УДК 510.649

Н. В. Лисак, к. т. н., доц.; Ю. В. Міронова, к. е. н.; О. Л. Рудковська

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ

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.*

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.

Метою роботи є розробка методичного підходу до оцінювання рівня захисту інформації на підприємстві, якому властива спрощена процедура ідентифікації захищеності за рахунок використання апарату нечіткої логіки.

Об'єктом дослідження є процес удосконалення системи оцінювання рівня захисту інформації на підприємствах.

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, privacy*) – 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 l_c (с $=\overline{1,C}$); сукупність показників, що розраховують на основі оцінювальних параметрів x_i (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:

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

На основі множини X параметрів x_i сформована сукупність функцій перетворення:

F_1 – функція ефективності роботи технічного забезпечення; F_2 – функція ефективності кадрового складника; F_3 – функція ефективності керування інформаційними потоками, F_4 – функція ефективності програмного забезпечення.

Рис. 1. Структура схеми оцінювання рівня захисту інформації на підприємстві

Як було зазначено вище, 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 [8]. Важливою перевагою нечітких моделей є їхня прозорість, яка дозволяє їм успішно конкурувати з різними індуктивними методами обробки даних [9].

Створення моделі оцінювання передбачає 7 етапів.

Перший етап передбачає визначення множини Т лінгвістичних термів, які складаються із сукупності лінгвістичних змінних. Необхідно зазначити, що лінгвістичною вважається змінна, яка набуває свого значення з переліку слів (словосполучень) природної чи штучної мови. За умови сукупності з трьох лінгвістичних термів маємо: Н – низький, С – середній, В – високий. За умови сукупності з п'яти термів: Н – низький, НС – нижче середнього; С – середній, ВС – вище середнього; В – високий. Така кількість лінгвістичних термів ураховує той факт, що найбільш точні та адекватні рішення експерти приймають за 7 аналізованих чинників.

Для оцінювання параметрів (x_{11}, x_{12}, x_{21}, x_{22}, x_{31}, …, x_{36}, x_{41}, …, x_{43}) доцільно використовувати три нечіткі терми, оскільки діапазон зміни параметрів не дуже великий. Необхідно зауважити, що діапазон зміни параметрів у межах від 0 до 1, оскільки попередньо

було проведено нормування значень. Таким чином було отримано функції належності μ^{E_j}, $j=\overline{1,J}$ трьох нечітких термів. Ураховуючи думки експертів щодо специфіки природи обраних параметрів було обрано види функцій належності. Для всіх параметрів була використана Гауссова функція належності, яка найбільшою мірою відповідає специфіці обраних параметрів [8].

Метою другого етапу є визначення графіків функцій належності. Графіки визначають для сукупності параметрів (x_{ij}). Для кожного лінгвістичного терму окремо визначають функцію належності на основі певного переліку функцій належності [10 – 12].

Загальний вигляд функції належності для різних параметрів наведено на рис. 2, рис. 3 і рис. 4.

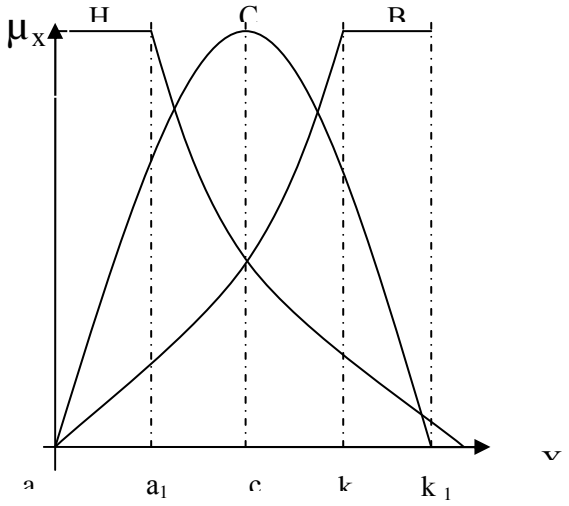

Рис. 2. Загальний вигляд функції належності трьох нечітких термів для параметрів x_{21}, x_{42}, x_{43}

