ISSN 2411-3816

УДК 004.413.4:004.056

О.В. Левченко,
кандидат військових наук, професор,
начальник Житомирського військового інституту
імені С.П. Корольова, м. Житомир,
Р.В. Грищук,
доктор технічних наук, старший науковий співробітник,
начальник науково-дослідного відділу наукового центру
Житомирського військового інституту
імені С.П. Корольова, м. Житомир,
О.В. Лагодний,
ад'юнкт науково-організаційного відділення
Житомирського військового інституту
імені С.П. Корольова, м. Житомир

УДОСКОНАЛЕНИЙ МЕТОД КОМПЛЕКСНОГО ОЦІНЮВАННЯ ОЗНАК ЗАГРОЗ ЦІЛЬОВІЙ АУДИТОРІЇ ЗА ДАНИМИ З МЕРЕЖІ ІНТЕРНЕТ

Актуалізація воєнних загроз державі в інформаційному просторі потребує розроблення нових підходів до захисту цільової аудиторії, на яку спрямований вплив. Пріоритетами державної політики щодо забезпечення інформаційної безпеки є створення інтегрованої системи оцінювання загроз та оперативного реагування на них, що досягається моніторингом засобів масової інформації й ресурсів мережі Інтернет. З метою реалізації зазначеного у статті розкрито сутність удосконаленого методу комплексного оцінювання ознак загроз цільовій аудиторії за даними з мережі Інтернет, який може бути покладений в основу спеціалізованого програмного забезпечення сучасних зразків озброєння.

Ключові слова: *загроза, мережа Інтернет, метод оцінювання, ознака, показник, рівень.*

Актуализация военных угроз государству в информационном пространстве требует разработки новых подходов к защите целевой аудитории, на которую направлено воздействие. Приоритетами государственной политики по вопросам обеспечения информационной безопасности является создание интегрированной системы оценивания угроз и оперативного реагирования на них. Решение указанных задач достигается путем мониторинга средств массовой информации и ресурсов сети Интернет. В статье раскрыта сущность усовершенствованного метода комплексной оценки признаков угроз целевой аудитории по данным из сети Интернет, который в будущем может стать основой для разработки специализированного программного обеспечения современных образцов вооружения.

Ключевые слова: *угроза, сеть Интернет, метод оценки, признак, показатель, уровень.*

Actualization of military threats to the state in the information space requires the development of new approaches to the protection of the target audience to which the

impact is directed. Priorities of the state policy on information security provision are the creation of an integrated threat assessment and rapid response system, achieved through media monitoring and Internet resources. The solution of these tasks is achieved by monitoring the media and Internet resources. The essence of the advanced method of complex evaluation of the threats to the target audience according to the data from the Internet, which may be the basis of the specialized software of modern weapons samples is revealed.

Keywords: *threat, Internet network, method of evaluation, sign, indicator, level.*

Постановка проблеми

Інформаційне протиборство є характерною ознакою сучасних локальних війн та збройних конфліктів [1–4]. Реалізація новітньої концепції війн гібридного типу перетворила інформаційний простір на ключову арену боротьби держав за власні національні інтереси. Яскравим прикладом цьому є агресія Російської Федерації проти України, яка, в першу чергу, почалася в інформаційному просторі та згодом призвела до анексії АР Крим та дестабілізації суспільно-політичної ситуації на Донбасі [5]. Основним об'єктом впливу у війнах нового типу, які використовують сучасні інформаційні технології, є індивідуальна та масова свідомість громадян, яких називатимемо цільовою аудиторією (ЦА). Зокрема, психологічні впливи (ПсВ) на ЦА здійснюються протиборчими сторонами для пропагування війни, розпалювання ворожнечі, підсилення панічних настроїв тощо [6].

