МОДЕЛЮВАННЯ СКЛАДНИХ СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМ

УДК 330.46:004

О.К. Ткачова

кандидат наук з державного управління, доцент
Академія митної служби України,
м. Дніпропетровськ

ЗАСТОСУВАННЯ МЕТОДУ ЕКСПЕРТНОГО ОЦІНЮВАННЯ ПРИ ПРИЙНЯТТІ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті обґрунтовано концептуальні засади застосування експертного оцінювання при прийнятті рішень щодо інформаційної безпеки. Визначено основні факторні групи експертизи проекту.

Ключові слова: *управління, прийняття рішень, евристичні методи, експертне оцінювання, системи захисту інформації.*

I. Вступ

Останнім часом серед вітчизняних і зарубіжних науковців для розв'язання слабоструктурованих завдань, не виражених кількісно в явній формі, особливої актуальності набуває використання евристичних методів. Основна їх перевага – різнобічний аналіз кількісних та якісних аспектів проблеми, що дає можливість їх використання у складних системах з великою кількістю чинників. Не є винятком і сфера інформаційного забезпечення. Упровадження інформаційних технологій, а отже, і проблема інформаційної безпеки є об'єктивною реальністю та набуває особливого значення як на рівні сучасних організацій, так і на рівні державних структур і суспільства в цілому.

Незважаючи на досить повне висвітлення в наукових публікаціях проблем прийняття управлінських рішень, недостатньо уваги, на нашу думку, приділено розробці концептуальних засад застосування методів експертного оцінювання систем захисту інформації у сфері інформаційної безпеки.

У контексті нашого дослідження особливий інтерес викликають праці таких учених, як С. Бешелєв, Б. Грабовецький, А. Орлов, М. Кендел, В. Ейтінгон та ін. Питання забезпечення інформаційної безпеки, подолання загроз інформаційному суверенітету держави розглянуто в публікаціях В. Авер'янова, С. Гордієнко, Б. Кормич, В. Горбуліна, Г. Козаченко, І. Баймакової, О. Новікова та ін.

II. Постановка завдання

Метою статті є обґрунтування концептуальних засад застосування експертного оцінювання при прийнятті рішення щодо впровадження системи захисту інформації для усунення інформаційних ризиків.

III. Результати

В умовах формування глобального інформаційного суспільства інформаційна безпека кожної держави, зокрема й України, починає відігравати чи не основну роль у забезпеченні національної безпеки в цілому. У сучасній Україні вже є певні позитивні зрушення у правовому регулюванні інформаційних відносин. Так, основними нормативно-правовими актами, спрямованими на забезпечення належного стану інформаційної безпеки в сучасній Україні, зокрема, є Закони України "Про інформацію", "Про доступ до публічної інформації", "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про основи національної безпеки України", Указ Президента України "Про доктрину інформаційної безпеки України" від 08.07.2009 р. № 514/2009 [10] та деякі інші. Як зазначено в Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" [4], інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається завдавання шкоди через: неповноту, невчасність та невірогідність використовуваної інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [4].

Розширення та впровадження сучасних інформаційних технологій на всіх управлінських рівнях супроводжується порушенням режиму інформаційної безпеки. Виникнення інформаційного ризику впливає на якість роботи державного органу. Сьогодні для оцінювання інформаційного ризику використовують стандарт

ISO/IES 27005:2008 [11], в Україні – галузеві стандарти Національного банку України на основі міжнародних стандартів [6]. Однак загальноприйнятої методики управління інформаційними ризиками та їх оцінювання не існує.

Удосконалення системи управління в державних інститутах у напрямі забезпечення якості й ефективності надання відповідних функцій та послуг потребує не тільки поглибленого теоретико-методологічного дослідження, а й застосування сучасних евристичних методів, що дає змогу об'єднати формальний і неформальний аналіз.

Сьогодні в комп'ютерних і телекомунікаційних мережах широко використовують різноманітні системи та засоби захисту інформації [9]. Вони мають забезпечувати захист на належному рівні і водночас не повинні бути занадто складними й вартісними в розробці та функціонуванні [3].

