УДК 004.056

Д. О. Сікорський,
аспірант, Київський національний університет імені Тараса Шевченка

МЕТОДИКА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ В CRM СИСТЕМАХ НА ПІДГРУНТІ НЕЧІТКОЇ ЛОГІКИ

D. Sikorskiy,
post-graduate student, Taras Shevchenko Kyiv National University

TECHNIQUES OF EVALUATION OF INFORMATION RISKS IN CRM SYSTEMS BASED ON FUZZY LOGIC

У статті досліджено проблему ризиків інформаційної безпеки CRM систем. Запропоновано методику оцінювання ризиків, що грунтується на використанні апарату нечіткої логіки. Здійснено лінгвістичний опис рівня частоти можливих втрат внаслідок впливу чинників загрози. Визначено математичну форму запису вирішальних правил за допомогою функцій належності для визначення рівнів інформаційних ризиків.

The paper studies the question of information risks in CRM systems. The techniques of their evaluation based on fuzzy logic methods is proposed. The study contents linguistic description of the frequency of the possible losses caused by the danger influence. The mathematical form of critical rules for determination of information risks level is defined.

Ключові слова: інформаційна безпека, інформаційний ризик, корпоративна інформаційна система, лінгвістична змінна, лінгвістичний критерій, функція належності, нечітка множина.

Key words: information security, information risk, corporate information system, linguistic variable, linguistic criteria, membership function, fuzzy set.

ПОСТАНОВКА ПРОБЛЕМИ

Управління інформаційною безпекою має велике значення для будь-якого господарюючого суб'єкту, який у своїй діяльності використовує сучасні технології збору, зберігання й оброблення інформації. Невід'ємною частиною цього процесу є управління ризиками, яке визначається як формальні процеси, пов'язані з ідентифікацією, аналізом, оцінюванням ризиків та прийняттям рішень, які включають максимізацію позитивних і мінімізацію негативних наслідків настання ризикових подій. Запобігання загрозам безпеки шляхом управління ризиками спрямоване на захист економічних, соціальних та інформаційних інтересів підприємства та є дієвим інструментом економічного менеджменту.

Впровадження провідних інформаційних технологій завжди пов'язане з новими ризиками. Чим складнішою є структура CRM системи, тим вищим є ступінь ризику здійснення стосовно неї загроз: проникнення ззовні чи несанкціонований доступ зсередини підприємства, зокрема з метою фінансового шахрайства або розкриття комерційної таємниці, викривлення чи знищення інформації тощо.

З метою управління інформаційними ризиками розроблені спеціальні методики на базі міжнародних (ISO 17999, ISO 27005, ISO 15408) і національних стандартів. Так, виділяють якісні методики управління ризиками на основі вимог ISO 17999. Другу групу методик управління ризиками складають кількісні методики, актуальність яких обумовлена необхідністю вирішення оптимізаційних завдань, що виникають у господарській діяльності підприємства.

До третьої групи відносяться методики, які включають у себе частково автоматизовані методи, що дозволяють гнучко і ефективно аналізувати й оцінювати інформаційні ризики підприємства. Такі методики крім якісних характеристик ризику, дають і кількісні величини, що важливо для вирішення оптимізаційних завдань проведення аналізу ризиків.

На особливий інтерес заслуговує використання апарату нечіткої логіки. Нечіткі описи в структурі методу аналізу

Таблиця 1. База знань для визначення рівня вразливості

Номер вхідної комбінації	Узагальнені значення груп показників		Вага	Кінцева змінна
	h_{2_1}	h_{2_2}	q_{ij}	H_2
11	TC_VH	CS_VL	q_{11}	V_VH
12	TC_VH	CS_L	q_{12}	V_VH
…				
16	TC_M	CS_VL	q_{16}	
21	TC_VH	CS_H	q_{21}	V_H
…				
24	TC_L	CS_VL	q_{24}	
…				
51	TC_M	CS_VH	q_{51}	V_VL
…				
56	TC_VL	CS_VH	q_{56}	

Джерело: розроблено автором.

