УДК 004.056
DOI: 10.31673/2409-7292.2022.040002

Шуклін Г.В., Кравченко Б.А., Ковальчук В.А.

МЕТОДИКА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

У статті проведено аналіз сучасних методів моделювання інформаційних впливів, систематизовано проблеми оптимізації систем захисту кіберпростору від інформаційних впливів. А також досліджено методи оцінювання загроз в кіберпросторі та розроблено рекомендації щодо оптимізації методів захисту кіберпростору від інформаційних впливів.

Ключові слова: інформаційна безпека держави, інформаційний вплив, загроза, атака, інформаційна система, кіберпростір.

Вступ

Досвід відбиття збройної агресії з боку Російської Федерації щодня демонструє, що Інтернет є однією з ефективних форм протистояння – гібридної війни. У той же час проти України, Європейського Союзу та Сполучених Штатів Америки Російською Федерацією ведеться інформаційна війна. При цьому вона поєднує в собі дві складових – інформаційну (інформаційні операції) та психологічну (психологічні операції), які в ході інформаційного протиборства, в тому числі з використанням інформаційних систем, застосовуються для маніпулювання особистістю та групами людей. Тому, зважаючи на комплексний характер загроз інформаційній безпеці, проблема розроблення ефективних підходів до побудови системи забезпечення Інформаційної безпеки держави в умовах глобалізації та вільного обігу інформації є особливо актуальною.

Постановка проблеми

Виявлення користувачів, які є суб'єктами впливу для маніпулювання поведінкою аудиторії, проводиться на основі побудови профілю інформаційної безпеки з подальшим віднесенням до певного класу загроз. Формування узагальненого висновку про рівень загрози Інформаційній безпеці держави створює передумови для підвищення ефективності заходів з інформаційної протидії. Тому розробка методики оцінювання загроз Інформаційній безпеці держави є актуальним науковим завданням.

Аналіз дотичних робіт

Аналіз багатьох досліджень і публікацій [1, 2] свідчить про відсутність загальноприйнятої методики оцінювання рівня загроз Інформаційній безпеці держави. На сьогоднішній день провідна роль у виявленні та протидії загрозам Інформаційній безпеці держави належить об'єднаному центру передових технологій з кібероборони НАТО (Таллінн, Естонія) [3]. Так, у рамках проекту Академії електронного управління цієї країни вже тривалий час використовується National Cyber Security Index (NCSI) – глобальний індекс оцінки готовності країни запобігти реалізації основних інформаційних загроз, а також її здатність управляти інцидентами, злочинами і великомасштабними кризами. NCSI – це інструмент інструмент для оцінювання потенціалу інформаційної безпеки країни і заходів захисту її інформаційного простору.

Для формування індексу NCSI використовуються наступні дані:

а) загальний показник інформаційної безпеки;

б) базові показники інформаційної безпеки;

в) показники управління інцидентами і кризами інформаційної безпеки;

г) показники міжнародного впливу на інформаційну безпеку.

Складність застосування NCSI для оцінювання загроз Інформаційній безпеці держави полягає у відсутності детальної методології оцінювання окремих показників, неможливості їх виділення із загального контексту чи з сукупності інших інтегральних показників безпеки.

Як правило, оцінювання загроз здійснюється на основі кількісних та якісних методів [4]. Кількісні методи передбачають розрахунок ймовірності реалізації загроз на основі відомої інформації. Такі методи базуються на побудові гістограм розподілу проявів ознак

загроз і частот їх реалізації, або на основі розрахунку статистичних характеристик процесів, які супроводжують реалізацію таких загроз. Недоліком такого підходу є обмеженість застосування для оцінювання загроз інформаційній безпеці держави, пов'язана зі складністю збору необхідного обсягу статистичних даних і формалізації ознак інформаційних акцій.

