УДК 354.42

Олександр Віталійович Левченко *(канд. військ. наук, професор)*[1]
Олександр Миколайович Косогов *(канд. військ. наук, стар. наук. співр.)*[2]
Анатолій Олександрович Сірик[3]

[1]***Житомирський військовий інститут імені С.П. Корольова, Житомир, Україна***
[2,3]***Військова частина А1906, Київ, Україна***

МЕТОДИКА ОЦІНЮВАННЯ КІЛЬКІСНИХ ПОКАЗНИКІВ НЕГАТИВНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ

На основі комплексного аналізу заходів негативного інформаційного впливу запропоновано методику аналізу та оцінювання його кількісних базових показників (рівень інтенсивності, тривалість, поширеність джерела, масштабність об'єктів). Методика базується на згортці цих показників у вигляді нормованого узагальненого показника рівня негативного інформаційного впливу, який ставиться у відповідність до певної його форми (інформаційна атака, інформаційна акція, інформаційна операція, інформаційна кампанія). За значенням нормованого комплексного показника визначається рівень інформаційної загрози і він може бути: низьким, підвищеним, високим та критичним.

Методика може бути використана для розробки системи заходів протидії негативному інформаційному впливу.

Ключові слова: *інформаційний вплив, інформаційні загрози, аналіз та оцінювання загроз, інформаційні заходи.*

Вступ

Постановка проблеми.

Активне реформування воєнної організації держави з урахуванням досвіду антитерористичної операції (АТО) потребує адаптації наукових розробок, зокрема з питань виявлення, аналізу та оцінювання інформаційних загроз (ІЗ) Україні у воєнній сфері, до механізмів реалізації рішень вищого воєнно-політичного керівництва України.

Зазначений процес є найбільш характерним для особливого періоду, коли негативний інформаційний вплив (ІВ) противника став реальним явищем. Для періоду мирного часу необхідно проводити попереджувальні заходи на основі моніторингу інформаційного простору воєнної сфери, коли факту впливу ще немає, але є ситуація можливого виникнення ІЗ [1].

Зважаючи на вищенаведене, необхідним для визначення подальших шляхів удосконалення науково-методичного забезпечення процесу виявлення, аналізу та оцінювання ІЗ у воєнній сфері є проведення системного аналізу основних ІЗ державі у воєнній сфері з урахуванням особливостей, якісних та кількісних характеристик негативного ІВ та розроблення відповідної методики.

Аналіз останніх досліджень та публікацій. Аналіз спеціалізованої літератури, наприклад [2–5], показує, що на сьогодні у нашій державі та її Збройних Силах триває інтенсивний процес формування системи інформаційної безпеки, зокрема у Міністерстві оборони України розроблені концептуальні документи та плани щодо розгортання такої системи. У Збройних Силах України створюються відповідні підрозділи. Разом з тим, методичне забезпечення ефективного аналізу та оцінювання ІЗ державі в особливий період, в умовах якого цільовою аудиторією такого впливу розглядається особовий склад військ (сил) та органи військового управління, а об'єктами інформаційно-технічного впливу – засоби управління військами та зброєю, вивчено недостатньою мірою.

Тому розробка методики аналізу та оцінювання кількісних показників негативного ІВ є актуальним науково-практичним завданням.

Метою статті є викладення методики аналізу та оцінювання кількісних показників негативного ІВ.

Виклад основного матеріалу дослідження

В основу аналізу та оцінювання кількісних показників негативного ІВ покладено узагальнення за певний відрізок часу результатів щоденного моніторингу джерел інформації. Мінімальним відрізком часу доцільно вважати тиждень, оскільки за менший період неможливо виявити системність негативного ІВ, визначити форму його здійснення. Поглиблений аналіз зовнішнього негативного ІВ доцільно проводити за місяць, квартал, півріччя, рік.

Вихідними даними для методики є результати виявлення заходів негативного ІВ, що викладена в [6]. Методика аналізу та оцінювання кількісних показників негативного ІВ передбачає такі основні етапи.