Важливу роль у вирішенні зазначених вище завдань відіграє мережа Інтернет та ті дані, які в ній поширюються протиборчими сторонами. Як правило, загрози містяться в текстових повідомленнях, аудіо-, відеоданих тощо. Ефективна протидія таким загрозам потребує визначення загального рівня небезпеки за допомогою науково обґрунтованого методичного інструментарію, який ще й досі не є досконалим та перебуває на стадії розроблення. Інструментарій, що удосконалюється, у перспективі повинен стати основою спеціалізованого програмного забезпечення діючих та перспективних систем озброєння та військової техніки.

Огляд останніх досліджень і публікацій свідчить про те, що тема, яка розглядається, є достатньо актуальною. Їй присвячено значну кількість публікацій. Зокрема, в роботі [7] запропонована методика оцінювання кількісних показників негативного ПсВ, але не розкрито метод його визначення. Розкриті в [8] показники оцінювання відображені в кількісному вимірі та не узагальнені, що ускладнює їх сприйняття. Поданий у [9] підхід на основі експертного методу ґрунтується суто на суб'єктивних оцінках. Ефективність його практичного впровадження суттєво залежить від рівня кваліфікації експертів. Таким чином, кожен із проаналізованих методів та підходів має свої особливості, переваги й недоліки, а тому застосовується для вирішення вузькоспеціалізованих завдань. Отже, подальший розвиток методів оцінювання загроз за даними з мережі Інтернет є актуальним завданням, що потребує свого вирішення.

Метою статті є удосконалення методу комплексного оцінювання ознак загроз ЦА за даними з мережі Інтернет, який позбавлений від недоліків відомих методів.

Виклад основного матеріалу

Розглянемо відомі кільця впливу Уордена (рис. 1). Нехай кожному з кілець присвоюється деяка вага S_i, $i=\overline{1,5}$. Причому вага кілець є різною, тобто $S_1 < S_2 < ... < S_5$, де S_1 – особовий склад збройних сил, S_2 – населення держави,

S_3 – комунікаційна інфраструктура держави, S_4 – промисловість держави, S_5 – уряд держави [10; 11].

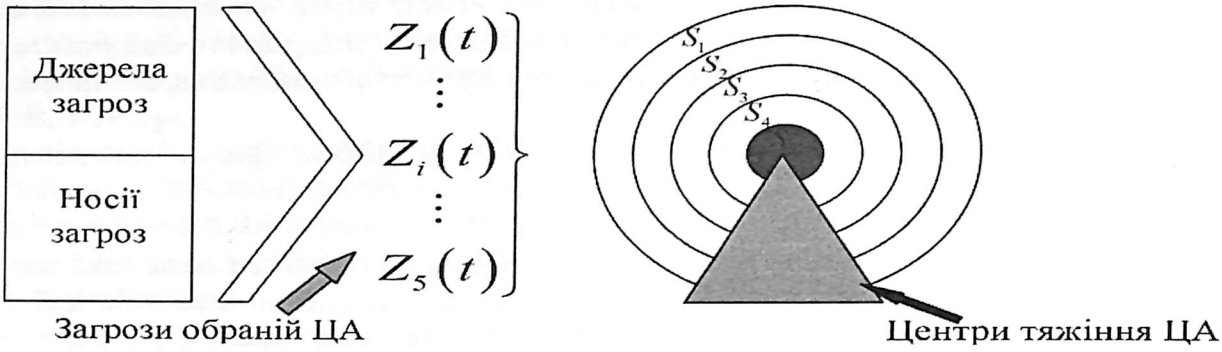

Рис. 1. Класична модель п'яти стратегічних кілець впливу Уордена

Визначимо для прикладу ознаки загроз для зовнішнього кільця з вагою S_1. Тобто як ЦА в подальшому оберемо особовий склад збройних сил. Тут і далі під ознаками загроз ЦА розуміються кількісні і якісні показники, які характеризують текстове повідомлення в мережі Інтернет, що містить ПсВ. Таким чином, сутність удосконалення методу, що розробляється, полягає у урахуванні одночасно кількісних і якісних характеристик ознак загроз та у подальшому їх комплексуванні в єдиний зведений показник рівня загрози.

Ураховуючі [6; 11], основними ознаками загроз можна вважати: значущість обраної ЦА; величину впливу джерела загроз; частоту оновлення інформації з ознаками маніпуляції; змістовність тематики.

