УДК 004.02:004.056

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

ФОРМАЛІЗОВАНА ПОСТАНОВКА НАУКОВОГО ЗАВДАННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ЗАГРОЗ ЗА ДАНИМИ З МЕРЕЖІ ІНТЕРНЕТ

У статті розкрито особливості ведення інформаційного протиборства в умовах гібридної війни з використанням мережі Інтернет, яка використовується як засіб для розповсюдження загроз психологічного впливу визначеній цільовій аудиторії. Обґрунтовано й доведено необхідність удосконалення математичного забезпечення діючих та перспективних зразків озброєння та військової техніки, які використовуються для вирішення завдань інформаційного протиборства.

Ключові слова: *загроза, Інтернет, математичне забезпечення, психологічний вплив.*

В статье приведены особенности ведения информационного противоборства в условиях гибридной войны с использованием сети Интернет как средства для распространения угроз психологического воздействия на целевую аудиторию. Обоснована и доказана необходимость совершенствования математического обеспечения современных образцов вооружения и военной техники для выполнения задач информационной борьбы.

Ключевые слова: *угроза, Интернет, математическое обеспечение, психологическое воздействие.*

Paper reveals the peculiarities of the conduction of information confrontation in a hybrid war with the use of the Internet, which is used as means to spread the threats of psychological impact on a specific audience. It is substantiated and proved the necessity of an improvement of the mathematical support of active and perspective models of weapons and military equipment used for solving information confrontation problems.

Keywords: *threat, Internet, mathematical support, psychological influence.*

Інформаційне протиборство є невід'ємною складовою інформаційної боротьби за національні інтереси. З метою ведення психологічних операцій під час інформаційного протиборства дедалі активніше й масштабніше застосовуються електронні засоби масової інформації й особливо ресурси мережі Інтернет. Діапазон використання мережі Інтернет достатньо широкий, що надає можливості для здійснення впливу на формування суспільної думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника та розповсюдження спеціально підготовленої інформації (дезінформації) тощо [1]. Тому формування обґрунтованих пропозицій із протидії психологічному впливу (ПсВ) можливе за умови ефективного виявлення ознак загроз, оцінювання їх рівня та прогнозування динаміки їх подальшого поширення.

Виконання зазначених завдань у збройних силах (ЗС) провідних держав покладається на підрозділи сил спеціальних операцій. Зокрема, до сьогодні ті

ЗС, які не мають належного фінансування, вирішували зазначені завдання в "ручному" режимі за рахунок залучення великої кількості операторів [2]. Такий підхід є досить суб'єктивним, а оцінки поточної ситуації не забезпечують належну достовірність, оперативність і ефективність виконання поставлених завдань. Таким чином, динамічна зміна ситуації в сучасних бойових діях потребує кардинального перегляду існуючих підходів до вирішення зазначеного завдання [3]. Зокрема, удосконалення потребує математичне забезпечення діючих зразків озброєння та військової техніки (ОВТ).

Огляд останніх досліджень і публікацій [4–10] засвідчив, що протиборство конфліктуючих сторін зміщено в бік невійськових способів досягнення мети, які за своєю ефективністю значно переважають силу зброї. Цей факт свідчить про постійне зростання ролі інформаційної складової. Так, інформаційне протиборство відкриває широкі можливості щодо зниження бойового потенціалу противника за рахунок проведення асиметричних заходів із використанням мережі Інтернет. З цією метою в [11–13] розкрито нові підходи, а також розроблено методики та методи із протидії деструктивному інформаційно-психологічному впливу під час проведення інформаційних та психологічних операцій. Наприклад, у [11] авторами запропоновано методику аналізу та оцінювання кількісних базових показників негативного інформаційного впливу. За такі показники обрано рівень інтенсивності, тривалість, поширеність джерела, масштабність об'єктів. У [12] запропоновано методику визначення рівня інформаційного впливу, яка ґрунтується не тільки на апріорних знаннях про дії противника, а й враховує інші додаткові дані. У [13] розкрито сутність методу захисту цільової аудиторії (ЦА) від негативного інформаційно-психологічного впливу, який враховує специфіку діяльності соціуму в інформаційному просторі. Отже, як засвідчив критичний аналіз наведених вище та інших публікацій за темою дослідження, окреслена вище проблема, незважаючи на її багатогранність, важливість для науки і практики, і надалі залишається актуальною, а тому потребує свого вирішення.

