

ФІЛОСОФІЯ, МЕТОДОЛОГІЯ, ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ

Кацалан В.О.,

*кандидат військових наук, старший науковий співробітник
науково-дослідного відділу проблем інформаційної безпеки та суспільної
актуалізації воєнної політики Центру воєнно-стратегічних досліджень
Національного університету оборони України імені Івана Черняхівсько*

МЕТОДИЧНИЙ ПІДХІД ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОГО ВПЛИВУ НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ)

Розглянуто можливість оцінки елементів інформаційної безпеки України у воєнній сфері в умовах інформаційної протидії. Аналізуються рівні виникнення ймовірних інформаційних загроз для особового складу на основі використання інформації про інформаційно-психологічний вплив противника.

Ключові слова: *інформаційна безпека, інформаційно-психологічний вплив, інформаційні акції (атаки)*

The possibility of evaluation of elements of the information security of Ukraine in the military sphere in the information counter. Analyzed the levels of the probable information threats to personnel on the basis of information about information-psychological influence of the enemy.

Keywords: *information security, information-psychological influence, informational actions (attacks)*

Забезпечення ефективного управління військами (силами) в ході проведення антитерористичної операції вимагає своєчасного реагування на прояви інформаційного впливу противника, зокрема, інформаційно-психологічного впливу з боку терористів (сепаратистів). Перелік заходів, які проводяться в антитерористичній операції, викладений у законі України “Про боротьбу з тероризмом” [1] та в Указі виконуючого обов’язки Президента України № 405/2014 від 13 квітня 2014 року Про рішення РНБО України “Про невідкладні заходи щодо подолання терористичної загрози і збереження територіальної цілісності України” [2], а розподіл повноважень за напрямками діяльності сектору безпеки і оборони України – у Стратегічному оборонному бюлетені [3]. Аналіз наведених джерел вказує на наявність певних невідповідностей у визначенні елементів протидії інформаційно-психологічному впливу як на терористів, так і країну, яка їх підтримує (зокрема Російську Федерацію) [1].

Прийняття рішення про локалізацію виявлених інформаційно-психологічного впливу противника принципово відрізняється від обчислення або вибору рішення про рівні загроз інформаційній безпеці у воєнній сфері [2] не тільки відсутністю формальної процедури, але й змістом, яким є прийняття

рішення до якого входить переоцінка корисності результату отриманого системою розвідки на підставі внутрішніх критеріїв більш високого рівня, що залежать від ситуації.

Ціль ухвалення рішення щодо локалізації інформаційно-психологічного впливу противника складається в досягненні Збройними Силами України деякого бажаного результату – запобігання або зниження можливого ураження об'єктів, а також своїх сил і засобів.

Метою статті є викладення методичного підходу визначення рівня інформаційного впливу на особовий склад військ (сил), яка на відміну від існуючих дозволяє прийняти остаточне рішення про наявність або відсутність інформаційно-психологічного впливу на особовий склад Збройних Сил України.

Як, було показано раніше [3], наміри сепаратистів (терористів) застосувати сили і засоби до проведення бойових дій за часом можуть виявитися раніше, ніж почнуться безпосередні дії [4].

Тому, розрахунки значень рівнів інформаційно-психологічного впливу противника із кількістю проведених ним заходів є як би заключним етапом.

Методичний підхід визначення рівня інформаційного впливу на особовий склад військ (сил) під час проведення антитерористичної операції з боку ймовірного противника (сепаратистів, терористів) ґрунтується на виявленні розходжень станів діяльності Збройних Сил України в зоні проведення антитерористичної операції, що перебуває в районах бойового призначення наших засобів розвідки.

Оцінка рівнів інформаційного впливу на особовий склад Збройних Сил України ґрунтується на апріорних знаннях про інформаційно-психологічні дії противника і дані про інформаційні акції, атаки його сил і засобів, що одержані в результаті безпосереднього спостереження за об'єктами розвідки.

