СЕКЦІЯ 9
МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 330.46

Гриценко К.Г.
кандидат технічних наук, доцент,
доцент кафедри економічної кібернетики
Сумського державного університету

ВИКОРИСТАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН ДЛЯ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ БАНКІВСЬКОЇ УСТАНОВИ ВІД КІБЕРШАХРАЙСТВ[1]

USING THE THEORY OF FUZZY SETS FOR ASSESSING THE LEVEL OF BANK SECURITY FROM CYBER FRAUDS

АНОТАЦІЯ

Банківські установи є об'єктами критичної інфраструктури держави. Вони надзвичайно привабливі для злочинців. У зв'язку із цим обґрунтування вибору банківської установи для незалежного аудиту її кібербезпеки є актуальним завданням. Завдяки аудиту кібербезпеки можна сформулювати конкретні практичні рекомендації щодо поліпшення кібербезпеки. Інструментом попереджувального кіберзахисту є нечітка модель оцінки рівня захищеності банківської установи від кібершахрайств, що використовує як кількісні показники, так і якісні анкетні дані. Вона може бути використана для обґрунтування вибору банківської установи з метою проведення першочергового незалежного аудиту її кібербезпеки. Рівень захищеності банківської установи від кібершахрайств оцінюється з використанням деревоподібного зваженого графа.

Ключові слова: банківська установа, кібершахрайства, рівень захищеності, шкала оцінювання, нечіткі множини, нормалізація, ієрархічне дерево.

АННОТАЦИЯ

Банковские учреждения являются объектами критической инфраструктуры государства. Они очень привлекательны для кибермошенников. В связи с этим обоснование выбора банковского учреждения для независимого аудита его кибербезопасности является актуальной задачей. Благодаря аудиту кибербезопасности можно сформулировать конкретные практические рекомендации по улучшению кибербезопасности. Инструментом предупредительной киберзащиты является нечеткая модель оценки уровня защищенности банковского учреждения от кибермошенничества, использующая как количественные показатели, так и качественные анкетные данные. Она может быть использована для обоснования выбора банковского учреждения с целью проведения первоочередного независимого аудита его кибербезопасности. Уровень защищенности банковского учреждения от кибермошенничества оценивается с использованием древовидного взвешенного графа.

Ключевые слова: банковское учреждение, кибермошенничества, уровень защищенности, шкала оценивания, нечеткие множества, нормализация, иерархическое дерево.

ANNOTATION

All over the world, the fight against cyber frauds has recognized as a priority issue. In today's conditions, it is especially important to develop effective methods for preventing cyber frauds. As is well known, banking institutions are the objects of critical infrastructure of the state. They are extremely attractive for cybercriminals. The intellectual level of cyber-attacks and the complexity of fraudulent schemes are permanently increasing. In connection with this, the actual task is to justify the choice of a banking institution for an independent audit of its cyber security. Because of cyber security audit, specific practical recommendations for improving cybersecurity could be formulating. The fuzzy model of assessing the level of a bank security from cyber frauds is an instrument of warning cyber frauds. This model can use both quantitative indicators and qualitative data from questionnaires. Each questionnairy can contain the grading scale which has linguistic description in the form of fuzzy sets. Fuzzy sets of linguistic variable are described by trapezoidal membership functions. Linguistic analysis on this basis is non-contradictory. Thus fuzzy model could be using to justify the choice of a banking institution for conducting an urgent independent audit of its cyber security. The level of security of the banking institution from cyber frauds might be estimating using a tree-like weighed graph. In general, the quantitative values of the input factors have different dimensions. That is why the quantitative values of the input factors and the parameters of the trapezoidal membership functions of fuzzy sets should be normalized. For the input factors-incentives the procedure of natural normalization is used. For the input factors-disincentives the Savage's procedure of normalization is used. Normalized input factors is associated with corresponding normalized linguistic variables. For each vertex of a tree-like weighed graph an aggregation of normalized input factors should be performed. Values of the linguistic variables are being got as the result of aggregation. They are identified by fuzzy filtration operations.

Key words: banking institution, cyber frauds, security level, scale of assessment, fuzzy sets, normalization, hierarchical tree.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Банківські установи належать до об'єктів критичної інфраструктури держави. Вони є надзвичайно привабливими для кіберзлочинців через велику кількість грошових коштів, сконцентрованих на банківських рахунках, різноманітність електронних банківських послуг і велику кількість клієнтів банківських установ, що користуються цими послугами. Слід відзначити, що інтелектуальний рівень кібершахрайств і складність шахрайських схем постійно зростають. Особливо важливим є розроблення дієвих методів попе-

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».