Метою статті є формалізована постановка наукового завдання для підвищення ефективності виявлення загроз за даними з мережі Інтернет.

Вище було показано, що зміна підходів до асиметричних способів ведення військових дій позначилася на оцінці ролі інформаційного протиборства в сучасних локальних війнах, збройних конфліктах та на переосмисленні заходів з організації інформаційної і кібернетичної безпеки держави [4; 5]. Нині існує дуже широкий спектр можливостей використання інформаційної зброї, що становить прецедент для досягнення перемоги без застосування традиційних засобів збройної боротьби.

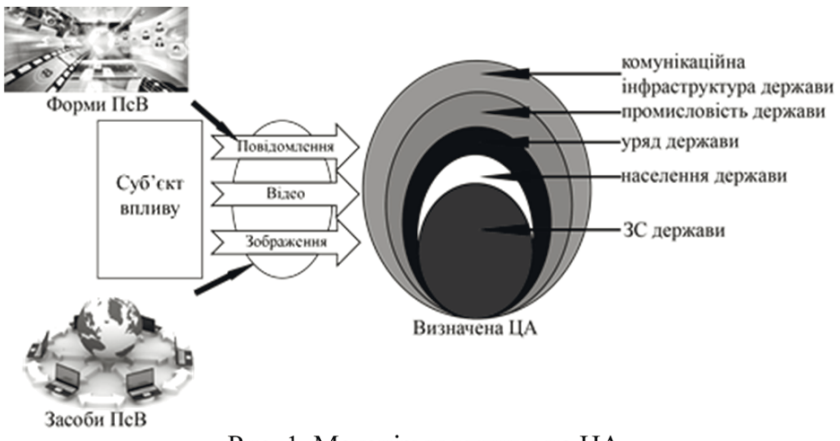

Рис. 1. Механізми впливу на ЦА

З огляду на досвід збройного конфлікту в Україні можна зробити висновок, що в зоні конфлікту особовий склад ЗС України був та залишається ЦА для здійснення ПсВ з боку супротивника через мережу Інтернет (рис. 1). Провідна роль при цьому відводиться загрозам текстового характеру, які у вигляді текстових повідомлень розміщуються на новинних сайтах та в соціальних мережах [3; 14; 15].

Діючі зразки ОВТ, які використовуються в зоні конфлікту, не призначені для вирішення завдань з інформаційного протиборства, оскільки їх математичне забезпечення не відповідає вимогам сучасності, а це, як наслідок, істотно знижує їх бойові можливості. Крім того, у спеціальних зразків ОВТ відсутні можливості щодо автоматизованого моніторингу даних з мережі Інтернет з метою виявлення ПсВ та здійснення аналізу виявлених загроз. Також істотним недоліком наявних зразків ОВТ є відсутність доступу до глобальної мережі Інтернет тощо. Отже, на сьогодні існує об'єктивне протиріччя між недосконалістю (відсутністю) математичного забезпечення діючих зразків ОВТ спеціального призначення та вимогами з ведення інформаційного протиборства на сучасному етапі (рис. 2).

