УДК 510.649

Н. В. ЛИСАК

ОЦІНЮВАННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ЗАСОБАМИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

Вінницький національний технічний університет

Анотація

У роботі розглянуто вплив значень показників окремих параметрів на загальний стан захищеності інформації. У результаті дослідження розроблено математичну модель оцінювання рівня захисту інформації на підприємстві засобами математичного апарату нечіткої логіки.

Ключові слова: захист інформації, математична модель, нечітка логіка.

Abstract

The paper considers the influence of the values of certain parameters on the data security state in general. As a result of the research, mathematical model of the enterprise data protection level evaluation has been developed using mathematical apparatus of fuzzy logic.

Keywords: data protection, mathematical model, fuzzy logic.

Вступ. Захист інформаційних ресурсів є одним із пріоритетних завдань безпеки підприємств України, оскільки перехід до інформаційного суспільства змінив статус інформації. Наразі вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. За умов постіндустріального етапу інформація перетворилась на стратегічний ресурс економічного і науково-технологічного прогресу. Відтак, захист інформації на підприємствах потребує достатнього теоретико-методологічного підґрунтя [1]. Дослідження можливості застосування математичних методів для оцінювання захисту інформації на підприємстві є досить актуальним питанням за сучасних умов розвитку економіки.

Використання різних методик з метою оцінювання захисту інформації на підприємствах розглядали багато вчених, а саме: В. В. Бут, В. В. Микитенко, О. В. Гребенюк, М. О. Живко, О. А. Сороківська, В. С. Цимбалюк, А. М. Чорна. Проте нерозв’язаним питанням у сфері захисту інформації залишається обґрунтування необхідності використання математичних моделей та методів дослідження. Сучасні методи не завжди є доступними та зручними у використанні, потребують значних матеріальних витрат.

Виклад основного матеріалу. В економіці України після тривалих реформаційних, кризових та посткризових періодів спостерігаємо модифікацію умов функціонування підприємств. Результатом цього є нагальна необхідність забезпечення інформаційної безпеки, що відображатиме захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві. Відтак, захист інформації є складником загальної соціально-економічної безпеки підприємства.

Для висвітлення дискусійності ключових моментів коротко надамо трактування основних категорій.

Захист інформації (англ. data protection) – сукупність методів і засобів, які забезпечують цілісність, доступність і конфіденційність інформації за умов упливу на неї загроз природного або штучного характеру, реалізація яких може зашкодити власникам і користувачам інформації [2; 3].

Захищають інформацію для підтримки таких її властивостей:

● цілісність (англ. integrity) – захист інформації від несанкціонованої модифікації чи видалення її частини;

● доступність (англ. availability) – захист (забезпечення) доступу до інформації, а також можливості її санкціонованого використання з будь-якого місця і в довільний час;

● конфіденційність (англ. confidentiality, prіvacy) – захист інформації від несанкціонованого ознайомлення з нею [4]. Це досить складний процес, адже він вимагає врахування всіх вагомих чинників і встановлення правильних функціональних залежностей. Проте важливо профільтрувати множину чинників, щоб уникнути серед них колінеарних, обернених один до одного, взаємозалежних, взаємодоповнювальних і таких, які дублюють один одного.

Для оцінки інформаційної безпеки часто використовують методи рентабельності витрат на здійснення заходів щодо захисту інформації, методи оцінки шкоди від загрози хакерських атак. Значного поширення отримав метод нечітких множин. При цьому експертним шляхом оцінюють ймовірність подолання системи захисту інформації, імовірність доставки одиниці інформації до споживача, час доставки й апаратурну складність. Інколи використовують показники частки працівників інформаційних відділів у загальній кількості працівників, частки витрат на забезпечення інформаційної безпеки в загальній величині витрат.

Крім того, деякі науковці аналізують такі показники:

– продуктивність інформації;

– коефіцієнт інформаційної озброєності;

– коефіцієнт захищеності інформації [5; 6].

Перелік параметрів оцінювання рівня захисту інформації та ступінь їх конкретизації визначають такою методичною умовою: кількість оцінюваних параметрів повинна бути достатньо обмеженою з метою забезпечення оперативності управлінських рішень, які приймають. Формування та групування параметрів спирається на аналіз широкого комплексу проблем економічного і соціального характеру, тому множина вхідних чинників повинна задовольняти умови повноти, дієвості та мінімальності. За критерієм повноти необхідно визначити таку кількість параметрів, яка охоплювала б усі аспекти діяльності підприємства, але вилучення хоча б одного з них не змінювало результат. На основі сформованої множини за критерієм повноти необхідно виділити групу з максимальним ступенем результативності за критерієм дієвості. За критерієм мінімальності потрібно зменшити кількість параметрів, виключивши ті, які є оберненими, взаємозалежними, взаємодоповнювальними та дублюють один одного.