Оскільки для систем захисту інформації характерна велика кількість критеріїв, які, як правило, конфліктують між собою (наприклад, ціна – якість), то вибір конкретної архітектури системи захисту інформації є складною, багатопараметричною задачею, що значною мірою залежить від системи переваг особи або осіб, які здійснюють вибір [9].

Тобто для розв'язання задачі вибору та впровадження оптимальної системи захисту інформації у сфері управління доцільним є використання евристичних методів, а саме експертних оцінювань. Евристичні методи застосовуються при: визначенні цілей; експертному прогнозі; аналізі сценарію розвитку ситуації; генеруванні та дослідженні альтернатив; під час дослідження рейтингів об'єктів або процесів; для прийняття індивідуальних і колективних рішень, у задачах економічного прогнозу та моделювання тощо.

Метод експертних оцінювань є важливим засобом об'єднання формального й неформального методів аналізу. Застосування такого методу оцінювання зумовлене неможливістю повною мірою виміряти ефективність прийнятого рішення лише за допомогою статистичних розрахунків. Цей метод передбачає використання апріорних оцінок показників, що надаються авторитетними спеціалістами-експертами, які працюють у відповідних галузях проектування. Причини залучення експертів до відповідних оцінювань зумовлені багатьма чинниками: неможливістю кількісного вимірювання деяких показників, відсутністю відповідних вимірювальних приладів, складністю досліджуваних явищ, великими витратами коштів або часу при вимірюванні, відсутністю необхідних обсягів вірогідної інформації, суб'єктивністю досліджуваних характеристик тощо.

Під експертизою розуміють оцінювання експертами деяких властивостей та особливостей стану певної системи або процесу. Проведення експертизи – це встановлення відповідностей між якісними оцінками та кількісними значеннями. Якісні експерти є надійним і точним джерелом інформації про стан розвитку об'єкта. На підставі узагальненої думки групи експертів шляхом усереднювання їх індивідуальних думок з'являються оцінки, близькі до істинних значень [2].

Експертне оцінювання проекту є однією з базових функцій управління проектом, разом з управлінням предметною галуззю, тривалістю проекту, вартістю проекту. Для початку процесу оцінювання проекту необхідно мати інформацію про масштаб предметної галузі проекту, опис системи, стандарти й вимоги системи, документацію щодо системи якості. Проведення експертизи дає змогу детально проаналізувати проект, оцінити його ефективність, довести цінність інформаційних технологій, розглянути і зрозуміти зроблені помилки, щоб уникнути їх надалі. Окрім цього, експертиза дає можливість скоректувати стратегії розвитку й супроводу системи.

Для проведення експертизи необхідні такі умови [5]:

- наявність експертної комісії, що складається з фахівців, які знайомі з об'єктом експертизи і мають досвід експертної роботи;
- існування аналітичної групи, що професійно володіє технологією організації та проведення експертиз, методами отримання й аналізу експертної інформації;
- отримання надійної експертної інформації;
- коректна обробка та аналіз експертної інформації.

Виділяють такі основні етапи процедури:

- визначення мети експертизи;
- розробка анкет опитування;
- побудова об'єктів оцінювання або їх характеристик;
- створення групи експертів;
- визначення способу експертного оцінювання і способу надання експертних оцінок;
- проведення експертизи (експерт дає відповідь на запитання);
- обробка й аналіз результатів;
- повторний тур експертизи при необхідності уточнення або зближення думок експертів;
- прийняття рекомендацій.

На початковому етапі організації експертного опитування важливо правильно сформувати групу експертів, кількісний і якісний склад якої забезпечить одержання достовірних результатів. Згідно зі статистичним підходом, викладеним російськими вченими у [7], необхідна й достатня кількість експертів для проведення якісної експертизи визначається за формулою (1):

$$N = \frac{t_\alpha^2}{\varepsilon_1}, \qquad (1)$$

де t_α – показник достовірності для заданої надійної ймовірності одержаного результату;

ε_1 – гранично допустима похибка, виражена як частка середнього квадратичного відхилення (δ): $\varepsilon_1 = \frac{\varepsilon}{\delta}$, де ε – абсолютна похибка.