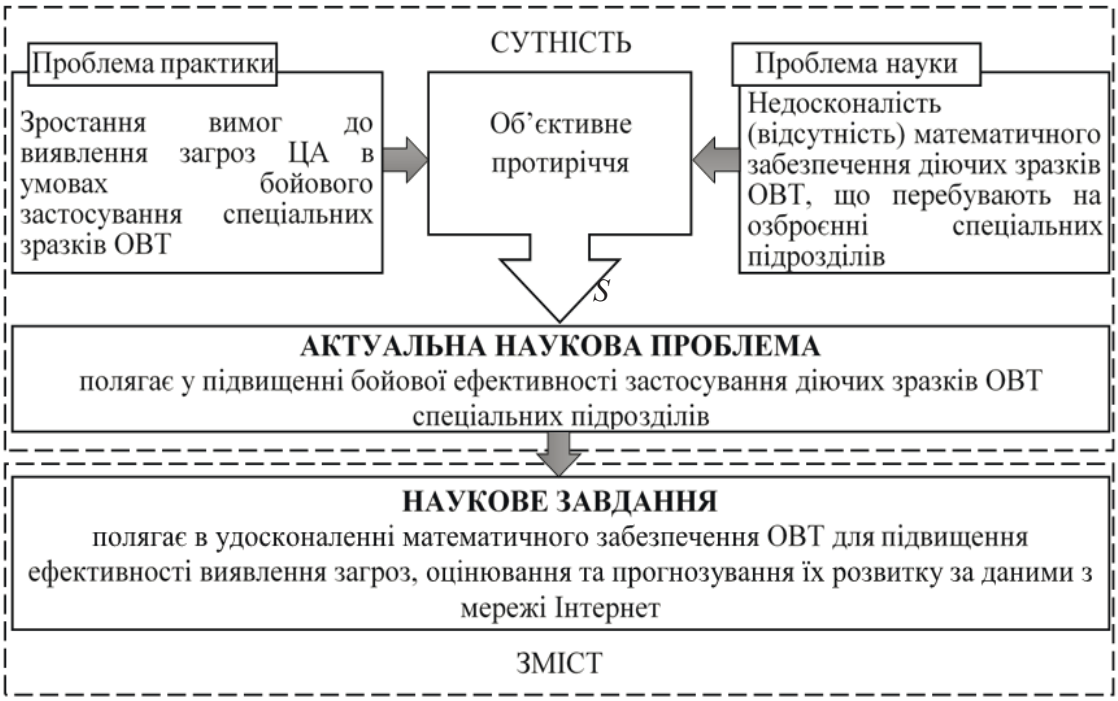

Рис. 2. Сутність і зміст наукового завдання

Для вирішення наукового завдання (див. рис. 2) спочатку пропонується розробити класифікатор ознак загроз за даними з мережі Інтернет, а на його основі модель джерела ПсВ на ЦА. Нехай існує множина загроз у мережі Інтернет $S = \{s_j\}, j = \overline{0, N}$; загрози ПсВ визначеній ЦА $S^O = \{s_q\}, q = \overline{0, n}, q \in j$ є підмножиною S. Потрібно вибрати загрози ПсВ визначеній ЦА S^O зі всієї множини загроз S за набором ознак, які заздалегідь формуються в класифікаторі ознак загроз, а саме

$$S^O = \left\{ s_i^O \in S \middle| P\left(s_i^O\right) \right\} = \left\{ s_i^O \middle| P\left(s_i^O\right) \right\}, \quad (1)$$

де S^O – множина загроз ПсВ визначеній ЦА, S – множина загроз в мережі Інтернет та $P\left(s_i^O\right)$ – ознаки, за якими здійснюється селекція загроз в мережі Інтернет, визначеній ЦА, на яку спрямований ПсВ.

Після отримання множини загроз ПсВ, визначеній ЦА, наступним кроком є їх оцінювання. Для оцінювання рівня загрози ПсВ, визначеній ЦА, Rz врахуванню має підлягати множина коефіцієнтів $K=\left\{Rz_1, Rz_2, Rz_3\right\}$, де Rz_1 – це ознаки загроз для обраної ЦА; Rz_2 – це ознаки загрози джерела для обраної ЦА; Rz_3 – ознаки загрози в текстовому повідомленні, які надходять від джерел з мережі Інтернет. За отриманою оцінкою рівня загрози визначеній ЦА приймається рішення висновок про небезпеку ПсВ вигляду

$$Rz \in X, \quad X\left[0;1\right), \tag{2}$$

де X – інтервальна оцінка, що відповідає визначення рівню ознак загроз.