ризиків з'являються у зв'язку із невпевненістю експерта, яка виникає в процесі класифікацій різного роду.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У сучасній науковій літературі, в національних і міжнародних стандартах приділяється значна увага проблемам управління ризиками, які пов'язані з використанням інформації в діяльності господарюючих суб'єктів. Разом з тим залишається невирішеним ціла низка проблем, головна з яких — відсутність методологій оцінювання інформаційних ризиків, що забезпечували б системний підхід до управління інформаційною безпекою як окремих інформаційних систем, так і підприємства в цілому.

МЕТА СТАТТІ

Метою статті є розроблення методики аналізу ризиків безпеки з врахуванням таких параметрів, як рівні частоти виникнення подій загрози та вразливості інформаційної системи, із застосуванням апарату нечіткої логіки. Така методика міститиме незначну частку суб'єктивізму та матиме властивості гнучкості й адаптивності за умов подальшого переоцінювання ризиків в процесі функціонування системи.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У науковій та спеціальній літературі виділяють чотири основні кроки аналізу інформаційних ризиків [1, с.10]:

I. Ідентифікація компонент:

1) інформаційних ресурсів (активів) підприємства, що можуть бути об'єктом ризику;

2) можливих загроз активу. Для управління ризиками необхідно ідентифікувати можливі небезпеки, які загрожують інформаційній системі. Такими можуть бути, наприклад, стихійне лихо, відключення електроживлення або атаки зловмисників із наслідками різного ступеню складності. На цьому етапі рекомендується врахувати всі ризики, але з оцінюванням тільки тих, реалізація яких можлива виходячи з прийнятої моделі порушника [3, с. 251]. Наприклад, якщо модель порушника не описує категорію віддалених користувачів, то ймовірність витоку інформації у результаті доступу до неї ззовні дуже мала, і нею можна знехтувати при розрахунку ризиків.

II. Оцінювання частоти подій можливих втрат внаслідок дії ризику [1, с. 27]:

— можливий рівень сили (Threat capability), з якою агенти загрози впливатимуть на актив. Припускається, що деяка частина популяції агентів загрози є більш здатною до впливу на актив, ніж інша;

— очікувана дієвість засобів контролю (Control strength) впродовж відведеного часового інтервалу. Взявши за основу зорієнтованість на середню здатності агентів загрози, приймається базовий рівень ефективності контролю;

— вразливість розглядається як результат впливу факторів можливого рівня сили загрози та дієвості засобів контролю;

— частота виникнення загрози — можлива частота реалізації чинників ризику (агентів загрози) в межах певного часового інтервалу. Під чинниками розуміють опис типів зловмисників, які навмисно або випадково, діями або бездіяльністю здатні нанести збитки CRM системі;

— частота виникнення подій втрат — можлива частота протягом визначеного часового інтервалу, з якою агент загрози завдає шкоди активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості.

III. Оцінювання величини можливих збитків:

— визначення можливої дії кожного з агентів загрози інформаційному активу;

— оцінювання величини кожної з можливих форм збитків, що пов'язані з дією певного агенту загрози;

— оцінювання величини всіх можливих форм збитків.

IV. Результат аналізу інформаційних ризиків CRM системи зводиться до оцінювання загального рівня інформаційних ризиків в інформаційній системі.