Етап 1. Визначення напрямів здійснення інформаційного впливу

На цьому етапі виявлені заходи ІВ групуються за спорідненими темами, і таким чином формуються напрями здійснення ІВ.

Напрями ІВ визначаються експертним шляхом окремо за кожною сферою життєдіяльності держави згідно із Законом України "Про основи національної безпеки України".

Кількість цих напрямів і їх наповнення можуть бути різними, залежно від умов обстановки, конкретних країн, від яких надходить негативний ІВ, та інших чинників.

Варіант можливих напрямів негативного ІВ стосовно об'єктів (цільової аудиторії) воєнної сфери життєдіяльності держави наведено в табл. 1.

Таблиця 1

Можливі напрями негативного інформаційного впливу стосовно об'єктів (цільової аудиторії) воєнної сфери (варіант)

№ напряму	Зміст напряму реалізації ІЗ державі
1	Розповсюдження інформації (дезінформація або спотворення інформації), що дискредитує військове керівництво та збройні сили держави
2	Інформаційні повідомлення (коментарі) та заяви офіційних (неофіційних) осіб іноземних держав в ЗМІ щодо дискредитації антитерористичної операції (далі – АТО)
3	Інформаційне насичення інформаційного простору інформаційними повідомленнями, які спрямовані на деморалізацію особового складу силових структур, що задіяний в АТО
4	Поширення інформації в ЗМІ щодо підбурювання зриву мобілізаційних заходів в Україні
5	Поширення викривленої, недостовірної та упередженої інформації, яка дискредитує військові формування, військову службу та військовий обов'язок
6	Поширення інформації іноземними ЗМІ щодо недопущення надання військової допомоги Україні лояльними до неї країнами
7	Інформаційні повідомлення (коментарі) та заяви офіційних (неофіційних) осіб іноземних держав в ЗМІ щодо звинувачення особового складу силових структур у причетності до незаконних дій в зоні конфлікту (участь у контрабанді, продаж озброєння та техніки)

Етап 2. Визначення та оцінювання базових показників для кожного напряму інформаційного впливу

Основними базовими показниками, які характеризують негативний ІВ, є:

1) рівень інтенсивності ІВ – K_i;

2) тривалість ІВ – $K_т$;

3) поширеність джерела ІВ – $K_д$;

4) масштабність об'єктів ІВ – $K_о$.

Рівень інтенсивності негативного ІВ K_i відображає ступінь негативності інформаційних заходів суб'єкта впливу (держави, організації) за певний проміжок часу. Він визначається як співвідношення кількості негативних інформаційних повідомлень до загальної кількості повідомлень, виявлених протягом певного періоду за одним визначеним вище напрямом, та виражається у відсотковому або коефіцієнтному вигляді:

0 – 0,2 (до 20% негативних повідомлень у загальній кількості повідомлень за визначений період) – низька інтенсивність;

0,2 – 0,4 (від 20% до 40% негативних повідомлень від загальної кількості повідомлень за визначений період) – середня інтенсивність;

0,4 – 0,6 (від 40% до 60% негативних повідомлень від загальної кількості повідомлень за визначений період) – підвищена інтенсивність;

0,6 – 0,8 (від 60% до 80% негативних повідомлень від загальної кількості повідомлень за визначений період) – висока інтенсивність;

0,8 – 1 (від 80% до 100% негативних повідомлень від загальної кількості повідомлень за визначений період) – критична інтенсивність.

Тривалість негативного інформаційного впливу $K_т$ – показник, який відображає період, упродовж якого спостерігається активна стадія впливу. Для спрощення процесу визначення форми ІВ доцільно встановити такі періоди його тривалості: від декількох днів до тижня; від декількох тижнів до декількох місяців; від місяця до декількох місяців; від декількох місяців до декількох років.

Коефіцієнт тривалості зовнішнього негативного ІВ $K_т$ обчислюється за допомогою залежності, яка близька до логарифмічної функції. Вона описується рівнянням:

$$K_т = \frac{x}{x + a} \qquad (1)$$

де x – тривалість негативного ІВ у календарних днях;

a – постійний коефіцієнт, який для періоду часу від декількох днів до року включно дорівнює 40,56; більше року – 19,21.