Значущість обраної ЦА Rz_1 – це показник, що визначає пріоритетність захисту ЦА, у відношенні якої організовується інформаційна протидія.

Величина впливу джерела ознак загроз Rz_2 – це узагальнений показник, що характеризує популярність, рейтинг, кількість користувачів, поширеність, тематику новинних сайтів, які найбільш впливають на обрану ЦА.

Величина ознак загрози в текстовому повідомленні Rz_3, яка визначається за: *частотою оновлення інформації з ознаками маніпуляції* – це частота появи текстових повідомлень у мережі Інтернет з ознаками загроз маніпуляції, спрямованих на обрану ЦА за визначений проміжок часу; *змістовністю тематики текстового повідомлення* – це ступінь впливу теми текстового повідомлення з ознаками загроз на обрану ЦА, який визначається актуальністю теми повідомлення, його спрямованістю та семантичним забарвленням.

Таким чином, рівень загрози за даними з мережі Інтернет Rz у формалізованому вигляді за визначеними ознаками може бути описаний вектором

$$Rz = \langle Rz_1, Rz_2, Rz_3 \rangle. \quad (1)$$

З урахуванням (1) розроблено структурно-логічну схему методу, що удосконалюється, загальний вигляд якої подано на рис. 2. У кожному з наведених на рис. 2 блоків визначено вхідні дані, розкрито математичний апарат, що використовується для їх оброблення, та зазначено цільову функцію, одиниці вимірювання. Розкриємо сутність методу, виходячи з наведеної структурно-логічної схеми.

У першому блоці визначається рівень ознак загрози для обраної ЦА. Система, для якої досліджуються ознаки загроз, у формалізованому вигляді описується математичною моделлю зваженого орієнтованого графа

$$G=(S,P), \tag{2}$$

де S – множина вершин, що відповідають елементам системи $S \in \{S_i\}$, $i=\overline{1,5}$; P – множина зважених дуг, які відображають взаємозв'язки між елементами графа P_j, $j=1,8$ [12].

Вхідні дані для побудови графа (див. рис. 2, блок І) одержано за результатами оброблення даних експертного оцінювання, проведеного за 9-ти бальною шкалою (табл. 1).

На підставі отриманих даних побудовано матрицю зв'язків досліджуваної системи табл. 2, де кольором виділено досліджуваний елемент та його зв'язки в досліджуваній графовій моделі (див. рис. 2, блок І).