На першому етапі необхідно сформувати набір окремих показників:

— для оцінювання рівня частоти виникнення подій загрози CRM системі:

$$H_1 = f_1\left(h_{1_1}, h_{1_2}, h_{1_3}, h_{1_4}, h_{1_5}, h_{1_6}, h_{1_7}\right) \quad (1),$$

де h_{1_1} — статистика зареєстрованих несприятливих подій у системах подібної структури; h_{1_2} — тенденції в статистиці за подібними порушеннями; h_{1_3} — наявність у системі інформації, в якій можуть бути зацікавлені потенційні внутрішні чи зовнішні порушники; h_{1_4} — оцінка моральних якостей персоналу; h_{1_5} — можливість отримати вигоду зі зміни інформації, що опрацьовується системою; h_{1_6} — наявність альтернативних способів доступу до інформації; h_{1_7} — статистика порушень в інших інформаційних системах підприємства;

— для оцінювання рівня вразливості системи:

$$H_2 = f_2\left(h_{2_1}, h_{2_2}\right) \quad (2),$$

де h_{2_1} — оцінка рівня сили загрози; h_{2_2} — оцінка рівня дієвості засобів контролю захисту інформації.

Для оцінювання та опрацювання лінгвістичної змінної H_2 сформовано шкалу з п'яти якісних термів [6, с. 187;

Таблиця 2. База знань для визначення рівня частоти можливих втрат активів від інформаційних ризиків

Номер вхідної комбінації	Узагальнені значення груп показників		Вага m	Кінцева змінна Υ
	H_1	H_2		
11	TF_VH	V_M	m_{11}	LEF_VH
12	TF_VH	V_H	m_{12}	
13	TF_VH	V_VH	m_{13}	
21	TF_VH	V_L	m_{21}	LEF_H
…				
24	TF_H	V_VH	m_{24}	
…				
51	TF_M	V_VL	m_{51}	LEF_VL
…				
58	TF_VL	V_VH	m_{58}	

Джерело: розроблено автором.

7, с. 313]: V_VH — "дуже високий" рівень вразливості, V_H — "високий", V_M — "середній", V_L — "низький", V_VL — "дуже низький". Терм-множина вихідної змінної H_2 матиме вигляд:

$$VL=\{V\_VH,V\_H,V\_M,V\_L,V\_VL\} \quad (3).$$

У таблиці 1 наведено фрагмент набору вирішальних правил, що були сформовані з використанням [1; 6; 8].

Наступним кроком є визначення математичної форми запису вирішальних правил за допомогою функцій належності та з використанням бази знань для визначення рівня вразливості CRM системи. Наприклад, вирішальне правило для визначення вразливості рівня V_M може бути записане таким чином:

$$\begin{aligned}\mu^{V-M}(h_{2_1},h_{2_2})&=q_{31}\left[\mu^{TC-VL}(h_{2_1})\bullet\mu^{CS-VL}(h_{2_2})\right]\vee\\ \vee q_{32}&\left[\mu^{TC-L}(h_{2_1})\bullet\mu^{CS-L}(h_{2_2})\right]\vee q_{33}\left[\mu^{TC-M}(h_{2_1})\bullet\mu^{CS-M}(h_{2_2})\right]\vee\\ \vee q_{34}&\left[\mu^{TC-H}(h_{2_1})\bullet\mu^{CS-H}(h_{2_2})\right]\vee q_{35}\left[\mu^{TC-VH}(h_{2_1})\bullet\mu^{CS-VH}(h_{2_2})\right],\end{aligned} \quad (4),$$

де $\mu^{V-M}(h_{2_1},h_{2_2})$ — функція належності вектора вхідних змінних (h_{2_1},h_{2_2}) значенню кінцевої змінної H_2; $q_{3k}(k=\overline{1,5})$ — ваговий коефіцієнт для відповідної k-ї комбінації; $\mu^{d_j}(h_{2_1})$ — функція належності параметра h_{2_1} до нечіткого терму $d_j\in D$ ($D=\{TC\_VH,TC\_H,TC\_M,TC\_L,TC\_VL\}$ —характеризує загальний рівень загрози); $\mu^{em_i}(h_{2_2})$ — функція належності параметра h_{2_2} до нечіткого терму $em_i\in EM$ ($EM=\{CS\_VH,CS\_H,CS\_M,CS\_L,CS\_VL\}$ — рівень дієвості засобів контролю).