На основі аналізу закордонних та вітчизняних праць [2 – 7] визначено ключові чинники, які визначають рівень захисту інформації на підприємстві. Можна встановити функціональну залежність між рівнем захисту інформації та факторами впливу на нього у вигляді структурно-логічної схеми. Отже, було розроблено структурно-логічну схему захисту інформації на підприємстві (рис. 1).

Пропонуємо множину вхідних параметрів lc (c $=\overline{1,C}$); сукупність показників, що розраховують на основі оцінювальних параметрів xi (i $=\overline{1,n}$); функцію перетворення вхідних параметрів на оцінювальні показники $F_1 : L \to X;$ множину функцій, на основі яких здійснюють ідентифікацію рівня ефективності політики інформаційної безпеки $F_2 = F(f_1,\ldots, f_i);$ множину вихідних параметрів $E = (e_j),\ j = \overline{1, J}$.

Отже, математична модель такого процесу набула вигляду:

$$L \xrightarrow{F_1} X \xrightarrow{F_2} E, \partial e\ L = (l_c), c = \overline{1,C}, X = (x_i), i = \overline{1,4}, E = (e_j), j = \overline{1,J}$$
$$F_1 = f(x_{11}, x_{12}); F_2 = f(x_{21}, x_{22}); F_3 = f(x_{31},\ldots, x_{36}); F_4 = f(x_{41},\ldots, x_{43}). \quad (1)$$

На основі множини X параметрів xi сформована сукупність функцій перетворення:

F1 – функція ефективності роботи технічного забезпечення; F2 – функція ефективності кадрового складника; F3 – функція ефективності керування інформаційними потоками, F4 – функція ефективності програмного забезпечення.

