

УДК 354.42

Володимир БОГДАНОВИЧ,
доктор технічних наук, професор,
головний науковий співробітник Центрального науково-дослідного
інституту Збройних Сил України, м. Київ

Руслан ГРИЩУК,
доктор технічних наук, старший науковий співробітник,
начальник науково-дослідного відділу інформаційної та кібернетичної
безпеки наукового центру Житомирського військового інституту
імені С. П. Корольова, м. Житомир

Олександр ЛЕВЧЕНКО,
кандидат військових наук, професор,
начальник Житомирського військового інституту
імені С. П. Корольова, м. Житомир

СИСТЕМА КРИТЕРІЇВ ТА ПОКАЗНИКІВ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах стрімкого зростання кількості й рівня воєнних загроз безпеці України в усіх сферах і особливо в інформаційній виключно важливу роль відіграє система забезпечення інформаційної безпеки як складова загальнодержавної системи забезпечення воєнної безпеки. Розгортання і нарощування її ефективності є нагальним державним завданням. У статті показано, що впровадження в практичну діяльність системи забезпечення інформаційної безпеки не може бути здійснене без на-

© Богданович В., Грищук Р., Левченко О.

лежного оцінювання очікуваної ефективності від її функціонування. З цією метою розроблено відповідну систему критеріїв та показників оцінювання її ефективності, обґрунтовано фізичний зміст введених критеріїв та наведено їх розмірність. Систему критеріїв запропоновано сформувати у складі трьох груп: група критеріїв функціональної ефективності; група критеріїв організаційно-технічної ефективності; група критеріїв цільової ефективності. Доведено, що розроблена система критеріїв та показників відповідає меті функціонування системи забезпечення інформаційної безпеки, а також характеризується повнотою опису основних факторів, які впливають на ефективність її функціонування.

Ключові слова: система, критерій, показник, ефективність, система забезпечення інформаційної безпеки.

Постановка проблеми в загальному вигляді. Зважаючи на досвід останніх воєнних конфліктів на пострадянському просторі, що свідчить про визначальну роль інформаційної боротьби в досягненні поставлених завдань [1–2], увага воєнно-політичного керівництва України має бути приділена питанням організації ефективного захисту від іноземного інформаційного впливу та активній протидії йому. Насамперед така протидія має бути організована системою забезпечення воєнної безпеки держави (СЗВБД) за рахунок функціонування ефективної системи забезпечення інформаційної безпеки (СЗІБ) у воєнній сфері як складової загальної СЗВБД.

Отже, подальше вдосконалення СЗІБ у воєнній сфері, уточнення її функцій та завдань, розвиток методичного забезпечення є актуальним науковим і практичним завданням, яке потребує вирішення.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опираються автори. Проблеми підвищення ефективності функціонування СЗВБД приділяється значна увага у фаховій науковій літературі як у теоретичному плані [3–8], так і в площині практичної реалізації запропонованих напрямів [9]. Більшість з проаналізованих наукових праць присвячені розробленню теоретико-методологічних основ побудови і функціонування СЗВБД,

питанням підвищення ефективності її функціонування в умовах дії різних небезпек та загроз, а також реформування в напрямі вдосконалення її організаційної структури, законодавчого забезпечення відповідної сфери.

Водночас питання впливу інформаційних загроз (ІЗ) на загальний стан воєнної безпеки держави, організації ефективної протидії їм до цього часу залишаються не розкритими в повному обсязі, а проблеми розвитку та функціонування СЗІБ у рамках загальнодержавної системи забезпечення воєнної безпеки, тим більше питання ефективності функціонування такої системи, взагалі не досліджені, що стримує подальший всебічний розвиток дієвої СЗВБД та її складових.