Для оцінювання й опрацювання лінгвістичної змінної H_1 сформовано шкалу з п'яти якісних термів: TF_VH — "дуже високий", TF_H — "високий", TF_M — "середній", TF_L — "низький", TF_VL — "дуже низький" рівень частоти виникнення подій загрози. Терм-множина вхідної змінної H_1 матиме вигляд:

$$TF=\{TF\_VH,TF\_H,TF\_M,TF\_L,TF\_VL\} \quad (5).$$

Для оцінювання значень кінцевої лінгвістичної змінної Υ, що є множиною ступенів частоти виникнення можливих втрат, використовуються терми: LEF_VH — "дуже висока" частота, LEF_H — "висока", LEF_M — "середня", LEF_L — "низька", LEF_VL — "дуже низька". Терм-множина вихідної змінної Υ матиме вигляд:

$$LEF=\{LEF\_VH,LEF\_H,LEF\_M,LEF\_L,LEF\_VL\} \quad (6).$$

На підставі розрахованих значень груп показників проводиться оцінювання рівня частоти виникнення можливих втрат активів інформаційної системи внаслідок впливу загроз:

$$\Upsilon=f_\Upsilon(H_1,H_2) \quad (7).$$

Визначається можливий діапазон змінювання контрольованих параметрів H_1, H_2 та кінцевої змінної Υ. Задається вигляд функцій належності нечітких термів для різних контрольованих параметрів.

Наступним етапом аналізу є формування системи нечітких знань для визначення кожного з рівнів частоти можливих втрат. На основі [1, 4, 6] сформовано набір вирішальних правил, які реалізують співвідношення (7). У таблиці 2. наведено фрагмент такого набору.

Критеріїв H_1 та H_2, які є значеннями зазначених груп показників, необхідно подати у вигляді математичних залежностей від вихідних чинників. Тобто сформувати систему нечітких знань для визначення рівнів загроз і вразливості CRM системи.

Наступним кроком є визначення математичної форми запису вирішальних правил за допомогою функцій належності для визначення рівнів частоти виникнення можливих втрат. Наприклад, вирішальне правило для визначення частоти можливих втрат рівня LEF_L може бути записане таким чином:

$$\begin{aligned}\mu^{LEF-L}(H_1,H_2)&=m_{41}\left[\mu^{TF-H}(H_1)\bullet\mu^{V-VL}(H_2)\right]\vee\\ \vee m_{42}&\left[\mu^{TF-M}(H_1)\bullet\mu^{V-L}(H_2)\right]\vee m_{43}\left[\mu^{TF-L}(H_1)\bullet\mu^{V-M}(H_2)\right]\vee\\ \vee m_{44}&\left[\mu^{TF-L}(H_1)\bullet\mu^{V-H}(H_2)\right]\vee m_{45}\left[\mu^{TF-L}(H_1)\bullet\mu^{V-VH}(H_2)\right],\end{aligned} \quad (8),$$

де $\mu^{LEF-L}(H_1,H_2)$ — функція належності вектора вхідних змінних H значенню кінцевої змінної Υ; $m_{4k}(k=\overline{1,5})$ — ваговий коефіцієнт для відповідної k-ї комбінації; $\mu^{tf_j}(H_1)$ — функція належності параметра H_1 до нечіткого терму $tf_j\in TF$; $\mu^{vl_i}(H_2)$ — функція належності параметра H_2 до нечіткого терму $vl_i\in VL$.

Величину втрати P інформаційних активів пропонуємо характеризувати за факторами: V_1 — продуктивність; V_2 — внутрішні витрати (реакція); V_3 — вартість заміни активу; V_4 — штрафи та санкції; V_5 — втрати, що призводять до зниження конкурентоспроможності організації; V_6 — репутація організації.

