуванням якості інформаційного наповнення та структури зв'язків дискусій в цих віртуальних спільнотах.

Розроблена методика та рекомендації прийняття рішення щодо протидії інформаційним загрозам у віртуальних спільнотах, використовуючи показників інформаційної загрози спільноти які розраховуються відповідно до виразу (4) за запропонованими підходами визначення критичної цінності віртуальної спільноти.

Література

1. Carley, K. Destabilizing networks [Text] / K. Carley, J. Lee, D. Krackhardt // Connections, 2002. – Vol. 24, Issue 3. – P. 79–92.
2. Stohl, C. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences [Text] / C. Stohl, M. Stohl // Communication Theory. – 2007. – Vol. 17, Issue 2. – P. 93–124. doi: 10.1111/j.1468-2885.2007.00289.x
3. Information operation roadmap [Text] / DoD US, 30 october 2003. – 78 p.
4. Горбулін, В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання [Текст] : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде – К.: Інтертехнологія, 2009. – 163 с.
5. Гумінський, Р. В. Віртуальні спільноти, як суб'єкт інформаційної безпеки держави [Текст] / Р. В. Гумінський // "Захист інформації" наук.-практ. журнал. – 2012 – № 3 (56). – С. 18–25.
6. Пелещишин, А. М. Загрози інформаційної безпеки держави в соціальних мережах [Текст] / А. М. Пелещишин, Р. В. Гумінський // Наука і техніка Повітряних сил Збройних Сил України: наук.-техн. журнал – 2013. – № 2(11). – С. 192–199.
7. Пелещишин, А. М. Модель інформаційного середовища віртуальної спільноти [Текст] / А. М. Пелещишин, Р. В. Гумінський // Східно-Європейський журнал передових технологій. – 2014. – Т. 2, № 2 (68). – С. 10–16. doi: 10.15587/1729-4061.2014.21867
8. Оцінка інформаційних загроз процесу функціонування віртуальних спільнот [Текст] : матер. IV міжн. наук.-тех. конф. / «ITSEC-2014»: Безпека інформаційних технологій. – Київ, 2014 – С. 59–60.
9. An assessment of informational threat in the functioning process of virtual community [Electronic resource] / Cybernetic Letters. – Available at: http://www.cybletter.com – 10.01.2015 – Title from the screen.
10. Бреер, В. В. Стохастические модели социальных сетей [Текст] / В. В. Бреер // Управление большими системами. – 2009. – № 27. – С. 169–204.
11. Домарева, В. В. Безопасность информационных технологий. Системный подход [Текст] / В. В. Домарева. – К.:Изд. «Диасофт», 2004. – 992 с.
12. Yatsko, V. Automatic genre recognition and adaptive text summarization [Text] / V. A. Yatsko, M. S. Starikov, A. V. Butakov // Automatic Documentation and Mathematical Linguistics. – 2010. – Vol. 44, Issue 3. – P. 111–120. doi: 10.3103/s0005105510030027