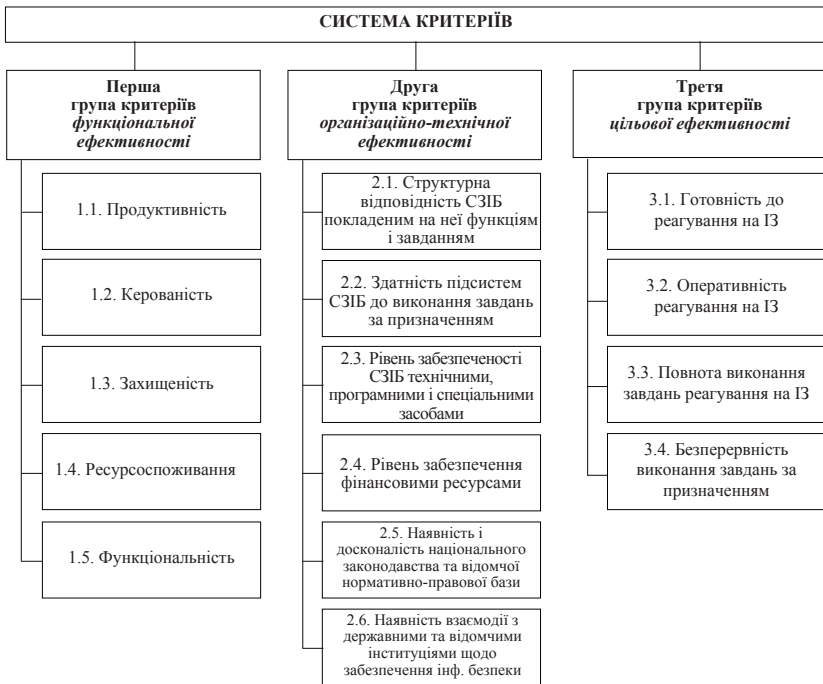
Невирішеною частиною загальної проблеми підвищення ефективності СЗІБ у загальній СЗВБД і надалі залишається завдання з розроблення та вдосконалення науково-методичного забезпечення системи в цілому та її складових. Зокрема, на сьогодні відсутня науково обґрунтована система критеріїв та показників оцінювання ефективності функціонування СЗІБ.

Метою статті є визначення системи критеріїв та показників оцінювання ефективності функціонування СЗІБ у загальній СЗВБД.

Виклад основного матеріалу дослідження. Виходячи з того, що інформаційні загрози спрямовуються на різні за природою, призначенням і характеристиками безпекові сфери, можна зробити висновок про їх багатогранний характер. Їм властиві багатокритерійність, багатофакторність та багатопараметричність. Як наслідок, оцінювання ефективності функціонування СЗІБ, яка протидіє таким загрозам, також повинне бути комплексним, а його критерії мають відповідати таким базовим вимогам [10]: відповідність критерію поставленій меті; повнота; вимірність; чіткий фізичний зміст; відсутність надлишковості; чутливість до зміни вхідних даних, а також до зовнішніх і внутрішніх факторів, які можуть суттєво обмежувати результативність системи. Відповідно до основних положень теорії систем оцінювання ефективності, функціонування подібних до СЗІБ систем, як правило, ґрунтується на системі критеріїв, які групуються за обраними ознака-

ми. Зокрема для СЗІБ такими ознаками можуть бути функціональні, організаційно-технічні й цільові.

Отже, ураховуючи результати аналізу СЗІБ та виходячи із зазначених положень теорії систем для оцінювання ефективності функціонування СЗІБ, доцільно сформулювати систему критеріїв, що складатиметься з таких груп: група критеріїв функціональної ефективності (перша); група критеріїв організаційно-технічної ефективності (друга); група критеріїв цільової ефективності (третя) (див. рисунок).



Система критеріїв оцінювання ефективності функціонування СЗІБ

Розкриємо фізичний зміст кожної із запропонованих груп.

Перша група критеріїв описує функціональну ефективність СЗІБ відповідно до визначених цілей та завдань. Основними критеріями

для даної групи пропонується обрати: продуктивність; захищеність, керованість; ресурсоспоживання та функціональність.

Друга група критеріїв характеризує ефективність СЗІБ, яка обумовлена організаційно-технічними аспектами функціонування системи. До неї пропонується включити такі критерії: структурної відповідності СЗІБ покладеним на неї функціям і завданням; здатності її підсистем до виконання завдань за призначенням; рівня забезпеченості СЗІБ технічними, програмними і спеціальними засобами; рівня забезпечення фінансовими ресурсами; наявності й досконалості національного законодавства та відомчої нормативно-правової бази; наявності взаємодії з державними та відомчими інституціями щодо забезпечення інформаційної безпеки.

Третя група критеріїв описує цільову ефективність функціонування СЗІБ. Основними її критеріями визначимо: готовність до реагування на ІЗ; оперативність реагування на ІЗ; повноту виконання завдань реагування на ІЗ; безперервність виконання завдань за призначенням.