Таблиця 3. База нечітких знань стосовно величини можливих збитків інформаційних активів

Номер вхідної комбінації	Вхідні змінні						Вагові коефіцієнти w	Вихідна змінна P
	V_1	V_2	V_3	V_4	V_5	V_6		
11	L_VH	L_VH	L_VH	L_VH	L_VH	L_VH	w^i_{11}	PL_VH
12	L_VH	L_VH	L_VH	L_VH	L_VH	L_H	w^i_{12}	
...								
$1k_1$	L_H	L_H	L_H	L_VH	L_VH	L_VH	w_{1k_1}	
21	L_H	L_H	L_H	L_H	L_VH	L_VH	w_{21}	PL_H
...								
$2k_2$	L_H	L_H	L_H	L_H	L_M	L_M	w_{2k_2}	
31	L_H	L_H	L_H	L_M	L_M	L_M	w_{31}	PL_Sg
...								
$3k_3$	L_M	L_M	L_M	L_M	L_H	L_H	w_{3k_3}	
	V_1	V_2	V_3	V_4	V_5	V_6		
41	L_M	L_M	L_M	L_M	L_M	L_H	w_{41}	PL_M
...								
$4k_4$	L_L	L_L	L_L	L_M	L_M	L_M	w_{4k_4}	
51	L_L	L_L	L_L	L_L	L_M	L_M	w_{51}	PL_L
...								
$5k_5$	L_VL	L_VL	L_VL	L_L	L_L	L_L	w_{5k_5}	
61	L_VL	L_VL	L_VL	L_VL	L_L	L_L	w_{61}	PL_VL
...								
$6k_6$	L_VL	L_VL	L_VL	L_VL	L_VL	L_VL	w_{6k_6}	

Джерело: розроблено автором.

Оцінювання фактору V_j, $j=\overline{1,6}$, проводиться експертом за шкалою: L_VH — "збитки дуже великі", L_H — "збитки великі", L_M — "збитки середні", L_L — "збитки малі", L_VL — "збитки дуже малі". Тобто, терм-множина вхідних змінних в загальному вигляді представляється у вигляді:

$$LA=\{L\_VH, L\_H, L\_M, L\_L, L\_VL\} \quad (9).$$

Для оцінювання та опрацювання лінгвістичного показника сформовано шкалу з шести якісних термів: PL_VH — "дуже високий" рівень збитків, PL_H — "високий", PL_Sg — "суттєвий", PL_M — "середній", PL_L — "низький", PL_VL — "дуже низький" рівень збитків у відповідних грошових одиницях відносно бюджету проекту інформаційної системи. А терм-множина вихідної змінної P записується у вигляді:

$$LD=\{PL\_VH, PL\_H, PL\_Sg, PL\_M, PL\_L, PL\_VL\} \quad (10).$$

На підставі значень групи показників V_j, $j=\overline{1,6}$ проводиться оцінювання величини можливих збитків інформаційних активів CRM системи від інформаційних ризиків:

$$P=\vartheta_P(V_1,V_2,V_3,V_4,V_5,V_6) \quad (11).$$

Базу нечітких знань стосовно величини можливих збитків інформаційних активів від інформаційних ризиків можна подати у вигляді табл. 3.

Систему нечітких знань для опису моделі оцінювання величини можливих збитків інформаційних активів CRM системи від інформаційних ризиків запишемо у вигляді:

$$u^{ld_i}(V_1,V_2,\ldots,V_6)=\bigvee_{p=1}^{k_i}\left(w_{ip}\left[\bigwedge_{j=1}^{6}\mu^{la^{ip}_j}(V_j)\right]\right), i=\overline{1,6}, \quad (12),$$

де $\mu^{ld_i}(V_1,V_2,\ldots,V_6)$ — функція належності вектора вхідних змінних $(V_1,V_2,\ldots,V_6)$ значенню вихідної змінної ld_i з множини (10); k_i — кількість комбінацій значень змінних $(V_1,V_2,\ldots,V_6)$, для яких вихідна змінна приймає значення ld_i з множини (10); w_{ip} — ваговий коефіцієнт для відповідної комбінації; $\mu^{la^{ip}_j}(V_j)$ — функція належності вхідної змінної V_j до нечіткого терму la_j з множини (9).