Якщо узяти $\varepsilon_1 = 0{,}5$ при надійній імовірності $\alpha = 0{,}85$, то необхідна кількість експертів дорівнює 7, що є найпоширенішим випадком [7, с. 8]. Таким чином, розрахункова кількість експертів є нижньою межею, яка забезпечує отримання достовірних результатів експертного оцінювання, а збільшення цієї кількості дасть змогу зменшити похибку достовірності оцінювання.

З іншого боку, збільшення кількості експертів подовжує тривалість проведення експертного опитування, підвищує обсяги фінансування дослідження, ускладнює узгодження думок експертів та формування колективного рішення. Вважається, що достатній обсяг вибірки становить 15–50 осіб, проте на результати експертизи впливає не лише кількість залучених експертів, а і якісний склад експертної групи (фаховий рівень, досвід роботи у відповідній сфері, відповідність посади тощо).

Звернемо увагу, що для отримання достовірних результатів експертизи при формулюванні питань анкети необхідно дотримуватися загальноприйнятих правил: однозначність трактування та вираження відповіді на кожне питання у вигляді кількісної оцінки. Крім того, щоб уникнути нав'язування експерту певних відповідей, доцільно поєднати закриті питання з відкритими, що дасть йому змогу вказати власну альтернативу. На достовірність результатів експертизи також впливає рівень деталізації проблеми: чим він більший, тим вищий рівень узгодженості експертних оцінок. Так, рівень надійності роботи системи захисту інформації може оцінюватися як високий, середній, низький. Проте з метою одержання більш точної оцінки можна застосувати розширену шкалу.

Експертиза проекту застосування системи захисту інформації у сфері управління передбачає проведення аналізу процедури управління проектом на етапі впровадження і включає вивчення всієї документації за проектом, інтерв'ювання експертів.

Незалежний деталізований експертний висновок показує [1]:

– рівень відповідності досягнутих результатів цілям проекту;
– співвідношення між бюджетом проекту й обсягом виконаних робіт;
– наявність ризиків упровадження проекту і шляхи їх мінімізації.

За необхідності розробляють ряд заходів, які дають змогу знизити ризики проекту, у тому числі пов'язані з недоліками виконання робіт за проектом, і підвищити ефективність інвестицій у проект розробки й упровадження системи захисту. Отриману від експертів інформацію об'єктивно обробляють на основі методів рангової кореляції та формалізують [5]. Під ранговою кореляцією розуміють статистичний зв'язок між порядковими змінними. Цей зв'язок слід аналізувати на підставі рядів вхідних статистичних даних, упорядкованих згідно з певними якісними факторними ознаками. Ряд упорядковується за спаданням ступеня прояву факторів, які вивчаються. Рангом факторної ознаки є її місце в цьому ряді.

Якщо експертизу проводять більше ніж два експерти, то узгодженість їх оцінок оцінюють за допомогою множинного коефіцієнта конкордації (W), запропонованого М. Кендалом і Б. Смітом (2):

$$W = \frac{12\sum_{i=1}^{m}(R_i - \bar{R})^2}{l^2(m^3 - m)}, \qquad (2)$$

де m – кількість об'єктів експертизи;

l – кількість експертів;

R_i – сумарний ранг i-го об'єкта за думками всіх експертів;

$\bar{R}$ – середнє значення сумарних рангів.

Коефіцієнт конкордації задовольняє умову: $0 \le W \le 1$ і показує, наскільки збігаються думки експертів. Якщо W = 0, то зв'язку між ранжуванням спеціалістів не існує; якщо W = 1, то всі експерти однаково оцінюють можливі варіанти. Звісно, що чим більше узгодженість поглядів, тим легше прийняти рішення.

Якщо існують повторення рангів (ранги зв'язані), то формула обчислення коефіцієнта конкордації має такий вигляд (3):

$$W = \frac{12\sum_{i=1}^{m}(R_i - \bar{R})^2}{l^2(m^3 - m) - l\sum_{j=1}^{l}(T_j)}, \qquad (3)$$

де T_j – показник зв'язаних рангів, виставлених j-м експертом, розраховується за формулою: $T_j = \sum_{k}^{H_j}(h_k^3 - h_k)$, де H_j – число груп однакових рангів в j-му ранжуванні, h_k – число однакових рангів k-й групі зв'язаних рангів у ранжуванні, виставленому j-м експертом.