реджувального, а не реагуючого кіберзахисту. Сьогодні в усьому світі протидія кіберзлочинності визнана пріоритетною проблемою, вирішення якої потребує проведення ґрунтовних наукових досліджень.

На державному рівні основним суб'єктом забезпечення кібербезпеки в банківському секторі є Національний банк України. Водночас на рівні бізнесу за кібербезпеку банківської установи відповідає її власник. Одним з ефективних засобів забезпечення функціонування національної системи кібербезпеки є аудит кібербезпеки об'єктів критичної інфраструктури держави. У зв'язку із цим актуальним науковим завданням, що має велике практичне значення, є обґрунтування вибору банківської установи для проведення першочергового незалежного аудиту її кібербезпеки, у результаті чого формулюються конкретні рекомендації щодо поліпшення кібербезпеки.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор. Кібербезпека визначається як стан захищеності окремих об'єктів держави, зокрема банківських установ, від ризику стороннього кібервпливу, за якого забезпечується їхній сталий розвиток, а також своєчасне виявлення, запобігання та нейтралізація реальних і потенційних викликів, кібернетичних утручань і загроз особистим, корпоративним і/або національним інтересам [1, с. 15]. Тематиці кібербезпеки присвячено велику кількість праць як вітчизняних, так і закордонних науковців.

У роботі [2] викладено основні аспекти та нормативне забезпечення формування системи кібербезпеки на державному рівні. Але невирішеними залишилися питання створення системи кібербезпеки на рівні бізнесу – в банківських установах, її взаємодії з національною системою фінансового моніторингу. У роботі [3] висвітлено зміст кібернетичної безпеки, її складники, форми, способи, методи, організаційні і технічні питання забезпечення кібербезпеки держави та підготовки фахівців, методологію організації та проведення навчань з кібербезпеки. Водночас не враховано специфіку банківської діяльності, що зменшує цінність цього дослідження саме для банківських установ. У роботі [4] досліджено основні загрози і механізми забезпечення безпеки банківських транзакцій у системах електронних платежів, основні вимоги стандарту Національного банку України до побудови системи управління кібербезпекою банківських установ. Водночас недослідженими залишилися питання надійності банківського персоналу. У роботі [5] розкрито сутність кібербезпеки та природу кіберзагроз, але не розкрито питання інтелектуалізації програмного забезпечення протидії кіберзлочинності, відсутні рекомендації для банківських установ. У роботі [6] наведено методологію оцінювання безпеки автоматизованої банківської системи України, яка дає змогу враховувати широкий спектр загроз кібербезпеки. Водночас не розкрите питання інтелектуалізації програмного забезпечення протидії кібершахрайствам.

Незважаючи на велику кількість наукових праць у сфері кібербезпеки, відсутні конкретні механізми та рекомендації щодо вдосконалення систем кібербезпеки банківських установ.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. До дієвих методів попереджувального кіберзахисту банківської установи належить незалежний аудит її системи кібербезпеки. Суб'єкт забезпечення кібербезпеки в банківському секторі може зробити обґрунтований вибір цільової банківської установи для проведення першочергового аудиту кібербезпеки на основі оцінки рівня захищеності банківської установи від кібершахрайств, яка враховує як кількісні, так і якісні показники. Науково-методичні засади такої оцінки поки ще не розроблені.

Формулювання цілей статті (постановка завдання). Метою статті є розвиток методичного інструментарію боротьби з кіберзлочинами в банківській сфері на основі теорії нечітких множин, зокрема розроблення нечітко-множинної моделі оцінки рівня захищеності банку від кібершахрайств, що може використовувати як кількісні показники, так і якісні анкетні дані.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Модель оцінки рівня захищеності банківської установи від кібершахрайств може бути представлена у вигляді деревоподібного зваженого графа (рис. 1), що описує ієрархічну структуру чинників, які впливають на рівень захищеності банківської установи.