З урахуванням значень постійного коефіцієнта a рівняння (1) матиме такий вигляд:

для періоду часу від декількох днів до року включно

$$K_т = \frac{x}{x + 40{,}56} \qquad (2)$$

для періоду часу більше року

$$K_{т} = \frac{x}{x + 19{,}21} \quad (3)$$

Числові значення коефіцієнта тривалості, залежно від періоду часунегативного ІВ, наведені у табл. 2.

Таблиця 2

Відповідність коефіцієнтів тривалості до періодів часу негативного інформаційного впливу

Період часу негативного ІВ	Коефіцієнт тривалості ІВ $K_{т}$
Тиждень (7 днів)	0,15
Декілька тижнів (14 днів)	0,26
Місяць (31 день)	0,43
Квартал (92 дні)	0,7
Дев'ять місяців (273 дні)	0,87
Рік (365 днів)	0,9
Два роки (730 днів)	0,97

Масштабність об'єктів ІВ $K_{о}$ – показник, який відображає максимально можливу кількість об'єктів, на які спрямовується ІВ, і визначається експертним шляхом:

а) одиночний об'єкт впливу – особа, яка приймає важливі рішення у воєнній сфері або визначальні структурні підрозділи у воєнній сфері;

б) груповий об'єкт впливу – являє собою групу одиночних об'єктів, об'єднаних єдиною цільовою функцією та зв'язками між собою;

в) масовий об'єкт впливу – сукупність одиночних та групових об'єктів, об'єднаних єдиною цільовою функцією та зв'язками між ними.

Масштабності об'єктів ІВ $K_{о}$ надаються такі числові значення:

одиночний об'єкт впливу – 0,1 – 0,3;

груповий об'єкт впливу – 0,3 – 0,7;

масовий об'єкт впливу – 0,7 – 1;

Конкретне числове значення в зазначених межах визначається методом експертних оцінок офіцерами-аналітиками.

Поширеність джерела ІВ $K_{д}$ – показник, який характеризує його якісну оцінку і означає обсяг охоплення цільової аудиторії та визначається експертним шляхом. За поширеністю джерел ІВ може мати такі масштаби: місцевий, регіональний, загальнодержавний та міжнародний, а числові їх значення приймаються такими:

а) місцевий масштаб – 0,25;

б) місцевий та регіональний масштаби (в межах окремого регіону держави) – 0,5;

в) місцевий, регіональний та загальнодержавний масштаби – 0,75;

г) місцевий, регіональний, загальнодержавний та міжнародний масштаби – 1,0.

Етап 3. Визначення форми інформаційного впливу (інформаційна атака, інформаційна акція, інформаційна операція, інформаційна кампанія)

Для кожного напряму ІВ визначається нормований узагальнений показник рівня негативного ІВ:

$$\overline{K}_{j}^{n} = \sum_{j=1}^{4} \frac{K_{j}}{\sqrt{\sum_{j} K_{j}^{2}}} \quad (4)$$

де:

K_{j} – базові показники негативного ІВ (K_{i} – рівень інтенсивності негативного ІВ; $K_{т}$ – тривалість негативного ІВ; $K_{д}$ – поширеність джерела ІВ; $K_{о}$ – масштабність об'єктів ІВ);

n – кількість напрямів ІВ за сферами.

За результатами обчислення нормованого узагальненого показника рівня негативного ІВ визначається форма ІВ.

Залежність форми ІВ від базових показників, кількості напрямів ІВ та $\overline{K}_{j}^{n}$ наведено у табл. 3.

Етап 4. Визначення рівня інформаційних загроз

1. Для кожної сфери, що підлягає аналізу, обчислюється нормований комплексний показник інформаційної загрози державі:

$$\overline{Z}_{n}^{c} = \sum_{n=1}^{N} \frac{\overline{K}_{j}^{n}}{\sqrt{\sum_{j} K_{j}^{2}}} \quad (5)$$

де $\overline{K}_{j}^{n}$ – нормований узагальнений показник рівня негативного ІВ n-го напряму c-ї сфери, розрахований на етапі 3;

n – кількість напрямів c-ї сфери.