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

1.1. 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

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

де K_C – показник продуктивності СЗІБ, $K_C \in [0,1]$; σ – нормуючий коефіцієнт, $\sigma = 3$; C_{max} , C_{min} – 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.

1.2. 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 посиленням складом чергових сил і засобів; повної готовності з повним складом сил і засобів. У формалізованому вигляді показник керованості СЗІБ визначається як

$$K_H = \begin{cases} H_1 - \text{звичайний стан з черговими силами;} \\ H_2 - \text{стан підвищеної готовності з посиленням складом} \\ \text{чергових сил і засобів;} \\ H_3 - \text{стан повної готовності з повним складом сил і засобів;} \end{cases} \quad K_H \rightarrow \max,$$

де K_H – показник керованості СЗІБ під дією керуючих впливів, що визначається експертним шляхом відповідно до таких значень:

H_1	H_2	H_3
0,3	0,7	1

1.3. Захищеність: K_S – ступінь захищеності СЗІБ від впливу противника, що поєднує в собі психологічну стійкість до негативного інформаційно-психологічного впливу особового складу, задіяного в реагуванні на ІЗ, та захищеність технічних, програмних і спеціальних засобів від кібератак та інших руйнівних дій противника. Показник захищеності визначається як

$$K_S = \begin{cases} S_1 - \text{незахищена;} \\ S_2 - \text{недостатньо захищена;} \\ S_3 - \text{достатньо захищена;} \\ S_4 - \text{незахищена,} \end{cases} \quad K_S \rightarrow \max,$$

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

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

1.4. Ресурсоспоживання: K_R – максимально можливий ефект від функціонування СЗІБ, який досягається за мінімального залучення сил та засобів. Матриця ефективності має такий вигляд:

$$K_R = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{15} \\ r_{21} & r_{22} & \dots & r_{25} \\ \dots & \dots & r_{ij} & \dots \\ r_{51} & r_{52} & \dots & r_{55} \end{pmatrix}, \quad K_R^* = \max_i \min_j r_{ij},$$

де r_{ij} – значення показника ресурсоспоживання СЗІБ K_R , який описує ефект, що досягається при витраті сил та засобів на забезпечення функціональної ефективності системи; K_R^* – оптимальний показник ресурсоспоживання СЗІБ за визначених обмежень; i -й – ефект, що досягається від функціонування СЗІБ, $i = \overline{1,5}$; j -і – витрати сил та засобів (ресурси), що виділяються СЗІБ для досягнення i -го ефекту, $j = \overline{1,5}$.

Для якісного оцінювання показника пропонуємо використовувати наведену нижче таблицю.

Визначення ресурсоспоживання СЗІБ

Рівень ресурсоспоживання, K_R		Досягнутий ефект, i				
		дуже низький	низький	середній	високий	дуже високий
j	Дуже низький	0,04	0,08	0,12	0,16	0,20
	Низький	0,08	0,16	0,24	0,32	0,40
	Середній	0,12	0,24	0,36	0,48	0,75
	Високий	0,16	0,32	0,48	0,64	0,80
	Дуже високий	0,20	0,40	0,75	0,80	1

1.5. Функціональність: K_F – показник, що описує можливість або неможливість виконання підсистемами СЗІБ поставлених завдань і визначених функцій. В аналітичному поданні функціональність СЗІБ описується таким виразом:

$$K_F = \sum_{l=1}^L \gamma_{0l} n_l, \quad K_F \rightarrow \max,$$

де K_F – показник функціональності СЗІБ, $K_F \in [0, 1]$; γ_{0l} – ваговий коефіцієнт пріоритету l -ї підсистеми СЗІБ, $\sum_{l=1}^L \gamma_{0l} = 1$; n_l – l -на підсистема СЗІБ, $l = \overline{1, L}$,

$$n_l = \begin{cases} 0, & \text{якщо } l\text{-на підсистема СЗІБ не виконує поставлені} \\ & \text{завдання й визначені функції;} \\ 1, & \text{якщо } l\text{-на підсистема СЗІБ виконує поставлені} \\ & \text{завдання й визначені функції.} \end{cases}$$

На основі одержаних кількісних оцінок показника функціональності СЗІБ K_F визначається її якісна (лінгвістична) оцінка. Для цього пропонуємо використовувати вербально-числову шкалу Харрінгтона [11]:

Функціональність СЗІБ	K_F
Функціонує в установленому режимі	0,8–1
Функціонування ускладнене	0,64–0,79
Функціонування порушене	0,37–0,63
Функціонування під загрозою зриву	0,2–0,36
Не функціонує	0–0,20