На підставі розрахованих значень груп показників рівня частоти подій втрат інформаційних активів та величини можливих збитків внаслідок інформаційних ризиків проводиться оцінювання загального рівня інформаційних ризиків в CRM системі:

$$\Lambda=f_\Lambda(\Upsilon,P) \quad (13),$$

де Υ — отримана з (7) оцінка рівня частоти подій втрат інформаційних активів; P — попередньо оцінена в (11) величина можливих збитків.

Для оцінювання та опрацювання лінгвістичної змінної Λ рекомендуємо скористатися шкалою з чотирьох якісних термів: C — "критичний", H — "високий", M — "середній", L — "низький" рівень ризику. Терм-множина вихідної змінної Λ представляється у вигляді:

$$IR=\{C,H,M,L\} \quad (14).$$

Наступним етапом аналізу є формування системи нечітких знань для визначення кожного з рівнів інформаційних ризиків. Використовуючи [1; 2; 5], сформовано набір вирішальних правил, які реалізують співвідношення (14). У таблиці 4 наведено фрагмент такого набору.

Наступним кроком є визначення математичної форми запису вирішальних правил за допомогою функцій на-

Таблиця 4. База знань для визначення рівня інформаційних ризиків

Узагальнені значення груп показників		Вага	Вихідна змінна Λ
Υ	P	r_{ij}	
LEF_M	PL_VH	r_{11}	C
…			
LEF_VH	PL_Sg	r_{16}	
LEF_VL	PL_VH	r_{21}	H
…			
LEF_VH	PL_L	r_{29}	H
…			
LEF_VL	PL_M	r_{41}	L
…			
LEF_M	PL_VL	r_{46}	

Джерело: розроблено автором.

лежності для визначення рівнів інформаційних ризиків. Наприклад, вирішальне правило для визначення інформаційних ризиків рівня *M* може бути записане таким чином:

$$\begin{aligned}\mu^{M}(\Upsilon,P)=\ & m_{31}\left[\mu^{LEF\_VL}(\Upsilon)\bullet\mu^{PL\_H}(P)\right]\vee\\ \vee\, & m_{32}\left[\mu^{LEF\_VL}(\Upsilon)\bullet\mu^{PL\_Sg}(P)\right]\vee m_{33}\left[\mu^{LEF\_L}(\Upsilon)\bullet\mu^{PL\_Sg}(P)\right]\vee\\ \vee\, & m_{34}\left[\mu^{LEF\_L}(\Upsilon)\bullet\mu^{PL\_M}(P)\right]\vee m_{35}\left[\mu^{LEF\_M}(\Upsilon)\bullet\mu^{PL\_M}(P)\right]\vee\\ \vee\, & m_{36}\left[\mu^{LEF\_M}(\Upsilon)\bullet\mu^{PL\_L}(P)\right]\vee m_{37}\left[\mu^{LEF\_H}(\Upsilon)\bullet\mu^{PL\_L}(P)\right]\vee\\ \vee\, & m_{38}\left[\mu^{LEF\_H}(\Upsilon)\bullet\mu^{PL\_VL}(P)\right]\vee m_{39}\left[\mu^{LEF\_VH}(\Upsilon)\bullet\mu^{PL\_VL}(P)\right],\end{aligned} \quad (15),$$

де $\mu^{M}(\Upsilon,P)$ — функція належності вихідної змінної Λ значенню M з нечіткого терму (14); $m_{3k}(k=\overline{1,9})$ — ваговий коефіцієнт для відповідної k-ї комбінації; $\mu^{lef_j}(\Upsilon)$ — функція належності параметра Υ до нечіткого терму lef_j з терм-множини LEF; $\mu^{ld_i}(P)$ — функція належності параметра P до нечіткого терму ld_i з терм-множини (10).