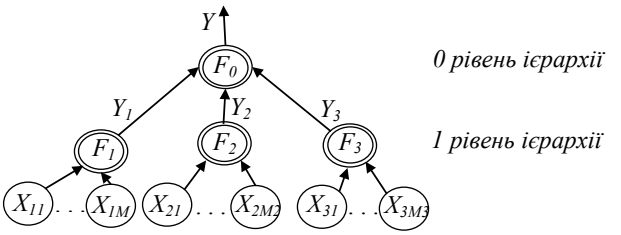

Рис. 1. Ієрархічна структура моделі

Спочатку в результаті агрегування вхідних факторів (X_{ij}) визначаються оцінки рівня захищеності банківської установи від кібершахрайств у розрізі таких критеріїв [7, с. 30]: захищеність інформаційно-телекомунікаційної системи банківської установи (Y_1), надійність персоналу банківської установи (Y_2), якість інформації для прийняття рішень (Y_3). Потім визначається рівень захищеності банківської установи у цілому. Елементи графа інтерпретуються так: Y – загальний рівень захищеності банківської установи від кібершахрайств; дуги, що виходять із вершин F_i, – вищезазначені критерії; X_{ij} – вхідні фактори, $i = \overline{1,n}; n = 3; j = \overline{1, M_i}$,

де n – кількість критеріїв, M_i – кількість факторів, що пов'язані з i-тим критерієм через вершину F_i, $i = \overline{1,3}$.

На нашу думку, до чинників, що визначають захищеність інформаційно-телекомунікаційної системи банківської установи, належать:

– якість систем життєзабезпечення даних департаментів банківської установи;

– якість технологічних процесів передачі, одержання, використання, розповсюдження і зберігання інформації;

– якість засобів забезпечення технічного захисту інформації;

– якість засобів забезпечення діяльності банківської установи, які мають вихід за межі контрольованої території;

– якість експлуатаційної документації, яка забезпечує інформаційну діяльність.

До чинників, що визначають надійність персоналу банківської установи, належать:

– плинність працівників банківської установи;

– готовність працівників банківської установи до нововведень;

– підготовленість персоналу банківської установи до розпізнавання шахрайств;

– досвід роботи працівників банківської установи;

– компетентність працівників банківської установи;

– мотивація працівників банківської установи.

До чинників, що визначають якість інформації для прийняття рішень, належать:

– якість політики класифікації інформаційних активів;

– якість політики безпеки персоналу;

– якість політики захисту від шкідливого та мобільного коду;

– якість політики використання корпоративної електронної пошти;

– якість політики управління інцидентами кібербезпеки.

Оцінки наведених вище вхідних чинників визначаються шляхом усереднення анкетних даних, тому анкети повинні містити кількісну (бальну) шкалу оцінювання. Можливі варіанти таких шкал наведено у [8, с. 1]. Наприклад, у класичній голландській системі оцінювання оцінки факторів знаходяться в межах від 0 до 10: 1–4 – низька оцінка; 5–7 – середня оцінка; 8–10 – висока оцінка.

Вибрана кількісна шкала оцінювання зіставляється з її лінгвістичним описом (нечіткою терм-множиною), як це показано, наприклад, у [9, с. 51]. Приклад зіставлення кількісної шкали оцінювання U з нечіткою терм-множиною наведено в табл. 1.

Трапецієподібні функції належності нечіткої терм-множини лінгвістичної змінної L, представленої в табл. 1, наведено на рис. 2.

Абсциси нейтральних точок на 01-носії рис. 2 мають координати (0.2, 0.4, 0.6, 0.8). Наведена на рис. 2 шкала оцінювання, побудована на основі трапецієподібних функцій належності нечітких термів, є «сірою» шкалою Поспєлова, і лінгвістичний аналіз на її основі є несуперечливим. Перевагою такого опису є його задоволення вимогам «сірої» шкали Поспєлова: наявність нейтральної точки посеред інтервалу невизначеності і монотонне спадання експертної впевненості в класифікації у міру зростання X.

Рівень захищеності банківської установи від кібершахрайств опишемо нечіткою ієрархічною моделлю:

$$Y=<G, L, F>, \qquad (1)$$

Таблиця 1

Шкала оцінювання

U	0,1	0,3	0,5	0,7	0,9
Нечіткий терм T лінгвістичної змінної L	Низький	Нижче середнього	Середній	Вище середнього	Високий

