УДК 004.681

Левченко Є.Г., Рабчун А.О.

ЕКСПЕРТНІ ОЦІНКИ В ЕКОНОМІЧНИХ ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним з важливих економічних завдань менеджменту інформаційної безпеки являється оптимізація розподілу ресурсів між об'єктами захисту інформації [1]. Рішення цієї задачі викликає ряд проблем, які мають як функціональний, так і обчислювальний характер. До ключових проблем слід віднести пошук цільової функції $f(x,y)$, яка визначає кількість вилученої інформації через ресурси x і y, спрямовані на кожний об'єкт нападом і, відповідно, захистом. Обчислювальні труднощі пов'язані зі значною кількістю змінних величин, частина яких (керовані змінні) задається захистом і може бути визначена з певною похибкою, а інша частина (некеровані змінні) задається нападом – її можна лише оцінити з деякою імовірністю.

Структуру цільової функції в загальних рисах можна подати у такому вигляді:

$$f(x,y) = g \cdot p \cdot q(x) \cdot F(x,y), \qquad (1)$$

де g – кількість інформації на об'єкті;

p – імовірність нападу на об'єкт;

$q(x)$ – імовірність виділення нападом ресурсів x для вилучення інформації з об'єкту;

$F(x,y)$ – залежність вилученої інформації від ресурсів x і y (її можна розглянути як умовну імовірність події).

Величина g, яка входить як параметр в розрахунок, відноситься до керованих змінних, але її визначення викликає певні труднощі через недостатню розробку методики розрахунку кількості інформації. Величини p_k і $q(x)$ – не керовані змінні і їх визначення ще більш проблематичне.

За браком статистичної інформації для визначення змінних, які вводяться в розрахунок, і вибору залежності $F(x,y)$, яка в найбільшій мірі відповідає реальним ситуаціям, доводиться звертатись до методу експертних оцінок [2].

Проілюструємо його на прикладі системи захисту інформації, яка складається з l об'єктів і оцінюється групою з m експертів.

На першому етапі оцінимо значення параметрів $g_k, k = \overline{1,l}$ - номер об'єкта. В табл.1 приведені значення величин, одержаних в результаті експертних оцінок:

G_{nk} – нормовані до 1 вагові коефіцієнти k–го об'єкта, визначені n–им експертом;

$\bar{G}_k$ – усереднене по всім експертам значення коефіцієнта G_{nk}, $\bar{G}_k = \frac{\sum_{n=1}^{m} G_{nk}}{m}$, m=5;

$\Delta G_{nk} = G_{nk} - \bar{G}_k$ – відхилення G_{nk} від середнього значення;

$\sum_{k=1}^{l} |\Delta G_{nk}|$ – сума абсолютних значень відхилень показників кожного експерта від середніх значень;

c_n – ваговий коефіцієнт кожного експерта, який визначається, як $c_n = \frac{1}{\sum_{k=1}^{l} |\Delta G_{nk}|}$;

$\sigma_k^2 = \sum_{n=1}^{m} \frac{\Delta G_{nk}^2}{l-1}$ – дисперсія оцінок параметра G_{nk}, даного експертами для k-го об'єкта;

$V_k = \frac{\sigma_k}{\bar{G}_k}$ – варіація оцінок G_{nk} для k–го об'єкта.

Таблиця 1

Результати експертних оцінок

Номер об'єкта, k / показник / Номер експерта n	1		2		3		$\sum_{k=1}^{3} \lvert\Delta G_{nk}\rvert$	c_n
	G_{n1}	ΔG_{n1}	G_{n2}	ΔG_{n2}	G_{n3}	ΔG_{n3}		
1	0,47	-0,07	0,33	0,05	0,20	0,02	0,14	0,18
2	0,50	-0,04	0,25	-0,03	0,25	0,07	0,14	0,18
3	0,50	-0,04	0,28	0,00	0,22	0,04	0,08	0,32
4	0,71	0,17	0,21	-0,07	0,07	-0,11	0,35	0,07
5	0,50	-0,04	0,33	0,05	0,17	-0,01	0,10	0,25
$\bar{G}_k$	0,54		0,28		0,18			
σ_k	0,138		0,073		0,067			
V_k	0,256		0,261		0,368			