Для оцінки значущості коефіцієнта конкордації використовують критерій Пірсона (χ^2). За відсутності зв'язку між рангами фактичне значення критерію Пірсона $\chi^2_{ф}$ обчислюють так: $\chi^2 = W \times l \times (m-1)$ або $\chi^2_{ф} = \frac{12 \times S}{l \times m \times (m+1)}$, де $S = 12 \times \sum_{i=1}^{m}\left(R_i - \bar{R}\right)^2$.

За наявності зв'язку між рангами, коли $t_j \neq 0$, $\chi^2_{ф}$ обчислюють так (4):

$$\chi^2_{ф} = \frac{S}{l \times m \times (m+1) - \frac{\sum_{j=1}^{l}\left(t_j^3 - t_j\right)}{m-1}}. \qquad (4)$$

Після цього перевірка значущості коефіцієнта конкордації здійснюється за правилом:

а) якщо $\chi^2_{ф} > \chi^2_{кр}$, при степені вільності $v = m-1$ і рівні істотності p = 0,95, що розраховується з таблиці критичних точок розподілу χ^2, то коефіцієнт конкордації вважається значущим, а оцінки експертів – узгодженими з надійністю $(1-\alpha)$;

б) якщо $\chi^2_{ф} < \chi^2_{кр}$, то коефіцієнт конкордації вважається незначущим, а оцінки експертів – неузгодженими з надійністю $(1-\alpha)$, де α – вибраний рівень значущості.

Перевірка значущості коефіцієнта конкордації гарантує отримання статистично надійних результатів.

Отже, при виборі системи захисту інформації необхідно виділити фактори (факторні групи) по експертизі (проекту) та факторні ознаки в кожній факторній групі. Нами виділено дві основні факторні групи: а) функціональність системи; б) економічність системи (табл. 1, 2). У кожній факторній групі можна виділити факторні ознаки, за якими експерти надають бали за сформованою шкалою.

Таблиця 1

Факторна група F_1: функціональність системи

№ з/п	Факторні ознаки	Бали	
		від (min)	до (max)
1	Оперативність роботи в режимі реального часу	0	20
2	Надійність системи	0	20
3	Складність в обслуговуванні системи	0	20
5	Продуктивність системи	0	20
6	Ступінь захисту системи	0	20
Загальна сума балів		100	

Таблиця 2

Факторна група F_2: економічність

№ з/п	Факторні ознаки	Бали	
		від (min)	до (max)
1	Зменшення кількості робочих місць	0	25
2	Ціна системи	0	50
3	Підвищення кваліфікації персоналу	0	25
Загальна сума балів		100	

У табл. 1, 2 наведено факторні ознаки (фактори) по кожній із груп і кількість балів, які проставляють експерти по кожному з факторів. Загальна кількість балів по факторній групі не може перевищувати 100 балів. Структуру відомості експертних оцінок якісних факторів наведено у табл. 3.

При оцінюванні узгодженості думок експертів важливо визначити, якою мірою кожний експерт впливає на узагальнену узгодженість групи. Для цього послідовно з розрахунків виключають одного експерта та обчислюють коефіцієнт конкордації без урахування думок виключеного експерта.

Таблиця 3

Відомість експертних оцінок якісних факторів

Експерти	Факторні групи		
	F_{11}	…	F_{11n}
1			
2			
…			
n			

Так, зменшення коефіцієнта конкордації при виключенні конкретного експерта з групи свідчитиме про зниження узгодженості між експертами, і навпаки. Однак виключати з розрахунків експертів треба обережно.

IV. Висновки

Доцільність застосування експертних методів оцінювання системи захисту інформації у сфері управління зумовлена неможливістю використання лише статистичних методів аналізу для оцінювання і прогнозування результатів упровадження управлінських рішень унаслідок їх специфічної індивідуальності. Достовірність результатів експертного оцінювання забезпечена: 1) оптимальним якісним складом експертної групи; 2) структурою анкети; 3) проведенням аналізу процедури експертизи проекту; 4) коректною обробкою та аналізом експертної інформації; 5) застосуванням формальних і неформальних методів аналізу.

Наведена у статті методика застосування експертного оцінювання дає можливість обґрунтування прийняття рішень стосовно проекту вибору та впровадження системи захисту інформації з подальшим її удосконаленням.

