УДК 355.40:356.35

к.т.н. **Рогов П.Д.** (НУОУ)
к.психол.н. **Малахов М.А.** (ВІКНУ)
Бухало Л.В. (НУОУ)

МЕТОДИКА ВИЗНАЧЕННЯ РІВНІВ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

Розглянуто можливість оцінки елементів інформаційної безпеки України у воєнній сфері в умовах інформаційної протидії. Аналізуються рівні виникнення ймовірних загроз інформаційній безпеці у воєнній сфері на основі використання інформації про засоби нападу противника.

Загрози, інформаційна безпека, воєнна організація держави.

Рассмотрены возможности по оценке элементов информационной безопасности Украины в военной сфере в условиях информационного противодействия. Анализируется уровни возникновения вероятных угроз информационной безопасности в военной сфере на основании использования информации о средствах нападения противника.

Угрозы, информационная безопасность, военная организация государства.

Opportunities are considered according to elements of information security of Ukraine in the military sphere in the conditions of information counteraction. It is analyzed levels of emergence of probable threats of information security in the military sphere on the basis of use of information on means of attack of the opponent.

Keywords: threats, information security, military organization of the state.

Постановка проблеми у загальному вигляді. Однією з найважливіших задач при розробці й створенні системи забезпечення інформаційній безпеці держави у воєнній сфері є розробка методик, що дозволяють по великій кількості розвідувальної інформації, що одержана від різних сил і засобів розвідки, скласти найбільш точне враження про наміри військово-політичного керівництва противника, стан бойової готовності його збройних сил і діяльності його засобів нападу. Тобто зробити висновок про наявність або відсутність загроз інформаційній безпеці у воєнній сфері [1].

Новизна проблеми. Прийняття рішення про локалізацію виявлених загроз інформаційній безпеці у воєнній сфері 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 загроз інформаційній безпеці у воєнній сфері складається в досягненні Збройними Силами України деякого бажаного результату – запобігання або зниження можливого ураження військових об’єктів, а також своїх сил і засобів.

Постановка завдання. У зв’язку із цим **мета статті** полягає у викладенні методики визначення рівнів загроз інформаційній безпеці у воєнній сфері, яка на відміну від існуючих дозволяє прийняти остаточне рішення про наявність або відсутність загрози.

Як, було показано раніше [3], намір противника застосувати силу і здатності до проведення бойових дій за часом можуть виявитися раніше, ніж почнеться безпосередня підготовка до вторгнення і проведення наступальної операції [4].

Тому, розрахунки значень рівнів загроз інформаційній безпеці у воєнній сфері із кількістю проведених противником заходів є як би заключним етапом.

Методика визначення рівнів загроз інформаційній безпеці у воєнній сфері з боку ймовірного противника ґрунтується на виявленні розходжень станів діяльності Збройних Сил України, (коаліції держав), що перебуває в зоні відповідальності наших засобів розвідки.

Оцінка рівнів загроз інформаційній безпеці у воєнній сфері ґрунтується на апріорних знаннях про заходи противника і дані про дії його засобів нападу, що одержані в результаті безпосереднього спостереження за об'єктами розвідки.

Для реалізації зазначеного вище підходу до оцінки рівня загроз інформаційній безпеці у воєнній сфері скористаємося переліком заходів, 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 загроз інформаційній безпеці та заходами щодо їх виявлення.

Постановка завдання. При рішенні завдання розпізнавання 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].

Виклад основного матеріалу. 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 $\left(V_{M_j,S_i}\right)$ розвідувальної ознаки визначається як кількість інформації, яка є в ознаці $S_i\left(i=1...N_j\right)$ щодо заходу $M_j=\left(j=1...M\right)$.

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

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

$P(M_j)$ – апріорна ймовірність M_j.

Відома рівність

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

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

Для системи ознак $\mathrm{R_n}$ інформаційна міра дорівнює:

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

$$V_{M_j,R_n}=V_{M_j,S_1}+V_{M_j,S_1/S_2}+...+V_{M_j,S_n/S_1...S_{n-1}}, \tag{4}$$

де $V_{M_j,S_i/S_1\ldots S_{i-1}} = \dfrac{P(M_j/S_1,S_2\ldots S_i)}{P(M_j/S_1,S_2\ldots S_{i-1})}$ – кількість інформації, що мається в ознаці S_i щодо заходу M_j якщо відомо, що ознаки $S_1,\ldots S_{i-1}$ мали місце;

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

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

$$V_{M_j,R_n} = \sum_{i=1}^{N_j} V_{M_jS_i} + \sum_{l=1}^{L} V_{M_jS_l}\ , \qquad (5)$$

де i=1…N_j – число незалежних ознак, що описують M_j захід;

l=1...L – число груп залежних ознак.

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

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

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 апріорні імовірності виявлення ознаки S_i при проведенні заходу M_j – $P(S_i/M_j)$.

Детермінований підхід у нашому випадку використається 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 противному випадку, виробляється аналіз на основі імовірнісної логіки.

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

$$P(M_j/R_n) \geq G_j\ , \qquad (7)$$

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

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

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

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 у порядкові по убуванню ймовірності $P(M_j/R_n)$.

Значення умовних ймовірностей $P(M_j/R_n)$ використається надалі для визначення рівнів загроз інформаційній безпеці у воєнній 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:

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

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

α=1, 2, 3 – номер рівня загрози;

t – момент часу визначення загрози.

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

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

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

$P(M_j/\alpha)$ - ймовірність 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 зневажити;

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 ймовірностями інших рівнів

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

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

Отже, загрози інформаційній безпеці у воєнній сфері можуть бути визначені в результаті виявлення проведених противником заходів з використанням детерміністської або імовірнісної логіки. Запропонована методика визначення рівнів загроз інформаційній безпеці у воєнній сфері 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 загроз інформаційній безпеці у воєнній сфері повинні встановлюватися з використанням великої кількості інформації. Критерії вибору граничних значень рівнів загроз інформаційній безпеці у воєнній сфері можуть змінюватися залежно від умов військово-політичної обстановки. Часовий інтервал аналізу загроз інформаційній безпеці у воєнній сфері розраховується зі здатності збройних сил противника підготувати наступальну операцію.

ЛІТЕРАТУРА:

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. Модель визначення джерел загроз інформаційній безпеці у воєнній сфері / Вещицький І.В., Кацалап В.О., Рогов П.Д., Бухало Л.В. // Труди 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: [Електронний ресурс]. – Режим доступу : http//www.rada.kiev.ua.

Без рецензії.