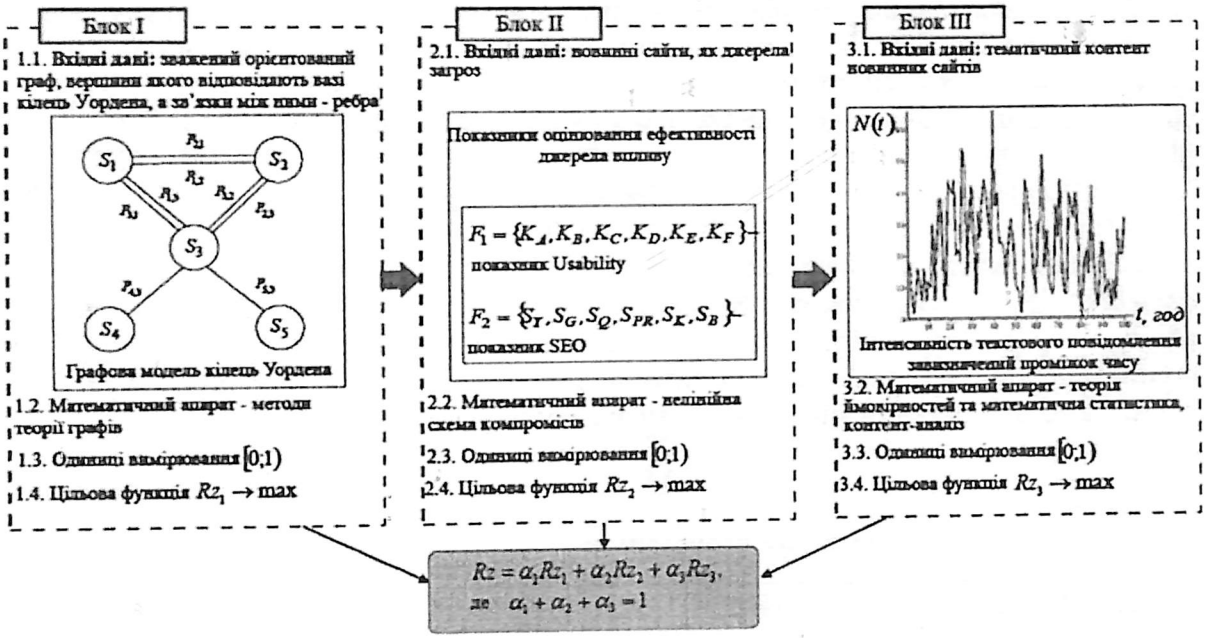

Рис. 2. Структурно-логічна схема удосконаленого методу комплексного оцінювання ознак загроз за даними з мережі Інтернет

Таблиця 1

Вихідні дані для побудови зваженого орієнтованого графа

S_i	Усереднена експертна оцінка (бали)	Ваговий коефіцієнт уразливості елемента	Ваговий коефіцієнт зав'язків елементів
S_1	8	0,35	P_{21}, P_{31}
S_2	6	0,25	P_{32}, P_{12}
S_3	4	0,17	$P_{13}, P_{23}, P_{43}, P_{53}$
S_4	3	0,13	
S_5	2	0,1	
$\sum$	23	1	

Таблиця 2

Матриця зв'язків досліджуваної системи

	s_1	s_2	s_3	s_4	s_5
s_1	S_1	$P_{1,2}$	$P_{1,3}$	0	0
s_2	$P_{2,1}$	S_2	$P_{2,3}$	0	0
s_3	$P_{3,1}$	$P_{3,2}$	S_3	0	0
s_4	0	0	$P_{4,3}$	S_4	0
s_5	0	0	$P_{5,3}$	0	S_5

За даними табл. 2 та [12] розраховується рівень ознаки загрози Rz_1 обраній ЦА S_1. У загальному вигляді він визначатиметься за величиною сукупного (повного) знищення досліджуваної системи, який складається зі збитку від виведення з ладу досліджуваної системи внаслідок прямого ураження її елементів Rz_1' та збитку, завданого внаслідок виникнення "каскадного ефекту" Rz_1'', тобто

$$Rz_1 = Rz_1' + Rz_1''. \quad (3)$$

Після розрахунку величини збитку від прямих і опосередкованих наслідків ураження ЦА S_1 виявленими ознаками загроз, отримання інтегральної оцінки рівня загрози відповідно до ситуації та її нормування – порівнюємо з фундаментальною нормованою інтервальною оберненою шкалою табл. 3 й отримуємо відповідний рівень загрози на обрану ЦА.

Таблиця 3

Фундаментальна нормована інтервальна обернена шкала

Інтервали шкали оцінювання	Категорія якості
1,00 – 0,71	Дуже високий
0,70 – 0,51	Високий
0,50 – 0,41	Значний
0,40 – 0,21	Помірний
0,20 і менше	Низький

У другому блоці визначається рівень ознак загрози джерела на обрану ЦА. Оцінювати ступінь важливості (рівень загрози джерела) пропонується за SEO та Usability показниками новинного сайту мережі Інтернет [13], які і є критеріями оцінювання. Встановлені критерії є суперечливими, що свідчить про необхідність приведення задачі оцінювання ефективності новинних сайтів як джерел ознак загроз до багатокритерійної форми. По кожному джерелу, яке вважається потенційно небезпечним і містить ознаки загроз обраній ЦА, проводиться розрахунок згідно з наведеним нижче виразом, методика якого подана в [14], тобто

$$Rz_2 = \sum_{l=1}^{k} \gamma_l^N \left(1 - Rz_{2l}^N\right)^{-1} \to \min, \quad (4)$$