Для якісного оцінювання рівня загроз Інформаційній безпеці держави використовуються експертні методи [5], які зводяться до узагальнення та статистичної обробки суджень експертів. Разом з тим, експертні методи оцінювання в задачах виявлення загроз суттєво обмежуються необхідністю обробки великих масивів вхідних даних, у яких часто бувають помилки або пропущені дані. Також, низькою є швидкодія оцінювання, яке потребує часу на підготовку значної кількості кваліфікованих експертів. Впливає на результативність також і суб'єктивність оцінок експертів. Дослідження багатьох джерел, як наведено, наприклад у [6], свідчить про значне зростання кількості загроз Інформаційній безпеці держави, що визначає суть протиріччя між рівнем сучасних загроз і науковим базисом їх оцінювання. Всі розглянуті фактори додатково актуалізують важливість проблеми розробки методики оцінювання інформаційних загроз.

Дуже часто виявлення загроз Інформаційній безпеці держави базується, зокрема, на виявленні ознак інформаційних операцій проти держави. При цьому, зважаючи на багатокритеріальний характер задачі, виділяють наступні групи методів [7]:

1) оптимізації ієрархічної послідовності критеріїв якості;

2) визначення множини Парето-оптимальних рішень;

3) на основі пошуку компромісу.

Недоліками перших двох груп методів є складність визначення структури ієрархічної послідовності окремих критеріїв та суттєву обмеженість Парето-оптимальних рішень областю компромісів. У свою чергу, використання компромісу, покладеного в основу третьої групи методів, забезпечує зниження якості за одними критеріями, яке не перевершує підвищення якості за іншими критеріями. Тому використання методів на основі компромісу для виявлення загроз є більш перспективним напрямком досліджень. Як приклад методу на основі компромісу, можна розглянути запропоновану Альбертом Вороніним нелінійну схему компромісів, яка забезпечує компроміс між частинними критеріями, а отримане рішення є оптимальним за Парето [8]. Перевагою даного методу є його обчислювальна простота, унімодальність, що забезпечує можливість відшукання єдиного рішення задачі та можливість адаптації до умов застосування.

Метою статті є дослідження методики оцінювання інформаційних впливів для забезпечення Інформаційної безпки держави та населення.

Виклад основного матеріалу

Як відомо, метою інформаційного впливу є порушення звичного режиму функціонування об'єкта впливу, тобто виведення інформаційної такого об'єкта за межі певного допустимого стану. По відношенню до об'єкта впливу джерело впливу може бути як зовнішнім, так і внутрішнім.

Зовнішні впливи, у разі цілеспрямованої інформаційної дії (інформаційної війни), як правило, приховані і полягають у боротьбі конкуруючих соціальних систем за загальні ресурси, що забезпечують таким системам допустимі умови існування. Причини внутрішніх впливів обумовлюються появою множини елементів всередині системи, для яких звичний режим функціонування став неприйнятним.

Допустимим режимом функціонування є таке функціонування соціальної чи будь-якої іншої системи, яке забезпечене необхідними матеріальними та іншими видами ресурсів. Відповідно, неприпустимим режимом – буде режим, у якому система повною мірою необхідними для нормального функціонування матеріальними ресурсами не забезпечена. Таким чином, інформаційний вплив базується на тих вхідних даних, які призначені для активізації в системі алгоритмів, відповідальних за порушення штатного режиму функціонування системи.

Методика оцінювання загроз Інформаційній безпеці держави

Зважаючи на проведений вище розгляд, для формування методики оцінювання загроз Інформаційній безпеці держави [9] найбільш доцільно обрати нелінійну схему компромісів [6, 8]. При цьому суть методики може бути зведена до декількох етапів.

Етап 1. Розрахунок показника ознак інформаційних операцій (I_1). Підхід [8] базується на пошуку публікацій і коментарів, розрахунку показників перегляду текстового/відео/аудіо контенту, підрахунок кількості коментарів, лайків, дизлайків та ін. Висновок про цілеспрямовану інформаційну операцію, направлену проти інформаційної безпеки особистості, суспільства, держави формується на основі відповідного узагальненого показника I_1, який приймає значення

$$I_1 = \begin{cases} 1, \text{якщо загроза існує;} \\ 0, \text{якщо загрози не існує.} \end{cases} \quad (1)$$