Для реалізації зазначеного вище підходу до оцінки рівня інформаційного впливу на особовий склад Збройних сил України скористаємося переліком дій, а також заданою сукупністю розвідувальних ознак, які характеризують ці заходи і можуть бути розкриті засобами розвідки, що входять у систему бойового забезпечення [5].

Крім того, будемо враховувати логічні й кількісні характеристики взаємозв'язків між рівнями інформаційних впливів та заходами щодо їх виявлення.

При рішенні завдання розпізнавання інформаційних заходів або дій у випадку, коли характер ознак імовірнісний, тобто коли між ознаками й заходами, до яких вони можуть бути віднесені, існують імовірнісні зв'язки, побудова алгоритмів, розпізнавання може бути заснована на результатах теорії статистичних рішень. При повній вихідній апріорній інформації ці результати можуть бути використані безпосередньо. При неповній вихідній інформації алгоритми розпізнавання також можуть бути засновані на результатах теорії статистичних рішень, хоча в цьому випадку ці результати можуть бути використані лише шляхом реалізації процедури навчання або самонавчання.

Можливі і інші підходи до рішення завдання розпізнавання. Зокрема після виміру (викриття) кожної чергової ознаки $S_1; S_1S_2; S_1S_2S_3$. Тоді по певному алгоритмі вирішується завдання розпізнавання на основі даних про наявні до сучасного стану ознаки. При цьому залежно від результатів порівняння отриманого рішення з деякими встановленими заздалегідь границями визначається чергова ознака, або припиняється подальше нагромадження інформації про цей захід.

Така процедура рішення завдання розпізнавання зобов'язана своїм виникненням одному з розділів статистики - послідовному аналізу [6].

При виявленні заходів, проведених противником в якості кількісної характеристики ступеня відповідності окремих розвідувальних ознак кожного із заходів з використанням інформаційної міри цих ознак.

Кількісно інформаційна міра (V_{M_j, S_i}) розвідувальної ознаки визначається як кількість інформації, яка є в ознаці $S_i (i=1...N_j)$ щодо заходу $M_j (j=1...M)$.

$$V_{M_j, S_i} = \frac{P(M_j / S_i)}{P(M_j)}, \quad (1)$$

де $P(M_j / S_i)$ – імовірність того, що має місце захід M_j при виявленні ознаки S_i ;

$P(M_j)$ – апіорна ймовірність M_j .

Відома рівність

$$\frac{P(S_i / M_j)}{P(S_i)} = \frac{P(M_j / S_i)}{P(M_j)} \quad (2)$$

У зв'язку з тим, що при проведенні противником заходів може бути розкрита система ознак $R_n \in (S_1, S_2, \dots, S_i, \dots, S_n)$, важливим елементом розпізнавання є обчислення інформаційної міри системи ознак V_{M_j, R_n} з урахуванням їх взаємозв'язків.

Для системи ознак R_n інформаційна міра дорівнює:

$$V_{M_j, R_n} = \frac{P(M_j / R_n)}{P(M_j)} \quad (3)$$

$$V_{M_j, R_n} = V_{M_j, S_1} + V_{M_j, S_1 / S_2} + \dots + V_{M_j, S_n / S_1 \dots S_{n-1}}, \quad (4)$$

де $V_{M_j, S_i / S_1 \dots S_{i-1}} = \frac{P(M_j / S_1, S_2 \dots S_i)}{P(M_j / S_1, S_2 \dots S_{i-1})}$ – кількість інформації, що мається в ознаці

S_i щодо заходу M_j якщо відомо, що ознаки S_1, \dots, S_{i-1} мали місце;

$V_{M_j, S_i / S_1 \dots S_{i-1}}$ показує, яку додаткову інформацію щодо заходу M_j , містить розвідувальні признаки S_i , якщо раніше розвідкою були добуті ознаки S_1, \dots, S_{i-1} .