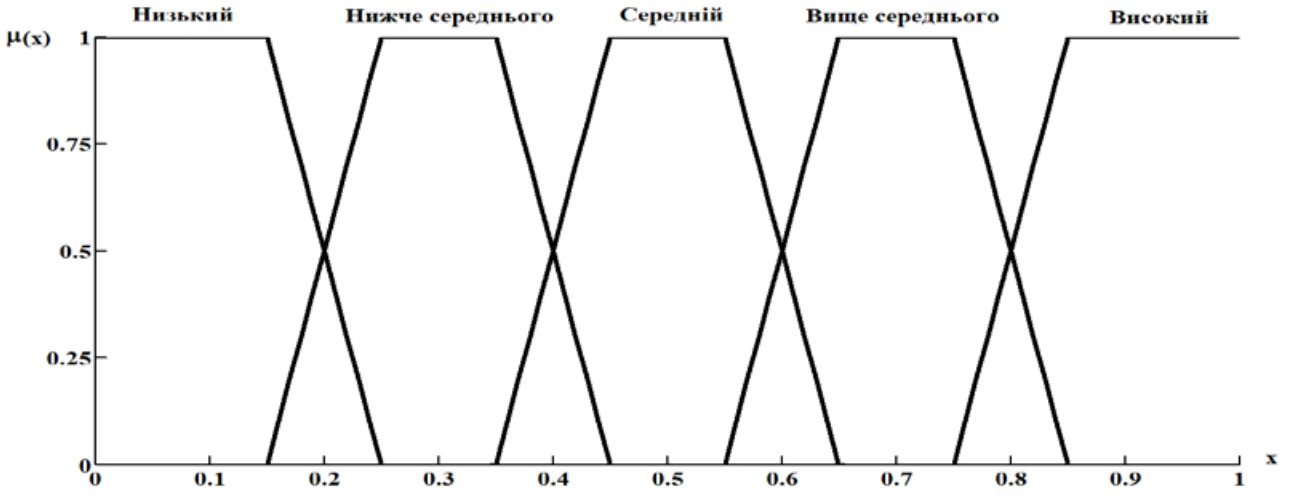

Рис. 2. Нечітка терм-множина лінгвістичної змінної *L*

де G – зважений ієрархічний граф, показаний на рис. 1; L – терм-множина нечітких оцінок вхідних факторів X_{ij}; F – функція згортки нечітких оцінок у відповідних вершинах графа (F_i). Ваги дуг графа відповідають ступеню впливу відповідних чинників на результуючу оцінку.

Рівень захищеності банківської установи від кібершахрайств у цілому представимо у вигляді лінгвістичної змінної $L^{(Y)}$ з множиною можливих значень (терм-множиною):

$$L^{(Y)} = \left\{ T_1^{(Y)}, \ ..., T_k^{(Y)}, ..., T_s^{(Y)} \right\}, \qquad (2)$$

де s – кількість нечітких термів лінгвістичної змінної $L^{(Y)}$.

Рівень захищеності банківської установи від кібершахрайств у розрізі окремих критеріїв Y_i ($i = \overline{1,3}$) представимо у вигляді лінгвістичних змінних $L^{(i)}$ з множиною можливих значень:

$$L^{(i)} = \left\{ T_1^{(i)}, ..., T_k^{(i)}, ..., T_s^{(i)} \right\}, \qquad (3)$$

де s – кількість нечітких термів лінгвістичної змінної $L^{(i)}$, $i = \overline{1,3}$.

Кожен вхідний фактор X_{ij} також представимо у вигляді лінгвістичної змінної з множиною можливих значень:

$$L^{(ij)} = \left\{ T_1^{(ij)}, ..., T_k^{(ij)}, ..., T_s^{(ij)} \right\}, \ i = \overline{1,3}; \quad j = \overline{1, M_i}, \qquad (4)$$

де s – кількість нечітких термів лінгвістичної змінної $L^{(ij)}$.

Для спрощення моделі (1)–(4) сформуємо одну терм-множину для всіх лінгвістичних змінних $L^{(Y)}$, $L^{(i)}$, $L^{(ij)}$:

$T_1^{(Y)}, T_1^{(i)}, T_1^{(ij)}$ – «низький рівень»;

$T_2^{(Y)}, T_2^{(i)}, T_2^{(ij)}$ – «середній рівень»;

$T_3^{(Y)}, T_3^{(i)}, T_3^{(ij)}$ – «високий рівень».

Кожному нечіткому терму («низький» (k=1), «середній» (k=2), «високий» (k=3)) лінгвістичної змінної $L^{(ij)}$ поставимо у відповідність трапецієподібну функцію належності μk(Xij) з параметрами $\underline{t_k^{(ij)}}; \overline{t_k^{(ij)}}; a_k^{(ij)}; b_k^{(ij)}$ ($k = \overline{1,3}$):

$$\mu_k\left(X_{ij}\right) = \begin{cases} 0, \text{ якщо } X_{ij} \le \underline{t_k^{(ij)}} - a_k^{(ij)} \text{ або } X_{ij} \ge \overline{t_k^{(ij)}} + b_k^{(ij)} \\ \dfrac{X_{ij} - \left(\underline{t_k^{(ij)}} - a_k^{(ij)}\right)}{a_k^{(ij)}}, \quad \text{якщо} \quad \underline{t_k^{(ij)}} - a_k^{(ij)} \le X_{ij} \le \underline{t_k^{(ij)}} \\ 1, \quad \text{якщо} \quad \underline{t_k^{(ij)}} \le \overline{t_k^{(ij)}} \\ \dfrac{\left(\overline{t_k^{(ij)}} + b_k^{(ij)}\right) - X_{ij}}{b_k^{(ij)}}, \text{ якщо} \quad \overline{t_k^{(ij)}} \le X_{ij} \le \overline{t_k^{(ij)}} + b_k^{(ij)} \end{cases} \qquad (5)$$