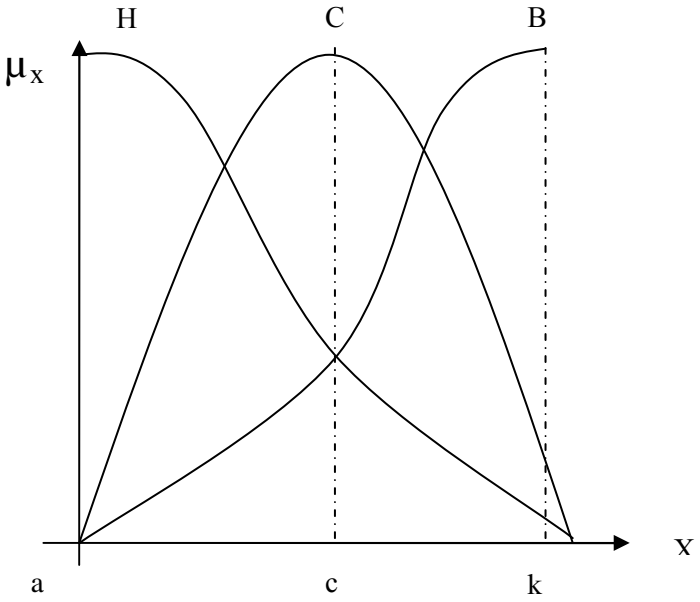

Рис. 3. Загальний вигляд функції належності трьох нечітких термів для параметрів x_{11}, x_{31}

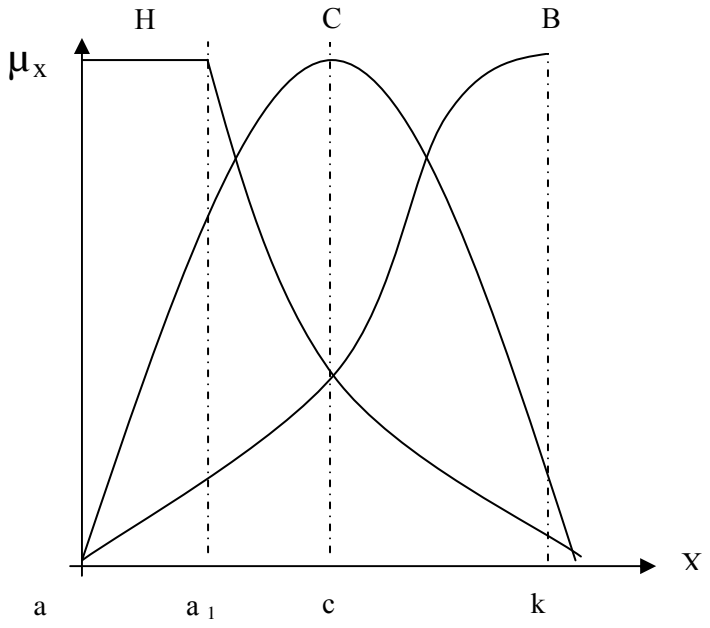

Рис. 4. Загальний вигляд функції належності трьох нечітких термів для параметрів $x_{12,}$ x_{22}, x_{32}, x_{33}, $x_{34,}$ x_{35}, x_{36}, x_{41}

Таблиця 1

Вхідні показники моделі оцінювання рівня захисту інформації підприємства

Скорочена назва показника	Повна назва показника
1. Ефективність роботи технічного забезпечення підприємства	
X_{11}	коефіцієнт технічного захисту інформації
X_{12}	рівень озброєності технічними засобами
2. Ефективність кадрового складника підприємства	
X_{21}	коефіцієнт фінансування інформаційних служб підприємства
X_{22}	коефіцієнт надійності персоналу
3. Ефективність керування інформаційними потоками підприємства	
X_{31}	коефіцієнт правової захищеності інформації
X_{32}	коефіцієнт повноти інформації
X_{33}	коефіцієнт точності інформації
X_{34}	коефіцієнт суперечливості інформації
X_{35}	коефіцієнт своєчасності надання інформації
X_{36}	коефіцієнт надійності інформації
4. Ефективність програмного забезпечення підприємства	
X_{41}	коефіцієнт програмної захищеності інформації
X_{42}	ступінь забезпечення програмними засобами для захисту інформації
X_{43}	рівень ефективності роботи програмного забезпечення

Нижче наведено пояснення до обраних показників та залежності, за якими необхідно їх розраховувати:

1) коефіцієнт технічного захисту інформації (x_{11}):

$$K_{т.з.}=l_3/l_4, \qquad (2)$$

де l_4 – кількість інформаційних атак, на які не відреагував технічний захист;

2) рівень озброєності технічними засобами (x_{12}). Обчислюють як відношення кількості наявних технічних засобів до необхідних;

