3. Осадча Г. Соціальні мережі – зручний інструмент комунікації для старост та громад. *Радник старости.* 2019. № 3. URL: https://i.factor.ua/ukr/journals/rs/2019/september/issue-3/article-70466.html

4. Ступницька Я. Використання соціальних мереж для інформування населення органами місцевого самоврядування Рівненщини. URL: https://naub.oa.edu.ua/2013/vykorystannya-sotsialnyh-merezh-dlya-informuvannya-naselennya-orhanamy-mistsevoho-samovryaduvannya-rivnenschyny/

5. Турчин А. Класифікація соціальних мереж. *Актуальні задачі та досягнення у галузі кібербезпеки.* Матеріали Всеукраїнської науково-практичної конференції (23–25 листопада 2016 р., м. Кропивницький). URL: https://core.ac.uk/download/pdf/84825408.pdf

6. Що є що у світі соцмереж? URL: https://i.factor.ua/ukr/journals/rs/2019/september/issue-3/article-70466.html

Іванів В. І., слухач,
Національний університет оборони України
імені Івана Черняхівського, м. Київ

ОСОБЛИВОСТІ УДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Інформаційні загрози як різновид воєнних загроз мають багатогранний характер. Їм властиві багатокритерійність, багатофакторність та багатопараметричність. У кінцевому підсумку оцінка ефективності функціонування системи забезпечення інформаційної безпеки, яка протидіє таким загрозам, також повинна бути комплексною.

Враховуючи роль та місце системи забезпечення інформаційної безпеки в загальній системі забезпечення інформаційної безпеки держави в процесі захисту від воєнних загроз національних інтересів в інформаційній сфері, сформулюємо основні вимоги до системи критеріїв, що розробляються нижче. Зокрема, під час формулювання системи критеріїв пропонується дотримуватися базових принципів, визначених у [1, с. 15]:

- відповідність критерію поставленій меті;
- повнота;
- вимірність;
- чіткий фізичний зміст;
- відсутність надлишковості;
- чутливість до зміни вхідних даних.

Комплексне дослідження наявних складників системи протидії інформаційно-психологічному впливу [2, с. 18] показало, що керуючись основними поло-

женнями теорії систем, можна стверджувати, що система забезпечення інформаційної безпеки, ефективність якої підлягає оцінюванню, – це складна багатокомпонентна ієрархічна організаційно-технічна система. Зазвичай, оцінювання ефективності таких систем ґрунтується на системі критеріїв, які згруповані за обраними ознаками. Зокрема, для системи забезпечення інформаційної безпеки такими ознаками можуть бути функціональні, організаційно-технічні й цільові.

Метою тез є удосконалення системи інформаційної безпеки Міністерства оборони України та Збройних Сил України.

Враховуючи результати аналізу системи забезпечення інформаційної безпеки та керуючись зазначеними положеннями теорії систем для оцінювання ефективності системи забезпечення інформаційної безпеки, доцільно сформувати систему критеріїв, що складатиметься з таких груп [3, с. 10]: група критеріїв функціональної ефективності (перша); група критеріїв організаційно-технічної ефективності (друга); група критеріїв цільової ефективності.

Обґрунтуємо фізичний зміст запропонованих критеріїв та введемо показники для кожної з визначених груп.

Продуктивність. K_C – здатність СЗІБ обробляти інформаційні потоки, що мають ознаки ІЗ, приймати щодо них рішення на протидію та забезпечувати їх нейтралізацію. Тоді показник продуктивності визначається згідно з виразом:

$$K_C = \sigma^{-1} \cdot \left(\frac{C_{act} - C_{\min}}{C_{\max} - C_{\min}} + \frac{P_p}{P_p + P_n} + \frac{I_a}{I_a + I_b} \right), \qquad K_C \to \max, \tag{1}$$

де K_C – показник продуктивності СЗІБ, $K_C \in [0,1]$;

σ – нормуючий коефіцієнт, $\sigma = 3$;

$C_{\max}$, $C_{\max}$ – максимально та мінімально необхідні кількості інформаційних потоків з ознаками ІЗ воєнній безпеці в інформаційній сфері, які обробляються СЗІБ (числові значення встановлюються замовником у технічному завданні);

C_{act} – фактична кількість інформаційних потоків з ознаками загроз ІЗ воєнній безпеці в інформаційній сфері, які реально обробляються СЗІБ, $C_{\min} < C_{act} < C_{\max}$;

P_p, P_n – кількість прийнятих та неприйнятих рішень на протидію відповідно;

I_a, I_b – кількість нейтралізованих та не нейтралізованих системою ІЗ.

Керованість. K_H – здатність СЗІБ переходити з одного стану в інший під дією керуючих впливів з одночасним збереженням функціональних показників ефективності у визначених межах. Такими станами системи можуть бути: звичайний з черговими силами і засобами; підвищеної готовності з посиленим складом чергових сил і засобів; повної готовності з повним складом сил і засобів.

У формалізованому вигляді показник керованості СЗІБ визначається як:

H_1	H_2	H_3
0,3	0,7	1

Захищеність. K_S – ступінь захищеності СЗІБ від впливу противника, що поєднує в собі психологічну стійкість до негативного ІПсВ особового складу, задіяного в реагуванні на ІЗ, та захищеність технічних, програмних і спеціальних засобів від кібератак та інших руйнівних дій противника [4, с. 34]. Показник захищеності визначається:

S_1	S_2	S_3	S_4
0,25	0,50	0,75	1

де K_S – показник захищеності СЗІБ від впливу противника, що визначається експертним шляхом відповідно до таких значень.

Ресурсоспоживання. K_R – максимально можливий ефект від функціонування СЗІБ, який досягається за мінімального залучення сил та засобів. Матриця ефективності має такий вигляд, де r_{ij} – значення показника ресурсоспоживання СЗІБ K_R, який описує ефект, що досягається за витрати сил та засобів на забезпечення функціональної ефективності системи.

Отже, зважаючи на фізичний зміст показника відповідності системи забезпечення інформаційної безпеки покладеним на неї функціям та завданням K_Q, а також відповідно до таблиці зв'язності, залежно від одержаних оцінок у підсумку структурна відповідність системи забезпечення інформаційної безпеки.

Список використаних джерел

1. Мигунов А. Л. Тенденции китайской стратегии ведения информационной войны. *Военная мысль.* 2008. № 11. С. 62–67.

2. Цветкова Н. А. Программы Web 2.0 в публичной дипломатии США. *США и Канада: Экономика, политика, культура.* 2011. С. 109–122.

3. Confucius Institutes established worldwide. *Xinhua*. 13.07.2010. URL: www.news.xinhuanet.com/english2010/culture/2010-07/13/c_13398209.htm

4. Anderson E. C., Engstrom J. G. China's Use of Perception Management and Strategic Deception. Prepared for the U.S.–China Economic and Security Review Commission. Science Applications International Corporation.