Нечітка терм-множина лінгвістичної змінної $L^{(ij)}$ наведена на рис. 3.

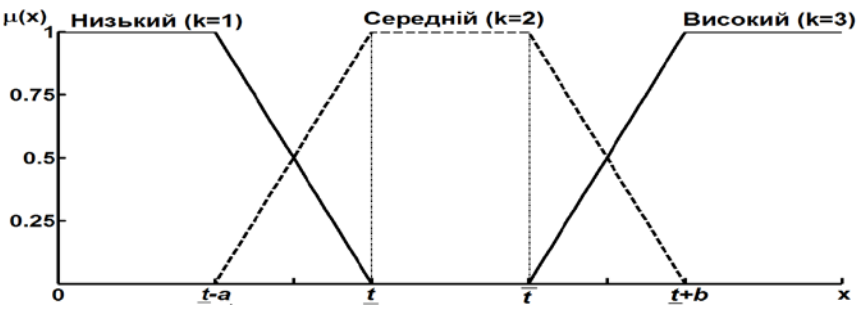

Рис. 3. Нечітка терм-множина лінгвістичної змінної $L^{(ij)}$

У загальному випадку кількісні значення вхідних факторів Xij (вісь абсцис на рис. 3) можуть мати різну розмірність. Їх можна агрегувати лише за умови нормування. Тобто необхідно привести параметри $\underline{t_k^{(ij)}}; \overline{t_k^{(ij)}}; a_k^{(ij)}; b_k^{(ij)}$ ($k = \overline{1,s}$) трапецієподібних функцій належності нечітких термів лінгвістичної змінної $L^{(ij)}$до інтервалу [0,1], як це показано, наприклад, на рис. 2.

Якщо вхідні фактори X_{ij} є стимуляторами, тобто їх зростання поліпшує значення агрегованого показника, то можна використати таку процедуру природньої нормалізації для $L^{(ij)} = \left\{ T_1^{(ij)}, \ ..., T_k^{(ij)}, ..., T_s^{(ij)} \right\}$:

$$\underline{t_{norm\,k}^{(ij)}} = \frac{\underline{t_k^{(ij)}} - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)},$$

$$\overline{t_{norm\,k}^{(ij)}} = \frac{\overline{t_k^{(ij)}} - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \qquad (6)$$

$$a_{norm}^{(ij)} = \frac{a_k^{(ij)}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)},$$

$$b_{norm\,k}^{(ij)} = \frac{b_k^{(ij)}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}.$$

Якщо вхідні фактори X_{ij} є дестимуляторами, тобто їх зростання погіршує значення агрегованого показника, то можна використати таку процедуру нормалізації Севіджа:

$$\underline{t_{norm\,k}^{(ij)}} = \frac{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \underline{t_k^{(ij)}}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)},$$

$$\overline{t_{norm\,k}^{(ij)}} = \frac{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \overline{t_k^{(ij)}}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \qquad (7)$$

$$a_{norm}^{(ij)} = \frac{a_k^{(ij)}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)},$$

$$b_{norm\,k}^{(ij)} = \frac{b_k^{(ij)}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}.$$

У результаті лінгвістична змінна $L^{(ij)} = \left\{ T_1^{(ij)}, \ ..., T_k^{(ij)}, ..., T_s^{(ij)} \right\}$ набуває нормованого вигляду $L_{norm}^{(ij)} = \left\{ T_{norm\,1}^{(ij)}, ..., T_{norm\,k}^{(ij)}, ..., T_{norm\,s}^{(ij)} \right\}$. Для кількісних значень самих вхідних факторів X_{ij} теж виконується процедура природньої нормалізації або нормалізації Севіджа.

Для того щоб оцінити рівень захищеності банківської установи від кібершахрайств із ви-

користанням ієрархічної структури, представленої на рис. 1, необхідно для кожного рівня ієрархії провести агрегування значень лінгвістичних змінних із пересуванням за напрямом дуг ієрархічного графа від нижніх рівнів ієрархії до верхніх.