3) коефіцієнт фінансування інформаційних служб підприємства (x_{21}):

$$K_{фін} = \frac{l_1}{l_2}, \tag{3}$$

де l_1 – витрати на фінансування інформаційних служб підприємства; l_2 – загальні витрати підприємства [3];

4) коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства (x_{22}):

$$K_{н.п} = \frac{l_7 - l_8}{l_7}, \tag{4}$$

де l_7 – загальна чисельність звільнених працівників; l_8 – чисельність працівників, звільнених через витік інформації;

5) коефіцієнт правової захищеності інформації (x_{31}):

$$K_{пр.з} = \frac{l_5}{l_6}, \tag{5}$$

де l_5 – обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, %; l_6 – загальний обсяг юридично захищеної інформації % [6];

6) коефіцієнт повноти інформації (x_{32}):

$$K_{п.ін.} = \frac{l_{10}}{l_9}, \tag{6}$$

де l_9 – обсяг інформації, яка є в розпорядженні %, $l_{10.}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення %;

7) коефіцієнт точності інформації (x_{33}):

$$K_{т.ін.} = \frac{l_{11}}{l_{12}}, \tag{7}$$

де l_{11} – обсяг релевантної інформації %, l_{12} – обсяг інформації, яка є в розпорядженні %;

8) коефіцієнт суперечливості інформації (x_{34}):

$$K_{с.ін.} = \frac{l_{13}}{l_{14}}, \tag{8}$$

де l_{13} – кількість незалежних свідчень на користь ухвалення рішення, l_{14} – загальна кількість незалежних свідчень у сумарному обсязі релевантної інформації;

9) коефіцієнт своєчасності надання інформації (x_{35}):

$$K_{с.н.ін.} = \frac{l_{15.}}{l_{16}}, \tag{9}$$

де $l_{15.}$ – обсяг своєчасно наданої інформації %, l_{16} – обсяг інформації, необхідної для ухвалення обґрунтованого рішення %;

10) коефіцієнт надійності інформації (x_{36}):

$$K_{н.ін.} = \frac{l_{17}}{l_{18}}, \tag{10}$$

де l_{17} – обсяг інформації, наданої з надійних джерел %, l_{18} – загальний обсяг наданої інформації %;

11) коефіцієнт програмної захищеності інформації (x_{41}):

$$K_{п.з.} = \frac{l_{19}}{l_{20}}, \tag{11}$$

де l_{19} – час безперебійного функціонування корпоративної інформаційної системи, l_{20} – нормативний час функціонування корпоративної інформаційної системи [6];

12) ступінь забезпечення програмними засобами для захисту інформації (x_{42}). Обчислюють як відношення кількості наявних програмних засобів до необхідних;

13) рівень ефективності роботи програмного забезпечення (множина характеристик і атрибутів якості згідно з ISO 9126) (x_{43}).

На третьому етапі здійснимо визначення математичних формул, які описують функції належності μ^{E_j}, $j=\overline{1,J}$, що були обрані попередньо.

Для першої функції належності, зображеної на рис. 2, математична формула має вигляд:

$$\mu^{H}(x) = \begin{cases} 1, x \in [a; a_1) \\ \left(\frac{k-x}{k_1-a_1}\right)^n, x \in [a_1; k] \end{cases}, \tag{12}$$

$$\mu^{C}(x) = \frac{1}{1+\left(\frac{x-c}{n}\right)^n}, \tag{13}$$

$$\mu^{B}(x) = \begin{cases} \left(\frac{x-a}{k-a}\right)^n, x \in [a; k] \\ 1, x \in (k; k_1] \end{cases}. \tag{14}$$

Для функції належності, графік якої зображено на рис. 3, математична формула має вигляд:

$$\mu^{H}(x)=\frac{1}{1+\left(\frac{k_1-x}{k_1-a}\right)^{n}}, \tag{15}$$

$$\mu^{C}(x)=\frac{1}{1+\left(\frac{x-c}{n}\right)^{n}}, \tag{16}$$

$$\mu^{B}(x)=\frac{1}{1+\left(\frac{x-k_1}{n}\right)^{n}}. \tag{17}$$

Для функції належності, зображеної на графіку рис. 4, математична формула має вигляд:

$$\mu^{H}(x)=\begin{cases}1, x\in[a;a_1)\\ \left(\frac{k-x}{k_1-a_1}\right)^{n}, x\in[a_1;k]\end{cases}, \tag{18}$$

$$\mu^{C}(x)=\frac{1}{1+\left(\frac{x-c}{n}\right)^{n}}, \tag{19}$$

$$\mu^{B}(x)=\frac{1}{1+\left(\frac{x-k_1}{n}\right)^{n}}. \tag{20}$$

На наступному етапі формуємо групи показників та встановлюємо числові межі для трьох термів (табл. 2). Залежно від необхідності врахування жорстких меж зміни низького та високого рівня параметрів обираємо для кожного з них одну з трьох функцій (графіків).