2. Рівень інформаційної загрози державі в обраній сфері встановлюється шляхом зіставлення обчисленого нормованого комплексного показника $\overline{Z}_{n}^{c}$ зі значеннями, наведеними у табл. 3 і може бути: низьким, підвищеним, високим та критичним.

Таблиця 4

Значення показників рівня інформаційної загрози

Межі значень показника рівня ІЗ	Показник рівня ІЗ
0 – 0,25	низький
0,26 – 0,5	підвищений
0,51 – 0,75	високий
0,76 – 1,0	критичний

Висновки й перспективи подальших досліджень

Методика аналізу та оцінювання кількісних показників негативного інформаційного впливу дає змогу аналізувати та оцінювати інформаційні загрози державі у воєнній сфері за якісними та кількісними показниками, визначати форми інформаційного впливу з боку іншої держави з урахуванням його базових показників (інтенсивність, тривалість, поширеність джерел, масштабність об'єктів впливу), визначати рівень інформаційних загроз державі з використанням нормованого комплексного показника рівня інформаційної загрози.

У подальшому доцільно спрямувати дослідження застосування методики для розробки системи заходів протидії негативному інформаційному впливу.

Таблиця 3

Залежність форми інформаційного впливу від базових показників, кількості напрямів інформаційного впливу та значень $\overline{K}_j^n$

Форма ІВ	Кількість напрямів ІВ	Рівень інтенсивності ІВ		Тривалість ІВ		Поширеність джерел ІВ		Масштабність об'єктів ІВ		Межі значень (формула 4) $\overline{K}_j^n$
		лінгвістична змінна	числове значення	лінгвістична змінна	числове значення	лінгвістична змінна	числове значення	лінгвістична змінна	числове значення	
Інформаційна атака	один напрям	середній	0,2 – 0,4	декілька днів – тиждень	0,15	місцеві та регіональні джерела	0,25 – 0,5	одиночний об'єкт	0,1 – 0,3	до 0,34
Інформаційна акція	один напрям	підвищений	0,4 – 0,6	від декількох тижнів до декількох	0,26 – 0,7	місцеві, регіональні та загальнодержавні джерела	0,5 – 0,75	одиночний об'єкт/ груповий об'єкт	0,1 – 0,3 0, 3– 0,7	0,37 – 0,69
Інформаційна операція	один або декілька напрямів у одній сфері	підвищений, високий	0,4 – 0,6 0,6 – 0,8	від місяця до декількох місяців	0,43 – 0,7	місцеві, регіональні, загальнодержавні та міжнародні джерела	0,75 – 1,0	груповий об'єкт/ масовий об'єкт	0,3 – 0,7 0,7 – 1	0,62 – 0,88
Інформаційна кампанія	декілька напрямів у різних сферах	високий, критичний	0,6 – 0,8 0,8 – 1	від декількох місяців до декількох років	0,7 – 0,97	місцеві, регіональні, загальнодержавні та міжнародні джерела	0,75 – 1,0	масовий об'єкт	0,7 – 1	0,69 – 1,0

Література

1. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навч. посіб. / В. М. Петрик, О. А. Штоквиш, В. І. Полевий та ін. – К. : Росава, 2006. – 208 с. – С. – 32–33.

2. Левченко О. В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки / О. В Левченко // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. № 3 (20). – С. 47 – 50.

3. Ланде Д. Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет-ресурсів / Д. Ланде, В. Фурашев // Правова інформатика. – 2009. – № 2 (22). – С. 49–57.

4. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: моногр. / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

5. Литвиненко О.В. Інформаційні впливи та операції: теорет.-аналіт. Нариси Methods, means and measures for ensuring information-psychological security of person, society, country Information Security of the Person, Society and State № 3 (7) 2011 77 / О. В. Литвиненко. – К. : Нац. ін-т стратег. дослідж., 2003. – 239 с. – (Вип. 6 : Сер. Нац.безпека).