У кожній вершині графа Fi ($i = \overline{1,3}$) виконується згортка значень, пов'язаних із нею нормованих вхідних факторів Xij, представлених відповідними нормованими лінгвістичними змінними $L^{(ij)}$– нечіткими термами $T_k^{(ij)}$, $j = \overline{1, M_i}$, $k = \overline{1,s}$.

Як функцію згортки використаємо OWA-оператор Ягера (OWA – Ordered Weighted Averaging):

$$L_{norm}^{(i)} = \sum_{j=1}^{M_i}\left(L_{norm}^{(ij)} \times \omega^{(ij)}\right) = \sum_{j=1}^{M_i}\left(\left\{T_{norm\,1}^{(ij)}, ..., T_{norm\,k}^{(ij)}, ..., T_{norm\,s}^{(ij)}\right\} \times \omega^{(ij)}\right) =$$

$$= \sum_{j=1}^{M_i}\left\{T_{norm\,1}^{(ij)} \times \omega^{(ij)}, ..., T_{norm\,k}^{(ij)} \times \omega^{(ij)}, ...T_{norm\,s}^{(ij)} \times \omega^{(ij)}\right\}, \quad (8)$$

де $\omega^{(ij)}$ – рівень значущості вхідного фактору X_{ij}, що через вершину F_i (функцію згортки) пов'язаний із критерієм Y_i. $\omega^{(ij)}$ описується трапецієподібною функцією належності з параметрами $\underline{t^{(ij)}}; \overline{t^{(ij)}}; 0; 0$, де ваговий коефіцієнт $\underline{t^{(ij)}} = \overline{t^{(ij)}} = k_{ij}$. У результаті отримуємо нечітку оцінку рівня захищеності банківської установи від кібершахрайств у розрізі критерію Y_i.

Оскільки функції належності нечітких термів лінгвістичних змінних $L_{norm}^{(ij)} = \left\{T_{norm\,1}^{(ij)}, ..., T_{norm\,k}^{(ij)}, ..., T_{norm\,s}^{(ij)}\right\}$ мають трапецієподібну форму, то і терми лінгвістичної змінної $L_{norm}^{(i)}$ теж мають трапецієподібну форму.

Для визначення рівня захищеності банківської установи від кібершахрайств у цілому виконуємо згортку отриманих вище нечітких оцінок $L_{norm}^{(i)}$:

$$L_{norm}^{(Y)} = \sum_{i=1}^{3}\left(L_{norm}^{(i)} \times \omega^{(i)}\right), \quad (9)$$

де $\omega^{(i)}$ – рівень значущості критерію Y_i, що через вершину F_0 (функцію згортки) пов'язаний із рівнем захищеності банківської установи від кібершахрайств в цілому Y. $\omega^{(i)}$ описується трапецієподібною функцією належності з параметрами $\underline{t^{(i)}}; \overline{t^{(i)}}; 0; 0$, де ваговий коефіцієнт $\underline{t^{(i)}} = \overline{t^{(i)}} = k_i$. У результаті отримуємо нечітку оцінку рівня захищеності банківської установи від кібершахрайств у цілому.

Вагові коефіцієнти k_{ij} та k_i у функціях згортки (8)–(9) вершин ієрархічного дерева пропонується розраховувати за схемою Фішберна [10, с. 207], яка використовується за умови, що відомі відношення пріоритетності між критеріями. Визначення величини вагових коефіцієнтів за схемою Фішберна відповідає максимуму ентропії наявної інформаційної невизначеності щодо вагових коефіцієнтів.