Список використаної літератури

1. Бабець І.Г. Застосування експертного опитування для оцінювання ефективності державного управління міжнародним співробітництвом регіону / І.Г. Бабець // Держава та регіони. Серія: Державне управління. – 2010. – № 3. – С. 157–161.

2. Грабовецький Б.Є. Економічне прогнозування і планування : навч. посіб. / Б.Є. Грабовецький – К. : ЦНЛ, 2003. – 188 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К. : ООО "ТИД "ДС", 2002. – 688 с.
4. Закон України "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/537-16/print1330337542993813.
5. Кендал М. Ранговые корреляции / М. Кендал ; пер. с англ. – М. : Статистика, 1975. – 216 с.
6. Лист Департаменту інформатизації НБУ від 03.03.2011 р. № 24-112/365/ [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua.
7. Методы организации экспертизы и обработки экспертных оценок в менеджменте : учеб.-метод. пособ. / [В.Н. Эйтингон, М.А. Кравец, Н.П. Панкратова, В.В. Давнис]. – Воронеж : Изд-во ВГУ, 2004. – 44 с.
8. Орлов А.И. Принятие решений. Теория и методы разработки управленческих решений / А.И. Орлов. – М. : ИКЦ "МарТ", 2005. – 496 с.
9. Титоренко Г.А. Информационные технологии управления : учеб. пособ. для вузов / под ред. проф. Г.А. Титоренко. – 2-е изд., доп. – М. : ЮНИТИ-ДАНА, 2003. – 439 с.
10. Указ Президента України "Про Доктрину інформаційної безпеки України" від 08.07.2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
11. ISO 27005 ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management [Текст]. – ISO / IEC, 2008. – 70 с.

Стаття надійшла до редакції 06.11.2013.

Ткачева О.К. Применение метода экспертной оценки при принятии управленческих решений в сфере информационной безопасности

В статье обоснованы концептуальные принципы применения экспертной оценки при принятии решений относительно информационной безопасности. Отмечены основные факторные группы экспертизы проекта.

Ключевые слова: *управление, принятие решений, эвристические методы, экспертная оценка, системы защиты информации.*

Tkachova O. Application of the method of expert estimation by decision-making in the field of informative safety

Application of the method of expert estimation by decision-making *of informative safety is outlined in the article. Introduction of information technologies and problem of informative safety are objective reality and takes on the special significance both at the level of modern organizations and at the level of state structures and society on the whole.*

There is the interest to the works of scholars such as S. Beshelev, B. Grabovetsky, A. Orlov, M. Kandel, V. Eytyngon etc. The problems of information security discussed in the sovereignty of the state papers of V. Averianova, S. Gordienko, B. Kormich, V. Gorbulina, G. Kozachenko, O. Novikov etc.

The purpose of this paper is the study and justification of conceptual basis for the use of expert estimation by decision-making *in introduction of the system protection of information in the field of informative safety.*

Today in the computer and telecommunications networks are widely used different systems and information security. They must provide protection and would not be too complex and too cost in the development and operation. So for solving the problems of selection and implementation of optimal information security systems it is advisable to use heuristic methods, especially – the method of expert estimation.

In general, heuristics are used for: setting goals, expert forecasts, scenario analysis of the situation, the generation and exploration of alternatives in the study of ratings of objects or processes, to take individual and collective solutions in problems of economic forecasting and modeling and so on.

Method of expert assessments is an important means of combining formal and non-formal methods of analysis. There are following basic steps in the procedure: determining the purpose of the examination; development of the questionnaires; construction of facilities or evaluating their performance; creation of the group of experts; determining of the expert assessment; examination (experts answer the questions); data processing and analysis of results; re-round expertise when it's necessary; adoption of the recommendations. The information obtained from experts objectively processed based on the method of rank correlation and formalized. Pearson criterion (χ^2) is used to assess the significance of the coefficient of concordance.

Thus, in the choice of information security, it is necessary to select factors (factor group) of the examination (project) and the factor variable in each factor group. We have identified two main factor groups: a) the system functionality, b) efficiency of the system. The method of expert estimation *makes it possible to support decision-making on the selection and implementation of information security systems.*

Key words: *management, decision-making, heuristic methods, expert estimation, system of information security.*