Таким чином формується вся база знань з використанням експертних даних та виводиться система нечітких логічних рівнянь.

ВИСНОВКИ

Результатом розробленої методики оцінювання ризиків інформаційної безпеки CRM системи, в основу якої покладена концепція та інструментарій оцінювання рівня частоти подій загроз та величини можливих втрат інформаційних активів, є лінгвістичний опис загального рівня інформаційних ризиків в інформаційній системі. Використанням апарату нечіткої логіки для управління ризиками дозволяє сформувати математичну модель не тільки з можливістю налагодження її на певну інформаційну систему, але й з урахуванням подальшого переоцінювання ризиків.

Література:

1. Jones J.A. An Introduction to FAIR / J.A. Jones — Trustees of Norwich University, 2005 — 67 p.
2. Zadeh L. A. Fuzzy sets / L. A. Zadeh. — Information and Control. — 1965. — № 8. — P. 338—353.
3. Вертузаєв М.С. Захист інформації в комп'ютерних системах від несанкціонованого доступу: навч. посібник / М.С. Вертузаєв, О.М. Юрченко, за ред. С.Г. Лаптєва. — К.: Вид-во Європ. ун-ту, 2001. — 321 с.
4. Єріна А.М. Статистичне моделювання та прогнозування: навч. посібник / А.М. Єріна. — К.: КНЕУ, 2001. — 170 с.
5. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений / Л. Заде. — М.: Мир, 1976. — 167 с.
6. Матвійчук А.В. Моделювання економічних процесів із застосуванням методів нечіткої логіки / А.В. Матвійчук. — К.: КНЕУ, 2007. — 264 с.
7. Мельник Г.В. Факторний аналіз і моделювання процесу управління інформаційними ризиками / Г.В. Мельник // Економіка: проблеми теорії та практики: Збірник наукових праць. — Дніпропетровськ: ДНУ, 2008. — Випуск 235: В 4 т. — Т. II. — С. 312—321.
8. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А.П. Ротштейн. — Винница: УНІВЕРСУМ-Вінниця, 1999. — 320 с.

References:

1. Jones, J.A. (2005), An Introduction to FAIR, Trustees of Norwich University.
2. Zadeh, L.A. (1965), "Fuzzy sets", Information and Control, vol. 8, pp. 338—353.
3. Vertuzaiev, M.S. and Yurchenko, O.M. (2001), Zakhyst informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu [Information security in computer systems from unauthorized access], Vyd-vo Yevrop. un-tu, Kyiv, Ukraine.
4. Yerina, A.M. (2001), Statystychne modeliuvannia ta prohnozuvannia [Statistical modeling and forecasting], KNEU, Kyiv, Ukraine.
5. Zade, L. (1976), Ponjatie lingvisticheskoj peremennoj i ee primenenie k prinjatiju priblizhennyh reshenij [Concept of Linguistic Variable and its Usage in Approximate Decisions Making], Myr, Moscow, USSR.
6. Matviichuk, A.V. (2007), Modeliuvannia ekonomichnykh protsesiv iz zastosuvanniam metodiv nechitkoi lohiky [Modeling of Economic Processes Using Fuzzy Logic Methods], KNEU, Kyiv, Ukraine.
7. Melnyk, G.V. (2008), "Factor Analysis and Modeling of Process of Information Risk Management", Ekonomika: problemy teorii ta praktyky, vol. 2, no. 235, pp. 312—321.
8. Rothstein, A.P. (1999), Yntellektual'nye tekhnolohyy ydentyfykatsyy: nechetkye mnozhestva, henetycheskye alhorytmy, nejronnye sety [Intellectual Technology of Identification: fuzzy set, genetic algorithms, neural network], UNIVERSUM-Vinnitsa, Vinnitsa, Ukraine.

Стаття надійшла до редакції 17.08.2015 р.