У тому випадку, якщо додатково внесена ознакою S_i інформація дорівнює його інформаційній мірі, тобто $V_{M_j, S_i / S_1 \dots S_{i-1}} = V_{M_j, S_i}$, то ознаку S_i , варто вважати незалежним від ознак S_1, \dots, S_{i-1} . Для зручності користування вираження (4) приведемо його до наступного виду:

$$V_{M_j, R_n} = \sum_{i=1}^{N_j} V_{M_j, S_i} + \sum_{l=1}^L V_{M_j, S_l} \quad (5)$$

де $i=1 \dots N_j$ – число незалежних ознак, що описують M_j захід;

$l=1 \dots L$ – число груп залежних ознак.

Перехід від інформаційної міри системи розвідувальних ознак до умовної ймовірності розпізнавання заходу здійснюється шляхом перемножування апіорної ймовірності заходу на інформаційну міру виявлених ознак:

$$P(M_j/R_n) = P(M_j) V_{M_j, R_n} \quad (6)$$

На підставі розглянутої методики пропонується алгоритм процесу ухвалення рішення про проведення противником того або іншого заходу.

Процес ухвалення рішення складається із двох етапів:

перший етап – характеризується використанням детермінованого підходу;

другий етап – імовірнісного.

Вихідними даними для імовірнісного підходу є апіорні ймовірності виявлення ознаки S_i при проведенні заходу M_j – $P(S_i/M_j)$.

Детермінований підхід у нашому випадку використовується при складанні для кожного заходу (якщо це можливо) набору розвідувальних ознак $R^j = \{S_i^j\}$, однозначно визначають даний j -захід і порівняння цих наборів з набором ознак $R_n = \{S_i\}$, отриманих на момент ухвалення рішення.

У випадку якщо $R_n \in R^j$ приймається рішення про проведення противником j -го заходу, у протилежному випадку, виробляється аналіз на основі імовірнісної логіки.

По формулі (5) розраховується сумарна інформаційна міра розкритих розвідувальних ознак V_{M_j, R_n} , потім по формулі (6) розраховується $P(M_j/R_n)$ і рівняється з порогом G_j .

$$P(M_j/R_n) \geq G_j \quad (7)$$

де G_j – поріг ухвалення рішення про те, що проводиться j -й захід.

Величини порогів для кожного заходу визначаються виходячи із припустимих значень ймовірностей правильних (P_{jj}) та помилкових (P_{jq}) рішень

$$G_j = \frac{1 - P_{jj}}{\left[\prod_{q=1}^M (1 - P_{jq}) \right]^{\frac{1}{m}}}, \quad j=1 \dots M; q \neq j \dots \quad (8)$$

Таким чином, при надходженні системи (набору) розвідувальних ознак R_n у результаті рішення завдання може бути отриманий остаточний висновок про проведений противником захід або список можливих заходів, що упорядковані по убуту ймовірності $P(M_j/R_n)$.

Значення умовних ймовірностей $P(M_j/R_n)$ використовується надалі для визначення рівнів загроз інформаційній безпеці у військовій сфері.

Крім того, рішення про заходи, що проводяться противником, доводять до командування збройних сил для аналізу й ухвалення рішення на проведення адекватних заходів щодо підвищення бойової готовності сил і засобів.

Стан загроз противника можна розглядати як повну групу неспільних подій (рівнів), для яких справедлива рівність:

$$\sum_{\alpha=1}^3 P_t(\alpha) = 1 \quad (9)$$

де $P_t(\alpha)$ – імовірність α -го стану (рівня) загрози;

$\alpha=1, 2, 3$ – номер рівня загрози ;

t – момент часу визначення загрози.