2.1. Структурна відповідність СЗІБ покладеним на неї функціям та завданням. K_Q – ступінь відповідності покладених функцій та завдань на СЗІБ щодо: моніторингу і виявлення ІЗ; аналізу та оцінювання ІЗ; вироблення і прийняття рішення щодо організації протидії ІЗ; виконання заходів протидії ІЗ та контролю їх виконання. Відповідний показник визначається як

$$K_Q = \frac{1}{L} \sum_{l=1}^L q_l, \quad K_Q \rightarrow \max,$$

де K_Q – показник структурної відповідності СЗІБ покладеним на неї функціям та завданням, $K_Q \in [0, 1]$; L – кількість підсистем у складі СЗІБ, на які покладено

визначені функції та завдання, $L = 5$; q_l – l -на підсистема СЗІБ, на яку покладено визначені функції та завдання,

$$q_l = \begin{cases} 0, & \text{якщо підсистема відсутня;} \\ 1, & \text{якщо підсистема присутня,} \end{cases} \quad l = \overline{1, L}.$$

Зв'язок між l -ю підсистемою СЗІБ та її функціями і завданнями такий:

q_l	Функції та завдання підсистем
$l = 1$	Моніторинг та виявлення ІЗ
$l = 2$	Аналіз та оцінювання ІЗ
$l = 3$	Прийняття рішення щодо протидії ІЗ
$l = 4$	Здійснення протидії ІЗ
$l = 5$	Контроль виконання заходів протидії ІЗ

Отже, виходячи з фізичного змісту показника відповідності СЗІБ покладеним на неї функціям та завданням K_Q , а також відповідно до таблиці зв'язності залежно від одержаних оцінок у підсумку структурна відповідність СЗІБ оцінюється як

$$K_Q = \begin{cases} 1 - \text{відповідає;} \\ 0,75 - \text{обмежено відповідає;} \\ 0,50 - \text{задовільно відповідає;} \\ 0,25 - \text{незадовільно відповідає;} \\ 0 - \text{не відповідає.} \end{cases}$$

2.2. Здатність підсистем СЗІБ до виконання завдань за призначенням: K_p – показник, що описує ймовірність виконання всіма підсистемами СЗІБ завдань за призначенням. У загальному вигляді він може бути визначений як

$$K_p = \frac{1}{L} \sum_{l=1}^L P_l, \quad K_p \rightarrow \max,$$

де K_p – показник здатності підсистем СЗІБ до виконання завдань за призначенням, $K_p \in [0, 1]$.

При цьому для числового розрахунку згаданого показника експерти керуються такими даними:

Критерій вибору P_l -ї ймовірності виконання l -ю підсистемою завдань за призначенням	Імовірність виконання підсистемою СЗІБ завдань за призначенням P_l
Підсистема здатна до виконання завдань за призначенням	1
Підсистема частково здатна до виконання завдань за призначенням	0,5
Підсистема не здатна до виконання завдань за призначенням	0

Висновок про ефективність функціонування СЗІБ за даним критерієм робиться залежно від одержаної числової оцінки відповідного показника K_p :

$$K_p = \begin{cases} 0,67 - 1 - \text{підсистеми СЗІБ здатні до виконання завдань за призначенням;} \\ 0,34 - 0,66 - \text{підсистеми СЗІБ частково здатні до виконання завдань за призначенням;} \\ 0 - 0,33 - \text{підсистеми СЗІБ не здатні до виконання завдань за призначенням.} \end{cases}$$

2.3. Рівень забезпеченості технічними, програмними та спеціальними засобами: K_z – це показник забезпеченості СЗІБ технічними, програмними та спеціальними засобами, якими є: комп’ютерна техніка; сервери; супутникові, телевізійні й радіоприймачі (технічні засоби); спеціальне програмне забезпечення (програмні засоби); теле- і радіопередавачі; звукомовні станції, засоби виготовлення і розповсюдження друкованої продукції; автоматизовані робочі місця тощо (спеціальні засоби). Він визначається як

$$K_z = \frac{\sum_{g=1}^{Z_{PL}^{TZ}} z_{ACTg}^{TZ} + \sum_{h=1}^{Z_{PL}^{PZ}} z_{ACTh}^{PZ} + \sum_{y=1}^{Z_{PL}^{SZ}} z_{ACTy}^{SZ}}{Z_{PL}^{TZ} + Z_{PL}^{PZ} + Z_{PL}^{SZ}}, \quad K_z \rightarrow \max,$$