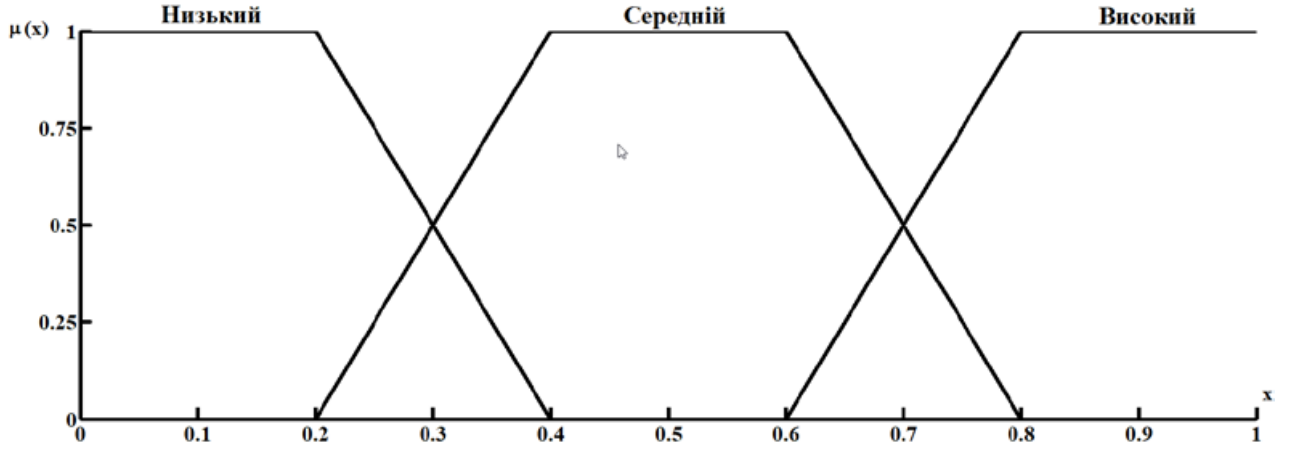

Рис. 4. Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(i)}$

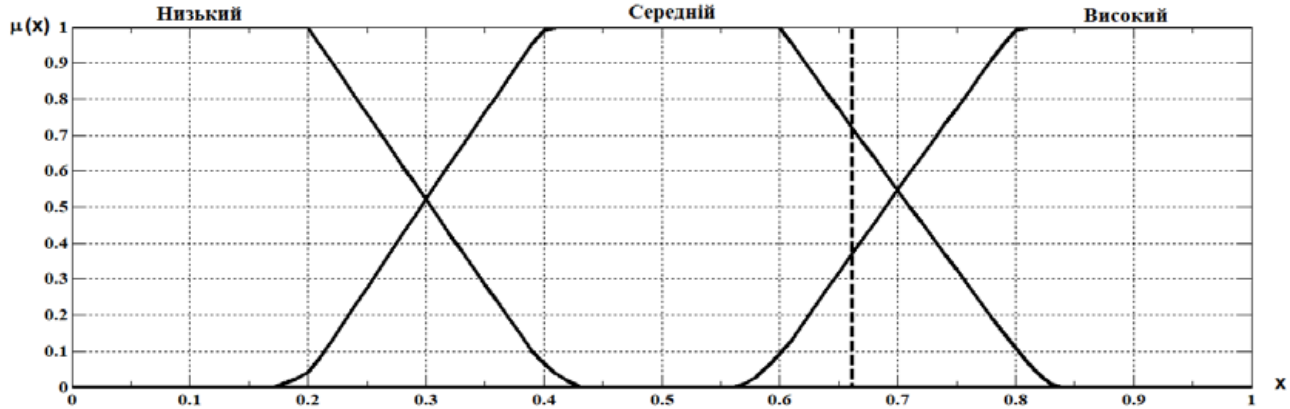

Рис. 5. Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(Y)}$

Отримані в результаті згортки значення лінгвістичних змінних у вигляді терм-множини (див. рис. 3) розпізнаються за допомогою операцій нечіткої фільтрації за показником можливості [11, с. 15].

Нехай для досліджуваної банківської установи нечіткі терм-множини нормованих лінгвістичних змінних критеріїв $L_{norm}^{(i)}$ мають вигляд, поданий на рис. 4.

Абсциси нейтральних точок на 01-носії рис. 4 мають координати (0.3, 0.7).

Нехай нормоване значення критерію захищеності інформаційно-телекомунікаційної системи банківської установи $L_{norm}^{(1)} = 0{,}5$; критерію надійності персоналу банківської установи $L_{norm}^{(2)} = 0{,}9$; критерію якості інформації для прийняття рішень $L_{norm}^{(3)} = 0{,}7$.

Виконаємо згортку критеріїв $L_{norm}^{(i)}$ у комплексний показник $L_{norm}^{(Y)}$ із рівнями значущості $k_1 = 0,5;\ k_2 = 0,3;\ k_3 = 0,2$. Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(Y)}$ наведена на рис. 5.

Нормоване значення комплексного показника дорівнює 0,66. Таким чином, із достовірністю 0,7 оцінка рівня захищеності банківської установи від кібершахрайств знаходиться в інтервалі середніх значень та є задовільною.