де $l = 1 \ldots k$ – кількість включених у згортку часткових критеріїв SEO та Usability; γ_l^N – нормований ваговий коефіцієнт; Rz_{2l}^N – нормований частковий критерій оптимальності. Для оцінювання рівня ознак загроз з усього переліку джерел, які підлягають моніторингу за визначеним критерієм (4), обираємо ті, поріг яких перевищує 0,51, тобто $Rz_2 \geq 0{,}51$. Ознаки загроз, рівень яких виявився меншим за визначений поріг, не розглядаються, оскільки вважаються такими, що не становлять ознаки загрози. У підсумку для джерел, які містять ознаки, визначається усереднене значення загрози

$$Rz_2' = \frac{\sum_{i=2}^{m} Rz_{2_i}}{m}, \tag{5}$$

де m – кількість джерел, що містять ознаки загроз, $i = \overline{2,m}$. Отримана аналітична оцінка (5) співставляється з даними табл. 3, унаслідок чого визначається рівень ознаки загрози джерела Rz_2 на обрану ЦА S_1.

У третьому блоці визначається величина ознак загрози в текстовому повідомленні джерел, що містять ознаки загроз на обрану ЦА.

Кількісні і якісні показники, які характеризують зміст текстового повідомлення, пропонується визначати за показниками персистентності та наявності в змісті повідомлення ознак маніпуляції [15].

Нехай коефіцієнт спостережності джерела загрози K_c – це відношення кількості виявлених джерел загроз m, які оцінюються, до загальної кількості джерел спостереження M

$$K_c = \frac{m}{M}. \tag{6}$$

Частота публікації текстового повідомлення за досліджуваною тематикою C_i – це співвідношення кількості публікацій текстових повідомлень за досліджуваною тематикою n_i до загальної кількості публікацій N за усіма тематиками за визначений проміжок часу спостереження в виявлених джерелах загроз

$$C_i = \frac{n_i}{N}, \tag{7}$$

де n_i – i- а досліджувана тематика, $i = \overline{1,N}$.

Коефіцієнт тривалості публікації текстового повідомлення за досліджуваною тематикою K_t може бути визначеним як [16]

$$K_t = \frac{\Delta t}{\Delta t + a}, \tag{8}$$

де Δt – тривалість публікації текстових повідомлень за досліджуваною тематикою за визначений період, доба;

a – корегований коефіцієнт, який залежить від тривалості періоду моніторингу Δt.

Наявність маніпуляцій в текстових повідомленнях свідчить про посилення впливу на ЦА через обрані джерела загроз. Коефіцієнт маніпуляції K_{ps} – це відношення кількості текстових повідомлень, в яких виявлено ознаки маніпуляції w_k, до загальної кількості оцінених текстових повідомлень W за досліджуваною тематикою n_i у виявлених джерелах загроз, тобто

$$K_{ps} = \frac{\sum_{i=1}^{W} w_i}{W}. \quad (9)$$

Тоді, врахувавши (6) – (9), величина ознак загрози в текстовому повідомленні визнається співставленням значення виразу (10) з даними табл. 3

$$Rz_3 = K_c + C_i + K_t + K_{ps}. \quad (10)$$

Таким чином, загальний рівень ознак загроз ЦА за даними з мережі Інтернет за його складовими (3), (4), (5) та (10) розраховується як (див. рис. 2)

$$Rz = \alpha_1 Rz_1 + \alpha_2 Rz_2 + \alpha_3 Rz_3, \quad (11)$$

де α_i – i- й ваговий коефіцієнт важливості часткового показника рівня ознак загрози, $i = \overline{1,3}$, де $\sum_{i=1}^{3} \alpha_i = 1$. Одержана в результаті оцінювання кількісна оцінка рівня ознак загроз співставляється з якісною шкалою (табл. 4).