В табл.2 приведені значення $c_n G_{nk}$– параметра важливості k–го об'єкта, дані n–им експертом, з врахуванням його кваліфікації (вона оцінюється коефіцієнтом c_n), а також остаточні значення параметра g_k, який характеризує об'єм інформації на k–му об'єкті (тобто його важливість) і визначається як адитивна функція показників G_{nk} з ваговими коефіцієнтами c_n:

$$g_k = \sum_{n=1}^{m} c_n G_{nk}$$

Таблиця 2

Розрахунок показників g_k

$c_n G_k$ / n	$c_n G_1$	$c_n G_2$	$c_n G_3$
1	0,085	0,059	0,036
2	0,090	0,045	0,045
3	0,160	0,093	0,070
4	0,050	0,015	0,005
5	0,125	0,083	0,042
g_k	0,50	0,30	0,20

Аналізуючи дані, приведені в табл.1,2, зазначимо, що розкиданість значень в рядках можна розглядати як показник кваліфікації експертів, а в стовпчиках – як ступінь їх обізнаності про кожний з об'єктів.

Імовірності p і q також можуть бути визначені шляхом експертних оцінок за приведеною вище методикою. Після визначення параметрів розрахунку звертаємось до вибору залежності $F(x, y)$. При цьому врахуємо такі міркування:

1) залежність $F(x, y)$ повинна бути монотонною на відміну від широко вживаної функції Гросса, яка має кусочно-лінійний характер [3];

2) при $x \to 0$ $F(x, y) \to 0$, при $x \to \infty$ $F(x, y) \to 1$;

3) з попередньої умови випливає, що опуклість при $x \gg 1$направлена вгору;

4) опуклість при $x < 1$ (її визначає нахил залежності $F(x)$ при $x = 0$) може бути направлена як вгору, так і вниз;

5) при $x = 1$ $F(x, y) \approx 0{,}5$ (ця оцінка досить приблизна і «прив'язка» залежності $F(x, y)$ до реальної ситуації може бути здійснена в іншій точці);

Ці міркування привели до залежностей, обраних п'ятьма експертами і зображених кривими 1-5 на Рис. 1. Вагові коефіцієнти, присвоєні окремими залежностями, покладемо рівними, визначеними вище, коефіцієнтами C_n, які характеризують кваліфікацію кожного з експертів.

Таблиця 3

Вагові коефіцієнти для залежностей $F(x, y)$.

Номер кривої, n	1	2	3	4	5
Ваговий коефіцієнт, k_n	0,32	0,25	0,07	0,18	0,18

Результуючу залежність $F(x, y)$ побудуємо як адитивну функцію:

$$F = c_1F_1 + c_2F_2 + c_3F_3 + c_4F_4 + c_5F_5 \qquad (2)$$

Ця залежність зображена на Рис. 1 неперервною лінією (крива 6)