де K_z – показник рівня забезпеченості СЗІБ технічними, програмними і спеціальними засобами, $K_z \in [0,1]$; z_{ACTg}^{TZ} , z_{ACTh}^{PZ} , z_{ACTy}^{SZ} – показники реальної забезпе-

ченості СЗІБ технічними, програмними і спеціальними засобами відповідно, $g = \overline{1, G}$, $h = \overline{1, H}$, $y = \overline{1, Y}$, шт.; Z_{PL}^{TZ} , Z_{PL}^{PZ} , Z_{PL}^{SZ} – показники необхідної (визначеної або планованої) забезпеченості СЗІБ технічними, програмними і спеціальними засобами згідно з наявними потребами, шт.

Варто зауважити, що важливість забезпеченості СЗІБ технічними, програмними і спеціальними засобами однакова, тому при обчисленні даного показника коефіцієнт пріоритету для кожного з них окремо не враховується.

2.4. Рівень забезпечення фінансовими ресурсами: K_W – це показник, числове значення якого характеризує рівень фінансової забезпеченості діяльності як власне самої СЗІБ, так і заходів з протидії ІЗ, які вона проводить, тобто

$$K_W = \frac{W_{REAL}}{W_{PLAN}}, \quad K_W \rightarrow \max,$$

де K_W – показник рівня забезпечення фінансовими ресурсами СЗІБ та заходів протидії ІЗ, $K_W \in (0, 1]$; W_{REAL} , W_{PLAN} – реальні та заплановані бюджетні витрати матеріально-речових та інших ресурсів у грошовому еквіваленті, виділених для забезпечення функціонування СЗІБ, а також заходів протидії, грн.

2.5. Наявність і досконалість національного законодавства та відомчої нормативно-правової бази: K_A – це стан розвитку і повноти національної та відомчої нормативно-правової бази в галузі інформаційної безпеки держави, що визначається згідно з таким виразом:

$$K_A = \begin{cases} A_1 - \text{нормативно-правова база є і охоплює всі} \\ \text{аспекти інформаційної безпеки держави;} \\ A_2 - \text{нормативно-правова база є і охоплює не всі} \\ \text{аспекти інформаційної безпеки держави;} \\ A_3 - \text{є окремі нормативно-правові акти, які охоплюють} \\ \text{окремі аспекти інформаційної безпеки держави;} \\ A_4 - \text{нормативно-правова база не сформована.} \end{cases} \quad K_A \rightarrow \max.$$

Залежно від стану нормативно-правової бази зазначений показник набуває наведених нижче конкретних числових значень:

Наявність і досконалість національного законодавства та відомчої нормативно-правової бази	Значення показника K_A
A_1	1
A_2	0,6
A_3	0,2
A_4	0

2.6. Наявність взаємодії з державними та відомчими інституціями щодо забезпечення інформаційної безпеки: K_B – це ступінь налагодження взаємодії СЗІБ в інтересах спільного виконання заходів з виявлення та протидії ІЗ воєнній та національній безпеці з державними структурами (Міністерством інформаційної політики України, Міністерством закордонних справ України, Національною радою України з питань телебачення і радіомовлення) та іншими структурами сектора безпеки й оборони держави (Службою безпеки України, Міністерством внутрішніх справ України, Службою зовнішньої розвідки України тощо). Відповідний показник визначається як

$$K_B = \begin{cases} B_1 - \text{взає модія налагоджена;} \\ B_2 - \text{взає модія налагоджена ч астково;} K_B \rightarrow \text{max,} \\ B_3 - \text{взає модія не налагоджена,} \end{cases}$$

де числові значення показника K_B залежно від коефіцієнтів взаємодії B_1 , B_2 та B_3 обираються таким чином:

Коефіцієнт взаємодії	Значення показника K_B
B_1	1
B_2	0,5
B_3	0

3.1. Готовність до реагування на ІЗ. K_{FG} – здатність системи одразу після виявлення ІЗ розробляти та впроваджувати ефективні заходи

протидії, що приведуть до нейтралізації загрози. Даний показник визначається за таким виразом:

$$K_M = \begin{cases} M_1 - \text{система не готова реагувати на ІЗ}; \\ M_2 - \text{система обмежено готова реагувати на ІЗ}; K_M \rightarrow \text{max}, \\ M_3 - \text{система готова реагувати на ІЗ}, \end{cases}$$