На останньому кроці доцільно провести розрахунок показника Херста H для тематичного контенту, який містить ознаки загрози ПсВ визначеній ЦА [16]. Якщо показник Херста задовольняє умови персистентності, то тоді доцільно проводити статистичний аналіз активності тематичного контенту для отримання критеріїв нелінійних моделей $F\left(m_i\right)$, за якими обирається з множини моделей M модель m_i щодо проведення прогнозу поширення загроз в тематичному контенті мережі Інтернет вигляду

$$M=\left\{m_i\right\}, m_i \in M \left| F\left(m_i\right)\right., \tag{3}$$

де $\left(m_i\right)$ це: m_y – оцінка математичного сподівання моделі; σ_y – оцінка середнього квадратичного відхилення моделі; R^2 – достовірність апроксимації моделі фактичним даним. Обрана модель на інтервалі прогнозування T_p повинна забезпечувати максимальний інтервал прогнозу t_y та мінімальну похибку MSE, тобто

$$\begin{cases} t_y \to \max; \\ MSE \to \min; \end{cases} \Rightarrow \text{для } T_p. \tag{4}$$

Таким чином, наукове завдання з підвищення ефективності виявлення загроз, оцінювання та прогнозування їх розвитку за даними з мережі Інтернет з урахування (1)–(4) у формалізованому вигляді визначається як

$$\begin{cases} S^O=\left\{s_i^O \in S \left| P\left(s_i^O\right)\right.\right\}=\left\{s_i^O \left| P\left(s_i^O\right)\right.\right\}, \\ Rz \in X, X\left[0;1\right), \\ M=\left\{m_i\right\}, m_i \in M \left| F\left(m_i\right)\right., \\ \text{за умови} \begin{cases} t_y \to \max; \\ MSE \to \min; \end{cases} \Rightarrow \text{для } T_p. \end{cases} \tag{5}$$

Для досягнення мети поставленого наукового завдання побудовано структурно-логічну схему проведення дослідження (рис. 3). Ця схема систематизує сутність та зміст проведення етапів дослідження.