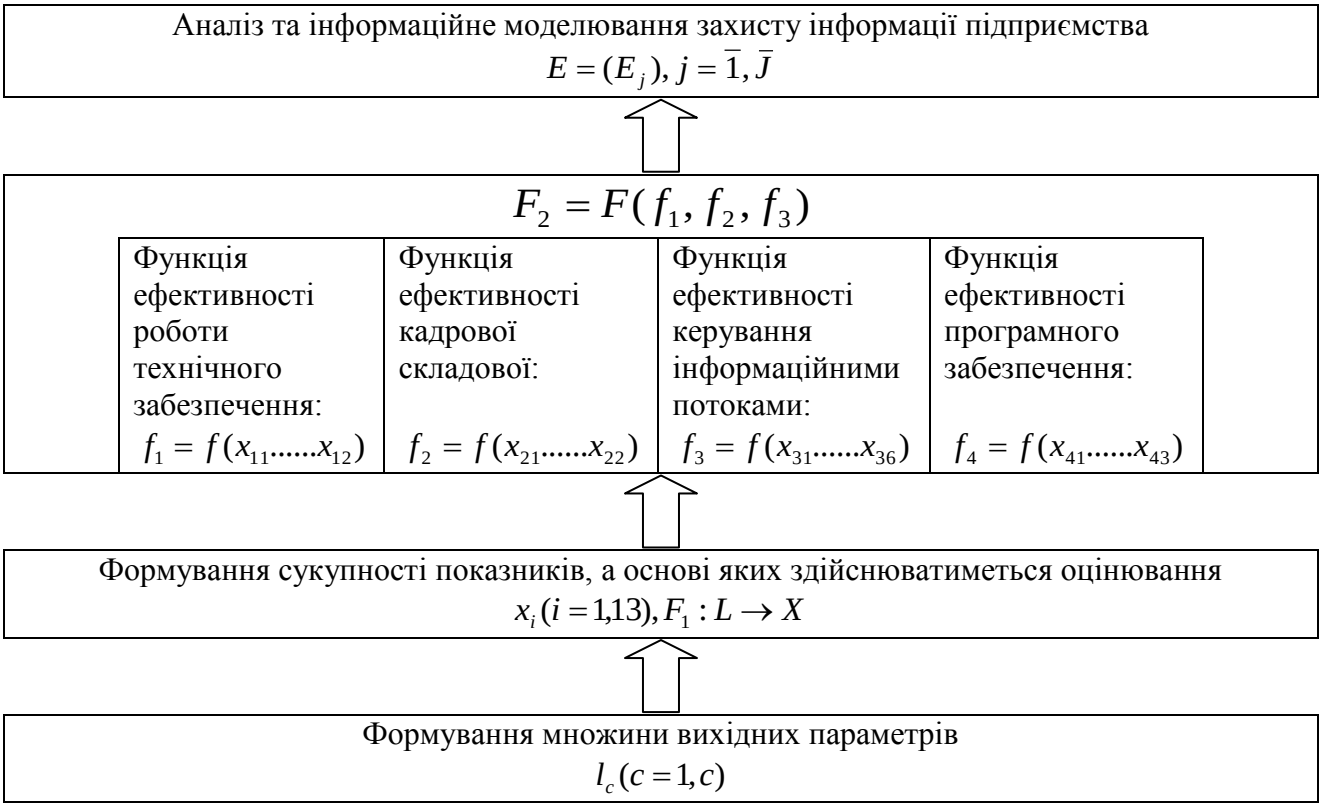

Рисунок 1 – Структура схеми оцінювання рівня захисту інформації на підприємстві

Використання окремих показників (рентабельності, захищеності інформації), а також методів експертних оцінок не дозволяє ефективно ідентифікувати рівень захисту інформації на підприємстві. Для ефективного оцінювання захисту інформації підприємств необхідно використовувати сучасні математичні апарати, які дозволять поєднати не тільки різні за змістом показники і моделі, але й різні за своєю природою – кількісні та якісні параметри. Саме таким інструментом виступає апарат нечітких множин [7]. Важливою перевагою нечітких моделей є їхня прозорість, яка дозволяє їм успішно конкурувати з різними індуктивними методами обробки даних .

Створення моделі оцінювання передбачає 7 етапів.

Результатом виступає сформований методичний підхід до оцінювання рівня захисту інформації на вітчизняних підприємствах, що дозволяє значно скоротити витрати від втрат інформації та безпеки інформаційного простору підприємств.

Висновок. Проведені дослідження методологічного інструментарію побудови математичної моделі дозволили побудувати комплексну модель оцінки ефективності захисту інформації, що дало можливість врахувати основні чинники впливу на рівень захисту інформації та визначити слабкі місця в політиці інформаційної безпеки.

Розроблена модель оцінки рівня захисту інформації на підприємстві дозволяє здійснювати оцінку, ураховуючи чотири групи показників відображення особливого рівня кількісної та якісної сторін ефективності захисту інформації: на рівні технічного захисту, на рівні ефективності роботи кадрів, що забезпечують захист інформації, на рівні ефективності управління інформаційними потоками та на рівні ефективності програмного складника. Модель складається з логічних рівнянь, які описують зв'язок між чинниками, що впливають на рівень захисту інформації.

Дотримання наданих рекомендацій дозволяє вітчизняним підприємствам підтримувати рівень інформаційної безпеки відповідно до вимог сьогодення.

СПИСОК ЛІТЕРАТУРИ

1. Сорокіна І.В. Теоретико-методологічні аспекти формування системи економічної безпеки підприємства // Актуальні проблеми економіки №12(102), 2009. – С. 114-122.

2. Архипов А. Е. Технологии експертного оценивания в задачах защиты информации / А. Е. Архи- пов, С. А. Архипова, С. А. Носок // Інформаційні технології та комп'ютерна інженерія : міжнар. наук.-техн. журн. – № 1. – 2005. – С. 89-94.

3. Степанов А.В. Характерные особенности задачи построения комплексной системы защиты информации распределенных корпоративных ресурсов / А.В. Степанов // Захист інформації. – 2007. – Спец. вип. – С. 131–134.

4. Дудикевич В.Б. Ієрархічна модель захисту даних в інформаційних технологіях / В.Б. Дудикевич, Г.В. Микитин, Ю.Р. Гарасим // Проблеми і перспективи Роозвитку ІТ-індустрії : зб. тез. доп. ІІ Міжнар. наук.-практ. конф. – Харків : Вид-во ХНУРЕ, 2010. – С. 212–213.

5. Ілляшенко, С.М. Економічний ризик : навч. посіб. 2-ге вид., доп., перероб. / С.М.Ілляшенко – К.: Центр навчальної літератури, 2004. – 220с.

6. Реверчук, Н.Й. Управління економічною безпекою підприємницьких структур [Текст]: монографія / Н.Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

7. Ермошин В.В. Методика оценки информационных рисков предприятия // Захист інформації. – 2009. – №4(45), С. 80-88.

Наталія Володимирівна Лисак – канд. техн. наук, доцент кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету, м. Вінниця.

Natalia Volodymyrivna Lysak – Cand. Sc. (Eng), Department of Management and Information Systems Security Vinnytsia National Technical University. Vinnitsa.