де K_M – показник готовності СЗІБ до реагування на ІЗ. Значення показників у наведеній системі визначаються в такий спосіб:

M_1	M_2	M_3
0,3	0,7	1

3.2. Оперативність реагування на ІЗ: K_O – це показник, що описує здатність СЗІБ оперативно реагувати на ІЗ у визначені часові нормативи. У формалізованому вигляді даний показник визначається відповідно до такого виразу:

$$K_O = 1 - \frac{T_F}{T_{ZAD} + T_F}, \quad K_O \rightarrow \text{max},$$

де K_O – показник оперативності реагування на ІЗ, $K_O \in (0,1)$; T_F , T_{ZAD} – фактичний та нормативно визначений час реагування СЗІБ на ІЗ відповідно, год.

3.3. Повнота виконання завдань реагування на ІЗ: K_{VV} – це здатність СЗІБ у повному обсязі виконувати всі завдання з реагування на конкретну виявлену ІЗ. Це завдання щодо моніторингу, виявлення, аналізу, оцінювання ІЗ, розроблення пропозицій та прийняття рішення щодо протидії їй, доведення завдань до виконавців, здійснення заходів протидії ІЗ, контроль їх результативності й коригування дій. Математичний вираз, що описує даний показник, має такий вигляд:

$$K_{VV} = \frac{\sum_{x=1}^V v_x}{V}, \quad K_{VV} \rightarrow \text{max},$$

де K_{VV} – показник повноти виконання завдань реагування на ІЗ, $K_{VV} \in [0,1]$; v_x – x -ве повністю виконане конкретне завдання, $x = \overline{1, V}$; V – загальна кількість завдань з реагування на виявлену ІЗ.

3.4. Безперервність виконання завдань за призначенням: K_{NP} – це здатність СЗІБ не допускати перерви в процесі виконання завдань за призначенням. Зокрема процес моніторингу, виявлення, аналізу, оцінювання ІЗ, розроблення пропозицій та прийняття рішення щодо протидії виявленій загрози, доведення завдань до виконавців та здійснення заходів протидії ІЗ має бути без перерв і затримок. Відповідний показник визначається як

$$K_{NP} = \frac{t_{NP}}{t_{ZAG}}, \quad K_{NP} \rightarrow \max,$$

де K_{NP} – показник неперервності виконання СЗІБ завдань за призначенням, $Z \in (0,1]$; t_{NP} – час неперервного виконання завдань за призначенням, год; t_{ZAG} – загальний час виконання СЗІБ завдань за призначенням, год.

Висновки та перспективи подальших досліджень. Розроблена система критеріїв оцінювання ефективності функціонування СЗІБ у загальній СЗВБД, на відміну від відомих, ґрунтується на групах критеріїв функціональної, організаційно-технічної та цільової ефективності. Перевагою запропонованої системи критеріїв є те, що вона враховує специфіку та особливості функціонування саме системи інформаційної безпеки. Введені критерії характеризуються розробленою та адаптованою до визначених умов відповідною системою показників, що мають чіткий фізичний зміст та прикладну практичну спрямованість.

У подальшому на основі наведеної системи критеріїв планується розробити метод та методику оцінювання ефективності функціонування СЗІБ.

Список використаної літератури

1. Горбулін В. П. “Гібридна війна” як ключовий інструмент російської геостратегії реваншу / В. П. Горбулін // Стратегічні пріоритети. – 2014. – № 4 (33). – С. 5–12.
2. Левченко О. В. Еволюція гібридної війни Російської Федерації проти України / О. В. Левченко // Наука і оборона. – 2017. – № 2. – С. 16–19.

3. Сніцаренко П. М. Методичний підхід до визначення критеріїв оцінки рівня інформаційного впливу на елементи інформаційної інфраструктури воєнної організації держави / Ю. О. Саричев, П. М. Сніцаренко, В. О. Кацалап // Зб. наук. праць № 31. – К. : НДІ ГУР МО України, 2011. – С. 126 – 139.

4. Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія / В. Б. Толубко. – К. : НАОУ, 2003. – 320 с.

5. Косевцов В. О. До питання оцінювання ефективності функціонування системи забезпечення воєнної безпеки держави / В. О. Косевцов, В. М. Телелим, А. А. Лобанов // Наука і оборона. – 2010. – № 3. – С. 8–12.