Таблиця 4

Якісна шкала рівнів загроз

Інтервальні значення шкали оцінок Rz	Рівень загрози
$0,7 \le Rz$	Високий
$0,5 \le Rz < 0,7$	Середній
$0,0 < Rz < 0,5$	Низький

Висновки та перспективи подальших досліджень. У результаті дослідження удосконалено метод комплексного оцінювання ознак загроз ЦА за даними з мережі Інтернет, який на відміну від відомих враховує: *ознаки загроз для обраної ЦА; ознаки загрози джерела на обрану ЦА; ознаки загрози в текстовому повідомленні*

джерел. Урахування запропонованих ознак дозволяє більш повно оцінювати рівень загроз обраній ЦА, чим сприяє підвищенню достовірності одержуваних оцінок та мінімізації їх залежності від суб'єктивного фактора.

Застосування на практиці розробленого методу дає змогу сформувати обґрунтовані пропозицій з протидії загрозам інформаційній безпеці держави у воєнній сфері. Подальші дослідження будуть спрямовані на практичну апробацію запропонованого методу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Підлісний А.Р.* Зміст і динаміка інформаційно-психологічного впливу США у військових операціях в Іраку (1990–2010 рр.). Вісник Національного університету "Львівська політехніка". 2012. № 724: Держава та армія. С. 221–228.
2. *Шумка А.В.* Інформаційне протистояння в ході грузинсько-російського конфлікту (8–12 серпня 2008 р.). Військово-науковий вісник. 2009. № 11. С. 254–260.
3. Конфликты и войны XXI века (Ближний Восток и Северная Африка). Институт востоковедения РАН. Москва: ИВ РАН, 2015. 504 с.
4. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп.; за заг. ред. А. Баровської. К.: НІСД, 2016. 109 с.
5. Світова гібридна війна: український фронт: монографія; за заг. ред. В.П. Горбуліна. Київ: НІСД, 2017. 496 с.
6. Про Доктрину інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017.
7. *Пузиренко О.Г., Іохов О.Ю., Горбов О.М.* та ін. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки. Системи озброєння і військова техніка. 2013. № 1. С. 123–128.
8. *Корченко А.Г., Иванченко Е.В., Казмирчук С.В.* Анализ и определение понятия риска для его интерпретации в области информационной безопасности. Науково-технічний журнал "Захист інформації". 2010. № 3. С. 1–5.
9. *Єрмошин В.В., Невойт Я.В.* Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем. Сучасний захист інформації. 2014. № 4. С. 12–22.
10. *Савин Л.В.* Сетецентричная и сетевая война. Введение в концепцию. Москва: Евразийское движение, 2011. 130 с.
11. *Певцов Г.В., Залкін С.В., Сідченко С.О.* та ін. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протиді. Наука і оборона. 2015. № 2. С. 28–32.
12. *Грищук Р.В., Чернишук С.В.* Методика оцінювання рівня небезпеки кібернетичних загроз. Сучасний захист інформації. Київ: ДУІКТ, 2013. Спецвипуск. С. 25–32.
13. *Даник Ю.Г., Писарчук О.О., Лагодний О.В.* та ін. Математична модель багатокритерійного оцінювання ефективності інтернет-сайтів цільового спрямування. Вісник ЖДТУ: нау. журнал. Житомир: ЖДТУ, 2016. № 1(76) С. 114–120.
14. *Воронин А. Н.* Нелинейная схема компромиссов в многокритериальных задачах оценивания и оптимизации. Кибернетика и системный анализ. 2009. Т. 45, № 4. С. 106–114.
15. *Грищук Р.В., Манько О.В., Орищук І.О.* Особливості організації та ведення моніторингу електронних засобів масової комунікації. Інформаційна безпека. 2014. № 3(15). С. 10–14.
16. *Левченко О.В., Косогов О.М., Сірик А.О.* Методика оцінювання кількісних показників негативного інформаційного впливу. Сучасні інформаційні технології у сфері безпеки та оборони. 2017. № 1(28). С. 31–35.

Отримано 13.11.2017
Рецензент Рибальський О.В., д.т.н., проф.