При цих умовах розрахунок імовірностей рівнів інформаційної безпеки у воєнній сфері доцільно робити з використанням ітераційного методу по формулі (10) [6]:

$$P_t(\alpha) = \frac{P_{t-1}(\alpha) \cdot \left\{ P(M_j/\alpha) \cdot P(M_j/R_n) + \frac{\sum_{\alpha=1}^3 P(M_j/\alpha)}{3} \cdot [1 - P(M_j/R_n)] \right\}}{\sum_{\alpha=1}^3 \left\{ P_{t-1}(\alpha) \cdot \left[P(M_j/\alpha) \cdot P(M_j/R_n) + \frac{\sum_{\alpha=1}^3 P(M_j/\alpha)}{3} \cdot [1 - P(M_j/R_n)] \right] \right\}} \quad (10)$$

$P_{t-1}(\alpha)$ - імовірність α -го рівня, розрахована на попередньому кроці обчислення;

$P(M_j/\alpha)$ - імовірність проведення супротивником M_j , заходу на α -м рівні загрози;

$P(M_j/R_n)$ - отримана умовна ймовірність виявлення M_j заходу якщо засобами розвідки розкритий набір R_n ознак.

Послідовне та багаторазове рішення завдання визначення рівнів загрози повітряного нападу з використанням на кожному кроці усі зростаючого числа виявлених заходів особливо доцільно у випадках, коли ухвалення рішення сполучене з певним ризиком.

Формула (2.10) може бути використана при виконанні наступних умов:

- заходи супротивника формулюються таким чином, що кореляційними зв'язками між ними можна було б знехтувати;

- можливе виникнення ситуації “циклічного нуля” вирішується відомими методами.

Імовірності $P(M_j/\alpha)$ можуть бути отримані на підставі наявних в органах розвідки статистичних даних щодо досвіду навчань і локальних конфліктів, або реальних заходів по переводу засобів повітряного нападу в підвищені ступені бойової готовності, або з використанням імітаційного моделювання. А при їхній відсутності – шляхом проведення експертного опитування колективу компетентних експертів.

Рішення про перехід загрози повітряного нападу на який-небудь рівень може бути прийняте за критерієм заданого перевищення ймовірності цього рівня над імовірностями інших рівнів

$$P_t(\alpha^*) - P_t(\alpha) \geq \Pi_{\alpha^*} \quad (11)$$

де Π_{α^*} – граничне значення ймовірностей.

Висновки. Отже, рівень інформаційного впливу на особовий склад Збройних Сил України під час проведення антитерористичної операції може бути визначений в результаті виявлення проведених противником (сепаратистами, терористами) інформаційних дій з використанням детерміністської або імовірнісної логіки. Запропонована методика визначення рівня інформаційного впливу на особовий склад Збройних Сил України під час проведення антитерористичної операції дозволяє врахувати не тільки апріорні знання про дії противника, які є в органах розвідки, але й розрахувати вірогідність формування заходів на підставі розкритих розвідувальних ознак. У зв'язку з високим ступенем відповідальності за прийняте рішення граничні значення для рівнів інформаційного впливу на особовий склад повинні встановлюватися з використанням великої кількості інформації. Критерії вибору граничних значень рівнів інформаційного впливу на особовий склад можуть змінюватися залежно від умов військово-політичної обстановки. Часовий інтервал аналізу інформаційного впливу розраховується зі здатності противника створювати відповідними елементами інформаційної інфраструктури середовище із ознаками інформаційно-психологічного впливу на особовий склад Збройних Сил України.

Список використаної літератури

1. *Балуев Д.Г.* Информационная революция и современные международные отношения: Учебное пособие. – Нижний Новгород: ННГУ, 2000. – 107 с.
2. *Бусленко Н.П.* Моделирование сложных систем. – М.: Наука, 1978. – 399 с.
3. *Вещицький І.В., Кацалап В.О., Рогов П.Д., Бухало Л.В.* “Модель визначення джерел загроз інформаційній безпеці у воєнній сфері” // Труды академії. – К. 2009. – № 89. – С. 38-45.
4. *Венцель Е.С.* Исследование операций. – М.: Знание, 1976. – 64 с.
5. *Морозов О.* Інформаційна безпека в умовах сучасного стану і перспективи розвитку державності // Віче. – 2007. – № 12. – Спецвипуск. – С. 23 – 25.
6. *Крюков А.І.* Информационная безопасность государства в условиях глобализации. – Режим доступу: <http://www.rada.kiev.ua>.