6. Косогов О. М. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел / О. М. Косогов, О. В. Левченко // Системи обробки інформації : збірник наукових праць. – Х. Харківський університет Повітряних Сил імені Івана Кожедуба. – 2016. Вип. 1 (138). – С. 100–102.

МЕТОДИКА ОЦЕНКИ КОЛИЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ НЕГАТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

***Александр Витальевич Левченко** (канд. воен. наук, профессор)[1]*
***Александр Николаевич Косогов** (канд. воен. наук, стар. науч. сотр.)[2]*
***Анатолий Александрович Сирык**[3]*

[1]Житомирский военный институт имени С.П. Королева, Житомир, Украина
[2,3]Войсковая часть А1906, Киев, Украина

На основе комплексного анализа мероприятий негативного информационного воздействия предложена методика анализа и оценки его количественных базовых показателей (уровень интенсивности, продолжительность, распространенность источников, масштабность объектов). Методика базируется на свертке этих показателей в виде нормированного обобщенного показателя уровня негативного информационного воздействия, который соответствует его определенной форме

(информационная атака, информационная акция, информационная операция, информационная кампания). По значению нормированного комплексного показателя определяется уровень информационной угрозы, и он может быть: низким, повышенным, высоким и критическим.

Методика может быть применена для определения системы мероприятий противодействия негативному информационному воздействию.

Ключевые слова: *информационное воздействие, информационные угрозы, анализ и оценка угроз, информационные мероприятия.*

ASSESSMENT METHOD QUANTITATIVE INDICATORS OF NEGATIVE INFORMATION INFLUENCE ITS IMPLEMENTATION IN FORM

Oleksandr V. Levchenko *(Candidate of Military Sciences, Professor)*[1]
Oleksandr M. Kosogov *(Candidate of Military Sciences, Senior Research Fellow)*[2]
Anatoliy O. Siryk [3]

[1]*ZhytomyrMilitaryInstitutenamedafter S. P. Korolyov, Zhytomyr, Ukraine*
[2,3]*Military Unit A1906, Kyiv, Ukraine*

Based on comprehensive analysis measures negative information influence the method of analysis and evaluation of its quantitative based indicators (level of intensity, prolongation, influence, scale of objects). The technique is based on shorts baseline in normalized form of generalized indicator of the negative impact of the information that is associated with it in some form (information attack, information action, information operation, information campaign). For the normalized value of the composite indicator determines the level of threat information (lower, high, higher, critical).

The method can be used for the development of measures to counteract negative information influence.

Keywords: *information impact, threat information, analysis and assessment of threats, information events.*

References

1. Modern technologies and means of manipulation, information warfare and special operations information: Navch.posib. / V.M. Petryk, O. A. Shtokvysh, V. I. Polevyyetc. – K : Rosava, 2006. – 208 p. – pp. 32–33.

2. Levchenko A. V. Conceptual approach to a comprehensive assessment of information security / A. V. Levchenko // Science and Technology of the Air Force of Ukraine. – 2015. № 3 (20).– pp. 47 – 50.

3. D. Lande Information operations through the prism monitoring and integration of Internet resources / D. Lande, V. Furashev // Legal Informatics. – 2009. – № 2 (22). – pp. 49–57.

4. Gorbulin V. P. Information operations and safety of society, threats, resistance, design, monogram. / V. P. Horbulin, O. H. Dodonov, D. V. Lande. – K : Intertehnolohiya, 2009. – 164 p.

5. Litvinenko O. V. Information influences and operations: teoret.-analyte. Essays on Methods, means and measures for ensuring information-psychological security of person, society, country Information Security of the Person, Society and State № 3 (7) 2011 77 / O. V. Lytvynenko. – K: Nat. strateh. doslidzh Inst., 2003. – 239 p. – (Vol. 6: Avg. Nats. bezpeka).

6. Kosogov O. M. Methods of detecting negative information influence events by analyzing open source / O. M. Kosogov, O. V Levchenko // Information processing systems: technologies. – H. Kharkiv Air Force University named after Ivan Kozhedub. – 2016.Vyp. 1 (138). – pp. 100–102.