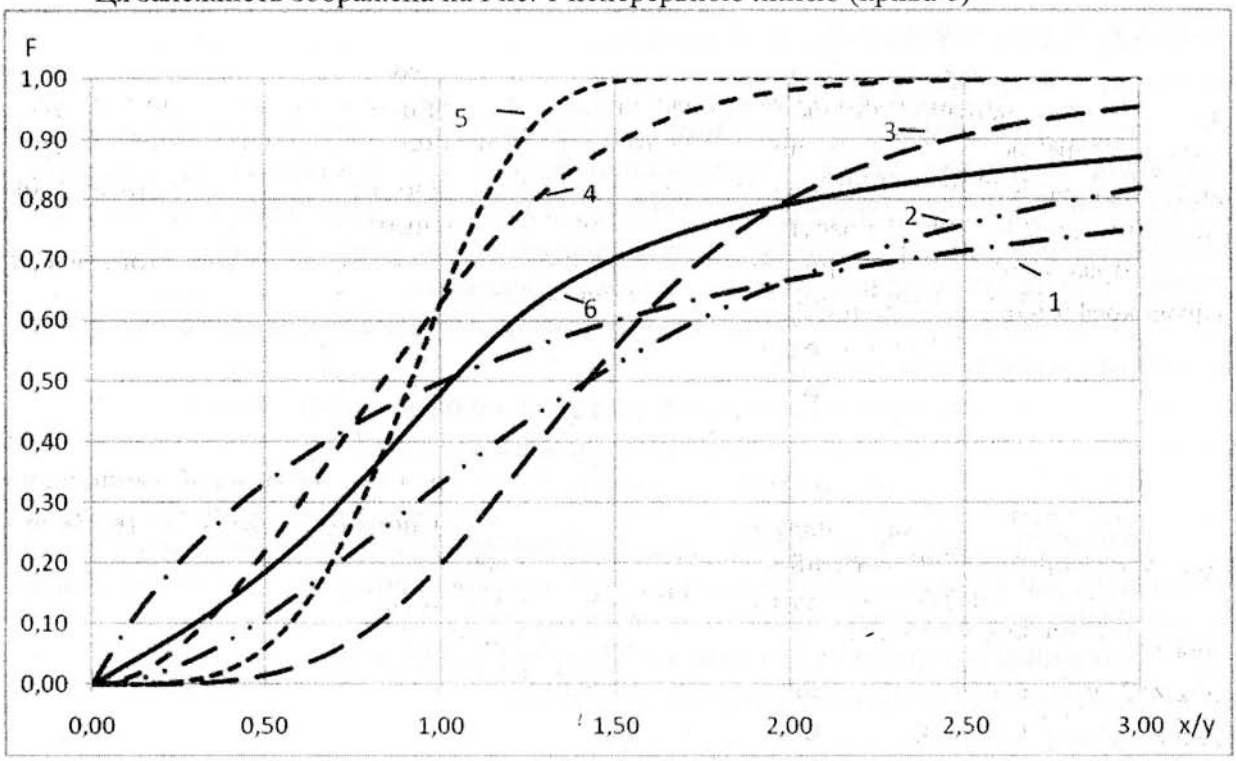

Рис. 1. Залежність об'єму втрат інформації від співвідношення ресурсів

1. $F(x,y) = \frac{(x/y)}{(x/y)+1}$; 2. $F(x,y) = \frac{(x/y)^2}{(x/y)^2+2}$; 3. $F(x,y) = \frac{(x/y)^4}{(x/y)^4+4}$;

4. $F(x,y) = 1 - e^{-(x/y)^2}$; 5. $F(x,y) = 1 - e^{-(x/y)^4}$;

Приведемо приклад застосування одержаних результатів для розрахунку втрат інформації в системі з $l = 3$ об'єктів. Наша мета: знайти оптимальний розподіл ресурсів захисту.

Параметри розрахунку, визначені в результаті експертних оцінок:

$g_1 = 0{,}5;\ g_2 = 0{,}3;\ g_3 = 0{,}2;$

$q_1 = 0{,}8;\ q_2 = 0{,}15;\ q_3 = 0{,}05;\ p = 1;$

Вважатимемо, що сторона нападу зосереджує всі ресурси на одному з об'єктів і розрахуємо втрати інформації на ньому за виразом (1), використовуючи в якості $F(x, y)$ функцію (2) (крива 6), тобто усереднену залежність $F(x, y)$.

Таблиця 4

Втрати інформації на об'єкті при різних розподілах ресурсів захисту, з врахуванням експертних оцінок

	z=1			z=2			z=3		
	$g_1 = 0{,}5$	$g_2 = 0{,}3$	$g_3 = 0{,}2$	$g_1 = 0{,}5$	$g_2 = 0{,}3$	$g_3 = 0{,}2$	$g_1 = 0{,}5$	$g_2 = 0{,}3$	$g_3 = 0{,}2$
y_k	**0,870**	**0,130**	**0,000**	**1,000**	**0,000**	**0,000**	**1,000**	**0,000**	**0,000**
f	**0,286**	**0,286**	**0,200**	**0,396**	**0,300**	**0,200**	**0,436**	**0,300**	**0,200**

Оптимальні розподіли y_k:

для z=1: $y_1 = 0{,}87,\ y_2 = 0{,}13,\ y_3 = 0;$

для z=2: $y_1 = 1,\ y_2 = 0,\ y_3 = 0;$

для z=3: $y_1 = 1,\ y_2 = 0,\ y_3 = 0;$

Результат, отриманий при z=1, можна порівняти з результатами наведеними в [1]. Без врахування експертних оцінок, і використанні функції Гросса в якості цільової функції, оптимальний розподіл становив $y_1 = 0{,}62,\ y_2 = 0{,}35,\ y_3 = 0{,}03$. Цей розподіл суттєво відрізняється від нашого і можна зробити висновок, що отримані результати є більш точними, а, отже, розподіл ресурсів захисту більш ефективним.

Врахуємо тепер імовірності q_x виділення ресурсів x нападом, використовуючи їх, як вагові коефіцієнти в розподілі $\{y_k^o\}$:

$$y_1^o = 0{,}87 * 0{,}8 + 1 * 0{,}15 + 1 * 0{,}05 = 0{,}896$$

$$y_2^o = 0{,}13 * 0{,}8 + 0 * 0{,}15 + 0 * 0{,}05 = 0{,}104$$

$$y_3^o = 0;$$

Розглянемо аналогічну задачу, що відрізняється від попередньої розподілом x_k. Припустимо, що сторона нападу розподіляє свої ресурси порівну на всі об'єкти. Знайдемо для цього випадку оптимальний розподіл ресурсів захисту.