6. Богданович В. Ю. Теоретико-методологічні засади забезпечення національної безпеки держави у її визначальних сферах : монографія / В. Ю. Богданович, А. І. Семенченко, Ю. В. Єгоров та ін. – К. : Кий, 2007. – 370 с.

7. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення : монографія / Г. В. Певцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський. – Х. : Цифрова друкарня № 1, 2013. – 272 с.

8. Телелим В. М. Напрями удосконалення процесу функціонування системи забезпечення воєнної безпеки / В. М. Телелим, В. О. Косевцов, А. А. Лобанов // Труді університету. – К. : НУОУ. – 2011. – № 1 (100). – С. 21–26.

9. Косошов О. В. Методичний підхід до розрахунку показників ефективності функціонування системи інформаційної безпеки / О. М. Косошов, А. О. Сірик, Д. В. Косаренко // Зб. наук. праць № 42. – К. : НДІ ГУР МО України, 2015. – С. 51–60.

10. Фишберн П. Теория полезности для принятия решений / П. Фишберн. – М. : Наука, 1978. – 352 с.

11. Методы экспертной оценки [Электронный ресурс] // Студопедия. – Режим доступа : https://studopedia.su/10_147713_metodi-ekspertnoy-otsenki.html/

Богданович В. Ю., Гришук Р. В., Левченко А. В. **Система критериев и показателей оценивания эффективности функционирования системы обеспечения информационной безопасности**

В условиях стремительного роста количества и уровня военных угроз безопасности Украины во всех сферах и особенно в информационной исключительно важную роль приобретает система обеспечения информационной безопасности как составляющая общегосударственной системы обеспечения военной безопасности. Развертывание и наращивание ее эффективности является важным государ-

ственным заданием. В статье показано, что внедрение в практическую деятельность системы обеспечения информационной безопасности не может быть осуществлено без надлежащего оценивания ожидаемой эффективности ее функционирования. С этой целью разработана соответствующая система критериев и показателей оценивания ее эффективности, обосновано физическое содержание введенных критериев и приведена их размерность. Систему критериев предложено сформировать в составе трех групп: группа критериев функциональной эффективности; группа критериев организационно-технической эффективности; группа критериев целевой эффективности. Доказано, что разработанная система критериев и показателей соответствует цели функционирования системы обеспечения информационной безопасности, а также характеризуется полнотой описания основных факторов, которые влияют на эффективность ее функционирования.

Ключевые слова: *система, критерий, показатель, эффективность, система обеспечения информационной безопасности.*

Bohdanovych V., Hryshchuk R., Levchenko O. **The system of criteria and indices for assessing the functioning efficiency of the system of ensuring the information security**

The system of ensuring the state military security plays a systemically important part in the process of providing for its military security. Under the conditions of the rapid increase in the level of military threats Ukraine faces in all spheres, especially in the information sphere, the system of ensuring the state military security has to perform additional functions and tasks, including those that were not typical for it before. In particular, the function related to protecting national interests in the information sphere was not characteristic of it up till now. The paper suggests imposing the task of implementing the above function on the system of ensuring the information security within the framework of the entire system of ensuring the state military security. The paper shows that introducing the system of ensuring the information security into practical activities cannot be accomplished without the appropriate assessment of the prognosticated efficiency of its functioning. With this in view the authors succeeded in:

systematizing current standards of national legislation in the part which concerns the protection of national interests against military threats in the information sphere; working out the corresponding system of criteria and indices of assessing the efficiency of the system of ensuring the information security; substantiating the physical content of the criteria introduced and suggesting their dimensions.

It has been suggested to form three groups of criteria: a group of criteria of functional effectiveness (productivity, vulnerability, controllability, resource consumption and functionality); a group of criteria of organizational and technical effectiveness (the structural conformity; the ability to perform designated tasks; the level of provision with technical, software and special means; the level of financial support; the availability and efficiency of national legislation; coordination with government agencies); a group of criteria of task effectiveness (readiness to respond to threats; operational responsiveness to threats; completeness of task performance in responding to threats; the continuousness of performing designated tasks).

The paper also shows that the developed system of criteria and indices fully corresponds to the purpose of the system of ensuring the information security and is characterized by the absolute description of basic factors affecting the efficiency of the system functioning.

Keywords: *system, criteria, indices, efficiency, system of ensuring information security.*