Етап 2. Визначення показника наявності інформаційного впливу на учасників інформаційної взаємодії (I_2). Виявлення таких прихованих інформаційних впливів полягає в інтелектуальному пошуку повторюваності окремих повідомлень, їх обговорюваності відмовідно до заданих наративів за критерієм актуальності та критичності [10 – 12]. Для визначення показника використовується семантичний аналіз на основі онтологій з використанням сигнатурного методу і методу виявлення аномалій. У результаті визначається показник I_2

$$I_2 = \begin{cases} 1, \text{якщо загроза існує;} \\ 0, \text{якщо загрози не існує.} \end{cases} \quad (2)$$

Етап 3. Оцінювання прояву маніпуляцій суспільною думкою (I_3). Розрахунок I_3 проводиться на основі урахування інформаційного впливу на користувачів інформаційної системи [13] та інтегрального показника інформаційної ентропії H_n контенту, тобто встановлення рівня невизначеності щодо використання технологій прихованого впливу на акторів. Зростання величини інформаційної ентропії H_n характеризує зменшення невизначеності, тому для задачі оцінювання прояву ознак маніпуляцій суспільною думкою показник I_3 набуває значень

$$I_3 = 1 - H_n, H_n \in [0; 1] \quad (3)$$

Етап 4. Оцінювання профілю інформаційної безпеки учасника інформаційної взаємодії (I_4). Розрахунок показника I_4 реалізований з використанням методу побудови профілів інформаційної безпеки учасників взаємодії [6]. Такий метод ґрунтується на технологіях інтелектуального аналізу даних (методах машинного навчання). Оцінка профілю інформаційної безпеки I_4 приймає значення у заданому діапазоні

$$I_4 \in [0; 1] \quad (4)$$

Варіант узагальнення загроз Інформаційні безпеці держави I_j , $j = \overline{1,4}$ та їх нормованих шкал оцінки наведено в табл. 1.

Етап 5. Встановлення вагових коефіцієнтів α_j ознак загроз Інформаційній безпеці держави. Такі вагові коефіцієнти встановлюються експертами на основі їх індивідуальних переваг і відповідають поточній ситуації у сфері інформаційної безпеки. Як варіант, вагові коефіцієнти ознак загроз Інформаційної безпеки держави можуть бути визначені за формулою [7]

$$\alpha_j \in \Gamma_\alpha, \Gamma_\alpha = \left\{ \alpha_j \geq 0, \sum_{j=1}^{m} \alpha_j = 1 \right\}, j \in [1; m] \quad (5)$$

Таблиця 1

Шкала оцінювання загроз ІБ

Прояв загроз	Шкала оцінки	Якісний показник рівня загрози
Організаційні ознаки загроз I_1	0	Відсутня
	1	Існує
Загрози у змісті текстового контенту I_2	0	Відсутня
	1	Існує
Прояв маніпуляцій I_3	0,91-1,00	Дуже висока
	0,75-0,90	Висока
	0,50-0,74	Значна
	0,21-0,49	Низька
	0,00-0,20	Дуже низька
Оцінка профілю ІБ користувача I_4	0,70-1,00	Дуже високий
	0,50-0,70	Високий
	0,40-0,50	Значний
	0,20-0,40	Допустимий
	0,00-0,20	Низький

Етап 6. Згортка показників загроз I за нелінійною схемою компромісів А. Вороніна. Багатокритерійна задача оцінки зводиться до моделі векторної оптимізації з різними ваговими коефіцієнтами ознак загроз Інформаційній безпеці держави [8].

$$\mathrm{I}^* = \arg\min_{I \in M} \sum_{j=1}^{m} \alpha_j \left(1 - I_j\right)^{-1} \quad (6)$$

Для якісної оцінки загроз проводиться нормування скалярної згортки (6) до мінімального значення [9]

$$I = 1 - \frac{1}{\mathrm{I}^*} \quad (7)$$

Отримане значення ставиться у відповідність якісній шкалі загроз (табл. 2), сформованій на основі оберненої нормованої шкали, запропонованої А. Вороніним [10]. У результаті моніторингу інформаційного простору з метою оцінювання загроз Інформаційній безпеці держави відбирається контент повідомлень і дані учасників взаємодії, які його поширюють. Такий текстовий контент досліджується на предмет наявності ознак проведення інформаційної операції, деструктивного інформаційного впливу на учасників, маніпуляцій суспільною думкою. На основі відібраних акаунтів учасників проводиться оцінювання їх профілів інформаційної безпеки.