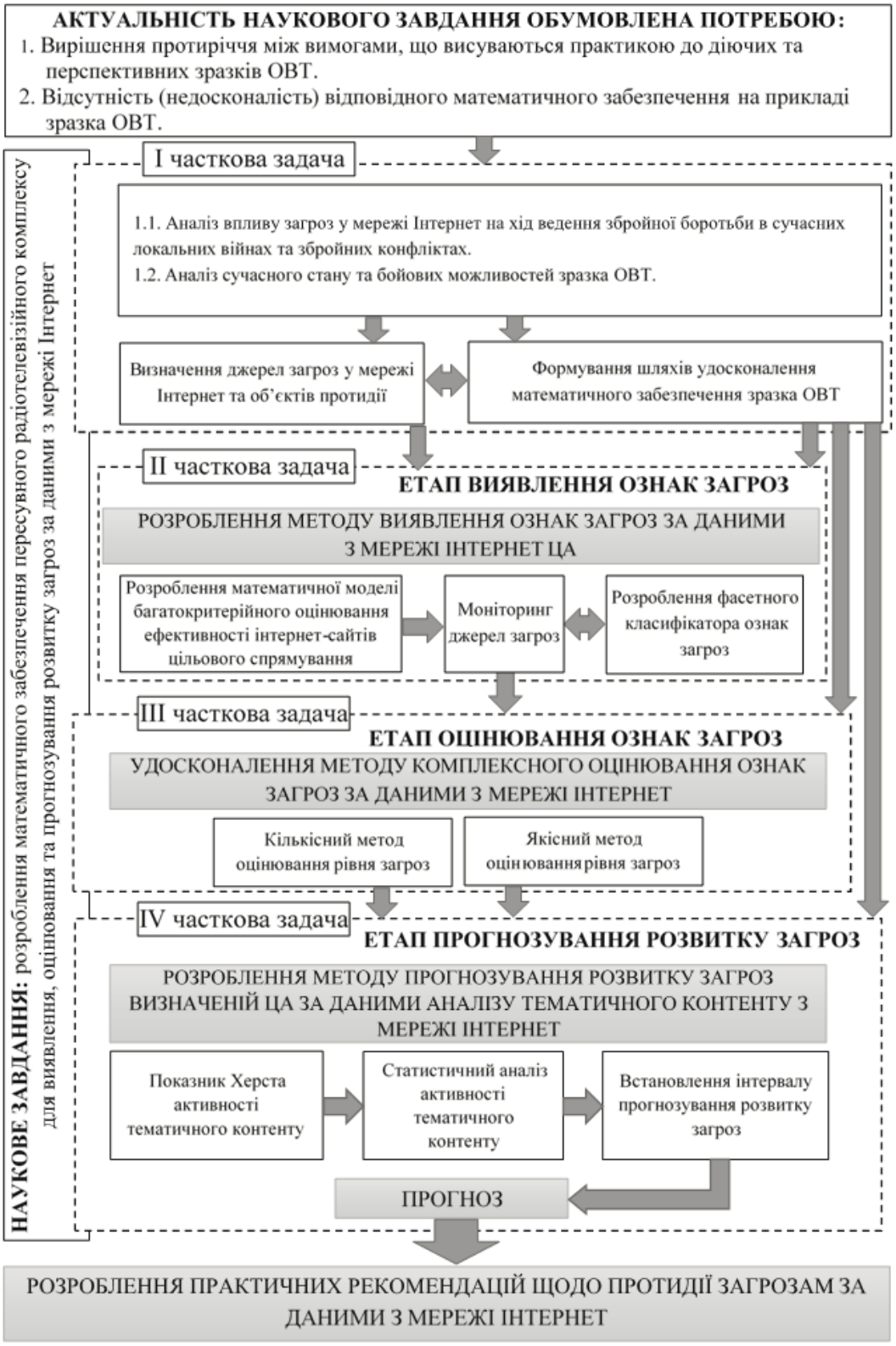

Рис. 3. Структурно-логічна схема проведення дослідження

У статті наведено формалізовану постановку наукового завдання, яке полягає в підвищенні ефективності бойового застосування діючих та перспективних зразків ОВТ, шляхом удосконалення їх математичного забезпечення. Результатом проведення дослідження будуть практичні рекомендації із протидії виявленим загрозам.

Перспективою подальших досліджень є створення спеціального програмного забезпечення на основі розробленого математичного забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Почепцов Г.* Сучасні інформаційні війни. Київ: Дім "Києво-Могилянська академія", 2015. 497 с.
2. *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.
3. *Грищук Р.В., Орищук І.О., Савчук В.С.* Аналіз ролі й місця сил та технічних засобів психологічних операцій в локальних війнах та збройних конфліктах сучасності. Інформаційні технології у сфері безпеки та оборони. К.: НУОУ, 2017. № 1. С. 27–30.
4. *Грищук Р.В., Даник Ю.Г.* Основи кібернетичної безпеки: монографія / за заг. ред. проф. Ю.Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.
5. Про Доктрину інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017.
6. *Макаренко С.И.* Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: монография. СПб.: Наукоемкие технологии, 2017. 546 с.
7. Конфликты и войны XXI века (Ближний Восток и Северная Африка) / Институт востоковедения РАН. М.: ИВ РАН, 2015. 504 с.
8. *Расторгуев С.П., Литвиненко М.В.* Информационные операции в сети Интернет / под общ. ред. А.Б. Михайловского. М.: АНО ЦСОиП, 2014. 128 с.
9. *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.
10. *Певцов Г.В., Гордієнко А.М., Залкін С.В.* та ін. Досвід і концепції ведення інформаційної боротьби у провідних країнах світу. Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 1(18). С. 12–16.
11. *Левченко О.В., Косогов О.М., Сірик А.О.* Методика оцінювання кількісних показників негативного інформаційного впливу. Інформаційні технології у сфері безпеки та оборони. 2017. № 1(28). С. 31–35.
12. *Кацалап В.О.* Методика оцінювання рівня інформаційного впливу на особовий склад Збройних Сил України в ході проведення антитерористичної операції. Імперативи розвитку цивілізації: матеріали міжвідомчої науково-практичної конференції "Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку". К.: ФОП О. С. Ліпкан, 2015. № 2. С. 38–42.
13. *Шиян А.А.* Метод захисту людини від негативного іфнормаційно-психологічного впливу на основі типології діяльності. Інформаційна безпека. 2014. № 3(15). С. 92–98.
14. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с.
15. Cyber and Information warfare in the Ukrainian conflict. Center for Security Studies (CSS), ETH Zurich. 2107. URL: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf (дата звернення: 07.11.2017).
16. *Ланде Д.В.* Фрактальные свойства тематических информационных потоков в Интернете. Реєстрація, зберігання і обробка даних: наук-техн. журнал. К.: ІПРІ НАНУ, 2006. № 2 (Т. 8). С. 93–99.

Отримано 27.12.2017
Рецензент Рибальський О.В., д.т.н., проф.