Оптимальні розподіли y_k і значення $f^o(x, y) = \sum_{k=1}^{3} f_k^o(x, y)$:

для z=1: $y_1 = 0{,}55,\ y_2 = 0{,}45,\ y_3 = 0;\ f^o(x, y) = 0{,}412$

для z=2: $y_1 = 1,\ y_2 = 0,\ y_3 = 0;\ f^o(x, y) = 0{,}635$

для z=3: $y_1 = 1,\ y_2 = 0,\ y_3 = 0;\ f^o(x, y) = 0{,}742$

Врахуємо імовірності p_x виділення ресурсів x нападом, та знайдемо оптимальний розподіл y_k^o:

$$y_1^o = 0{,}55 * 0{,}8 + 1 * 0{,}15 + 1 * 0{,}05 = 0{,}64$$

$$y_2^o = 0{,}45 * 0{,}8 + 0 * 0{,}15 + 0 * 0{,}05 = 0{,}36$$

$y_3^o = 0;$

Отже, при використанні цільової функції (2) і співвідношенні $g_1 : g_2 : g_3 = 0{,}5 : 0{,}3 : 0{,}2$; у випадку, коли напад здійснюється на один з об'єктів і імовірності цих подій як і імовірності виділення нападом ресурсів $z = 1, z = 2, z = 3$ однакові, оптимальний розподіл ресурсів захисту становить $y_1^o : y_2^o : y_3^o = 0{,}87 : 0{,}13 : 0$; у випадку коли напад розподіляє свої ресурси порівну і імовірності виділення нападом ресурсів $z = 1, z = 2, z = 3$ однакові $y_1^o : y_2^o : y_3^o = 0{,}55 : 0{,}45 : 0$; якщо ж останні імовірності співвідносяться як 0,8: 0,15: 0,05 (оцінки експертів), то $y_1^o : y_2^o : y_3^o =$ $= 0{,}64 : 0{,}36 : 0$. Цей результат, очевидно, можна вважати остаточним.

Список літератури

1. Левченко Є.Г. Оптимізація розподілу ресурсів між об'єктами захисту інформації. – К.: НТЖ «Захист інформації», №1, 2007.

2. Гуткин Л.С. Оптимизация радиоэлектронных устройств. М.: Радио, 1975.

3. Левченко Є.Г., Рабчун А.О. Модель Гросса в протистоянні двох сторін у сфері захисту інформації. – НТЖ «Захист інформації», №3, 2009.

Надійшла 12.02.09

УДК 342.738

Хорошко В.О., Артемов В.Ю.

ОКРЕМІ АСПЕКТИ ВПРОВАДЖЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СПЕЦІАЛЬНИХ СЛУЖБАХ УКРАЇНИ

Перехід до системи демократичних цінностей і відкритого суспільства, європейська та євроатлантична спрямованість України примушують державу та суспільство звертатися до системи міжнародних стандартів у такій делікатній галузі як безпека.

При цьому безпека розуміється в широкому сенсі – це і безпека держави, це і безпека особистості, це і безпека суспільної організації держави, це і безпека міждержавних об'єднань, таких як ЄС та НАТО.

До проблеми міжнародного співробітництва в галузі стандартизації зверталися такі відомі зарубіжні та вітчизняні науковці як Асландер Робертс, Олександр Бакалінський, Володимир Галатенко, Володимир Бетелін, Сергій Климчук, Павло Куберт, Віталій Безштанько, Василь Цукран та ін.

Метою даної статті є аналіз міжнародного стандарту з інформаційної безпеки ISO 27001 та його впровадження в спеціальних службах нашої держави.

Чому саме цей стандарт з інформаційної безпеки потрібен спецслужбам? Тому, що інформація стає не лише сферою професійної діяльності мільйонів людей ще тому, що не вугілля, залізо та нафта, а саме вона постійно перетворюється в основне загальнолюдське багатство.

Безумовно, жодне суспільство не може існувати без законодавства та нормативних документів, які регламентують правила, процеси, методи виготовлення і контролю якості товарів, робіт та послуг, а також гарантують безпеку життя, здоров'я і майна людей та навколишнього середовища. Стандартизація якраз і є тією діяльністю, яка виконує ці функції.

Стандартизація - діяльність, що полягає у встановлення положень для загального і багаторазового застосування щодо наявних чи можливих завдань з метою досягнення