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку. Використання розробленої нечітко-множинної моделі оцінки рівня захищеності банківської установи від кібершахрайств, що використовує як кількісні показники, так і якісні анкетні дані, значно спрощує вибір банківської установи для проведення повноцінного незалежного аудиту кібербезпеки. Це дає змогу реалізувати дієвий попереджувальний кіберзахист.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В.Л. Бурячок та ін. ; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. Київ : ДУТ, 2015. 288 с.
2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.
3. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки : монографія ; за ред. Ю.Г. Даник. Житомир : ЖНАЕУ, 2016. 636 с.
4. Король О.Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку України. *Системи обробки інформації.* 2015. Вип. 9(134). С. 88–95.
5. Jeremy Swinfen Green. Cyber Security: An Introduction For Non-Technical Managers. Gover. 2015. 246 p.
6. Євсєєв С.П. Методологія оцінювання безпеки інформаційних технологій автоматизованих банківських систем України. *Безпека інформації. Ukrainian Scientific Journal of Information Security.* 2016. Т. 22. № 3. С. 297–309.
7. Велігура А.В. Оцінювання стану інформаційної безпеки підприємства. *Управління проектами та розвиток виробництва.* 2014. № 4(52). С. 28–39.
8. Grading systems in the Netherlands, the United States and the United Kingdom. URL: https://people.eecs.berkeley.edu/~marten/pdf/gradingsystems.pdf (Last accessed: 30.01.2019).
9. Бутенко Л.М., Лозовик Ю.М. Аналітичні моделі швидкої діагностики підприємства та механізми їх забезпечення. *Економіка та держава.* 2010. № 4. С. 50–54.
10. Мірських Г.О., Реутська Ю.Ю. Комбіновані методи визначення вагових коефіцієнтів в задачах оптимізації та оцінювання якості об'єктів. *Вісник Національного технічного університету України «КПІ». Серія «Радіотехніка. Радіоапаратобудування».* 2011. № 47. С. 199–211.
11. Бирський В.В. Оцінювання стану економічної системи методами теорії нечітких множин. *Держава та регіони.* 2010. № 4. С. 11–15.

REFERENCES:

1. Buriachok V.L., Tolubko V.B., Khoroshko V.O., Toliupa S.V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk.* Kyiv : DUT. 2015. (in Ukrainian)
2. Buriachok V.L. (2013). *Osnovy formuvannia derzhavnoi systemy kibernetychnoi bezpeky : monohrafiia.* Kyiv : NAU. (in Ukrainian)
3. Hryshchuk R.V., Danyk Yu.H. (2016). *Osnovy kibernetychnoi bezpeky : monohrafiia.* Zhytomyr : ZhNAEU. (in Ukrainian)
4. Korol O.H. (2015). Analiz zahroz i mekhanizmiv zabezpechennia bezpeky informatsii v systemi elektronnykh platezhiv komertsiinoho banku Ukrainy. *Systemy obrobky informatsii*, vol. 9(134), pp. 88–95.
5. Jeremy Swinfen Green (2015). *Cyber Security: An Introduction For Non-Technical Managers.* Gover.
6. Evseev S.P. (2016). Metodolohiia otsiniuvannia bezpeky informatsiinykh tekhnolohii avtomatyzovanykh bankivskykh system Ukrainy. *Bezpeka informatsii. Ukrainian Scientific Journal of Information Security*, vol. 22, no. 3, pp. 297–309.
7. Velihura A.V. (2014). Otsiniuvannia stanu informatsiinoi bezpeky pidpryiemstva. *Upravlinnia proektamy ta rozvytok vyrobnytstva : zbirnyk naukovykh prats.* Luhansk : vyd-vo SNU im. V. Dalia, no. 4(52), pp. 28–39.
8. Grading systems in the Netherlands, the United States and the United Kingdom. Available at: https://people.eecs.berkeley.edu/~marten/pdf/gradingsystems.pdf (accessed 31 January 2019).
9. Butenko L.M., Lozovyk Yu.M. (2010). Analitychni modeli shvydkoi diahnostyky pidpryiemstva ta mekhanizmy yikh zabezpechennia. *Ekonomika ta derzhava*, no. 4, pp. 50–54.
10. Mirskykh H.O., Reutska Yu.Yu. (2011). Kombinovani metody vyznachennia vahovykh koefitsiientiv v zadachakh optymizatsii ta otsiniuvannia yakosti obiektiv. *Visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy «KPI». Seriia «Radiotekhnika. Radioaparatobuduvannia»*, no. 47, pp. 199–211.
11. Byrskyi V.V. (2010). Otsiniuvannia stanu ekonomichnoi systemy metodamy teorii nechitkykh mnozhyn. *Derzhava ta rehiony,* no. 4, pp. 11–15.