Таблиця 2

Формулювання показників за шкалою нечітких термів «0 – 1»

Повна назва показника	Скорочена назва показника	Графік	Значення показників для термів		
			Н	С	В
І. Ефективність роботи технічного забезпечення підприємства					
коефіцієнт технічного захисту інформації	X_{11}	Рис. 3	0	0,2	1
рівень озброєності технічними засобами	X_{12}	Рис. 4	0 – 0,2	0,5	1
ІІ. Ефективність кадрового складника підприємства					
коефіцієнт фінансування інформаційних служб підприємства	X_{21}	Рис. 2	0 – 0,3	0,5	0,7 – 1
коефіцієнт надійності персоналу	X_{22}	Рис. 4	0 – 0,3	0,5	1
ІІІ. Ефективність керування інформаційними потоками підприємства					
коефіцієнт правової захищеності інформації	X_{31}	Рис. 3	0	0,5	1
коефіцієнт повноти інформації	X_{32}	Рис. 4	0 – 0,2	0,4	1
коефіцієнт точності інформації	X_{33}	Рис. 4	0 – 0,2	0,4	0,6 – 1
коефіцієнт суперечливості інформації	X_{34}	Рис. 4	0 – 0,1	0,5	1
коефіцієнт своєчасності надання інформації	X_{35}	Рис. 4	0 – 0,1	0,5	1
коефіцієнт надійності інформації	X_{36}	Рис. 4	0 – 0,1	0,5	1
IV. Ефективність програмного забезпечення підприємства					
коефіцієнт програмної захищеності інформації	X_{41}	Рис. 4	0 – 0,1	0,5	1
ступінь забезпечення програмними засобами для захисту інформації	X_{42}	Рис. 2	0 – 0,3	0,5	0,6 – 1
рівень ефективності роботи програмного забезпечення	X_{43}	Рис. 2	0 – 0,3	0,5	0,6 – 1

На наступному етапі розроблення математичної моделі оцінювання ефективності політики інформаційної безпеки на підприємстві, використовуючи попередньо отриману інформацію про значення параметрів, було складено матриці знань для оцінювання груп параметрів оцінки. Побудовані матриці було описано логічними рівняннями, які встановлюють зв'язок між f_i .

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 [13].

Висновки

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 допомагає 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 / І. В. Сорокіна // Актуальні проблеми економіки. – 2009. – №12 (102). – С. 114 – 122.

2. Архипов А. Е. Технологии экспертного оценивания в задачах защиты информации / А. Е. Архипов, С. А. Архипова, С. А. Носок // Інформаційні технології та комп'ютерна інженерія : міжнар. наук.-техн. журн. – 2005. – № 1. – 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. – 220 с.

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

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

8. Ротштейн А. П. Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі : монографія / А. П. Ротштейн. – Вінниця : Універсум-Вінниця, 1999. – 320 с.

9. Штовба С. Д. Порівняння критеріїв навчання нечіткого класифікатора / С. Д. Штовба // Вісник ВПІ. – 2007. – № 6. – С. 84 – 91.

10. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : "МК-Прес", 2006. – 320 с

11. Самарский А. А. Математическое моделирование : Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов. – М. : Физматлит, 2001. – 213 с.

12. Сергеева Л. Н. Нелинейная экономика: модели и методы / Л. Н. Сергеева. – Запорожье : Полиграф, 2003. – 217 с.

13. Стасюк А. И. Анализ методов выполнения нечетких операций над нетолерантными числами для использования в системах защиты информации / А. И. Стасюк, А. Г. Корченко, В. В. Душеба, В. А. Рындюк, Н. В. Семенова // Зб. наук. пр. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова. – 2002. – Вип. 18. – С. 27 – 30.

Лисак Наталія Володимирівна – доцент кафедри менеджменту та безпеки інформаційних систем.

Міронова Юлія Володимирівна – старший викладач кафедри менеджменту та безпеки інформаційних систем.

Рудковська Ольга Леонідівна – асистент кафедри фінансів.
Вінницький національний технічний університет.