Таблиця 2

Якісна шкала рівнів загроз

Рівень загрози	Інтервальні значення шкали оцінок
Існує	0,71-1,00
Вищий середнього	0,51-0,70
Нижчий середнього	0,31-0,50
Відсутній	0,00-0,30

Після аналізу предметної області експерт оцінює пріоритетність ознак загроз Інформаційній безпеці держави, на основі яких розраховуються значення вагових коефіцієнтів α_j. Сформований вектор ознак загроз I_j використовується для скалярної згортки по нелінійній схемі компромісів. На заключному етапі виконується перехід від числових значень I до якісної шкали оцінок рівня загроз Інформаційній безпеці держави. Отримані оцінки використовуються для вироблення рекомендацій щодо переходу інформаційної системи до бажаного стану інформаційної безпеки.

Отже, розглянута методика оцінювання загроз Інформаційної безпеки держави, який опирається на нелінійну схему компромісів і забезпечує підвищення ступеня обґрунтованості управлінських рішень та ефективність заходів інформаційної протидії загрозам.

Висновки

Досліджено методику оцінювання загроз Інформаційній безпеці держави, яка ґрунтується на нелінійній схемі компромісів і відрізняється від відомих врахуванням ознак використання соціальних ботів для проведення інформаційних операцій, інформаційних впливів на акторів за змістом текстового контенту, інформаційно-психологічного впливу і профілів ІБ акторів. Завдяки узагальненому показнику рівня загроз Інформаційної безпеки держави метод дозволяє обґрунтувати вибір ефективних заходів з інформаційної протидії для нейтралізації виявлених загроз та забезпечення заданого рівня Інформаційної безпеки держави.

Перелік посилань

1. Стратегія управління інформаційною безпекою / В.І. Андрєєв, В.Д. Козюра, Л.М. Скачек, В.О. Хорошко. – К.: ДУІКТ, 2007. – 272 с.
2. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, Політика інформаційної безпеки, К.: ПВП “Задруга”, 2015.
3. Хохлачова Ю.Є. Моделювання критеріїв оптимальності та обмежень для захисту інформаційних систем / Ю.Є. Хохлачова // Захист інформації. – 2012. - №4(57). – С. 106-109.
4. В. А. Ліпкан, “Сутність гібридної війни проти України”, Імперативи розвитку цивілізації, № 2, с. 13–16, 2015.
5. М. Панченко, та В. І. Полевий, “Методика виявлення ознак інформаційного впливу в засобах масової інформації”, Інформаційна безпека людини, суспільства, держави, № 3(7), с. 70–77, 2011.
6. Р. В. Грищук, та Ю. Г. Даник, Основи кібернетичної безпеки. Монографія, Житомир: ЖНАЕУ, 2016.
7. І. В. Замаруєва, В. Б. Толубко, Л. О. Литвиненко, та О. Ю. Ніколаєвський, “Модель лінгвістичної бази даних в системах автоматичної обробки природномовної текстової інформації”, Інформатика та математичні методи в моделюванні, т. 3, № 1, с. 75–81, 2013.
8. К. В. Молодецька-Гринчук, “Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками”, Радіоелектроніка, інформатика, управління, № 2(41), с. 117–126, 2017.
9. В. А. Ліпкан, І. М. Сопілко, та В. О. Кір’ян, Правові засади розвитку інформаційного суспільства в Україні, К.: ФОП О. С. Ліпкан, 2015.
10. В. К. Конах, Національний інформаційний простір України: проблеми формування та державного регулювання: аналіт. доп., К.: НІСД, 2014.
11. Cyber Security Strategy. [Online]. Available: https://www.enisa.europa.eu/ topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_ Strategy.pdf. Accessed: Nov. 10, 2017.
12. The UK Cyber Security Strategy. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/UK_ NCSS.pdf. Accessed: Nov. 10, 2017.
13. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, та С. В. Толюпа, Інформаційна та кібербезпека: соціотехнічний аспект, Ред. В. Б. Толубко, Київ: ДУТ, 2015.

Надійшла: 21.10.2022 Рецензент: д.т.н., професор Гайдур Г.І.