Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»

СУЧАСНІ ІНСТРУМЕНТИ БОРОТЬБИ З КІБЕРШАХРАЙСТВАМИ У БАНКАХ

Монографія

За загальною редакцією О. В. Кузьменко, Г. М. Яровенко

Рекомендовано вченою радою Сумського державного університету

Суми
Видавництво "Ярославна"
2018

УДК 303.09:336.717.1

Авторський колектив:
О. В. Кузьменко, доктор економічних наук;
Г. М. Яровенко, кандидат економічних наук;
С. В. Лєонов, доктор економічних наук;
О. А. Криклій, кандидат економічних наук;
К. Г. Гриценко, кандидат технічних наук;
О.О. Пушко, кандидат економічних наук;
Я. В. Самусевич, кандидат економічних наук;
Т. В. Доценко, аспірант кафедри економічної кібернетики;
М. М. Бояджян, магістр економічної кібернетики;
В. О. Ковач, магістр економічної кібернетики;
С.В. Клімов, магістр економічної кібернетики.

Рецензенти:
І. О. Школьник – доктор економічних наук, професор, завідувач кафедри фінансів, банківської справи та страхування Науково-навчального інституту бізнес-технологій «УАБС» Сумського державного університету (м. Суми);
П. М. Григорук – доктор економічних наук, професор, завідувач кафедри автоматизованих систем і моделювання в економіці Хмельницького національного університету (м. Хмельницький);
О. В. Лебідь – кандидат економічних наук, доцент, професор кафедри банківської справи і фінансових послуг Харківського національного економічного університету ім. С. Кузнеця (м. Харків).

Рекомендовано до видання вченою радою
Сумського державного університету як
монографія (протокол № 6 від 15.11. 2018 року)

Сучасні інструменти боротьби з кібершахрайствами у банках : Монографія / О. В. Кузьменко, Г.М. Яровенко, С. В. Лєонов та ін. ; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. – Суми: видавництво "Ярославна", 2018. – 144 с.
ISBN 978-966-7538-52-1

Монографія складається із чотирьох частин. У першій частині «Концептуальні основи мінімізації операційних банківських ризиків в сфері інформаційної безпеки» викладено науково-методичний підхід до операційних ризиків, як складової інформаційної безпеки, з боку його моделювання та стандартизації. У другій частині «Аналіз та оцінка наслідків кібершахрайств у банках» зосереджено увагу на оцінці впливу макроекономічних факторів на формування схильності до шахрайства, моделювання збитків банків від їх залучення до шахрайських операцій. Третя частина «Математичне моделювання як інструмент попередження кібершахрайств у банках» базується на застосуванні інтелектуального аналізу, нечітких множин та динамічного моделювання для попередження кібершахрайств. У четвертій частині «Розробка комплексу автоматизованих превентивних заходів попередження шахрайств» наведено інформаційну модель та прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками.

Монографія призначена для студентів і викладачів вищих навчальних закладів, аналітиків, фахівців кібербезпеки банків.

УДК 303.09:336.717.1

ISBN 978-966-7538-52-1

ЗМІСТ

Застосування отриманої моделі на практиці допоможе працівникам банківського сектору виявляти в транзакціях ознаки кібернетичних загроз, тим самим попереджаючи користувачів мобільного та інтернет-банкінгу від можливих збитків, завданих злочинними діями. Інтеграція моделі в існуючу систему кіберзахисту банку дозволить проводити регулярний моніторинг транзакцій на предмет наявності ознак кіберзагроз, сприятиме підвищенню рівня довіри клієнтів до банків через підвищення захищеності та надійності.

3.3 Нечітко-множинна модель оцінки рівня захищеності банку від кібершахрайств

Кібербезпека визначається як стан захищеності окремих об'єктів держави, зокрема банківських установ, від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтролізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [72]. Актуальною задачею, що характеризується вираженою практичною спрямованістю, є вибір банківської установи (наприклад, відділення банку) для проведення аудиту її системи кібербезпеки, в результаті якого формулюються конкретні пропозиції по покращенню існуючої системи кібербезпеки. Для вирішення цієї задачі нами розроблена нечітко-множинна модель оцінки рівня захищеності банку від кібершахрайств, яка може працювати як з кількісними показниками, так і з анкетними даними. Використання цієї моделі значно спрощує процес вибору банківської установи для проведення повноцінного аудиту системи кібербезпеки.

Модель оцінки рівня захищеності банку від кібершахрайств може бути представлена у вигляді деревоподібного зваженого графа (рис.3.11), що описує ієрархічну структуру факторів, які впливають на рівень захищеності банку.

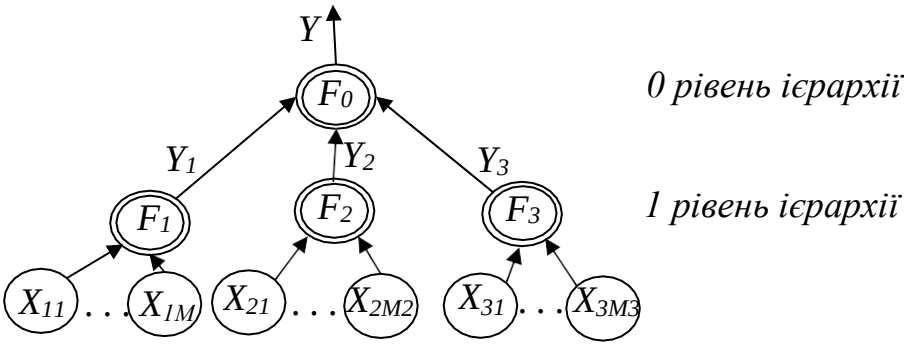

Рисунок 3.11 – Ієрархічна структура моделі

Спочатку в результаті агрегування вхідних факторів (X_{ij}) визначаються оцінки рівня захищеності банку від кібершахрайств в розрізі наступних критеріїв [73]: захищеність інформаційно-телекомунікаційної системи банку (Y_1), надійність персоналу банку (Y_2), якість інформації для прийняття рішень (Y_3). Потім визначається рівень захищеності банку в цілому. Елементи графа інтерпретуються наступним чином: Y – загальний рівень захищеності банку 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 факторів, що визначають захищеність інформаційно-телекомунікаційної системи банку, відносяться:

– якість систем життєзабезпечення даних департаментів банку;

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

– якість засобів забезпечення технічного захисту інформації;

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

– якість експлуатаційної документації, яка забезпечує інформаційну діяльність.

До факторів, що визначають надійність персоналу банку, відносяться:

– плинність працівників банку;

– готовність працівників банку до нововведень;

– підготовленість персоналу банку до розпізнавання шахрайств;

– досвід роботи працівників банку;

– компетентність працівників банку;

– мотивація працівників банку.

До факторів, що визначають якість інформації для прийняття рішень, відносяться:

– 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 інформаційної безпеки.

Оцінки зазначених вище вхідних факторів визначаються шляхом усереднення анкетних даних, тому анкети повинні містити кількісну (бальну) шкалу оцінювання. Можливі варіанти таких шкал наведені в [74]. Наприклад, в класичній голандській системі оцінювання оцінки факторів знаходяться в межах від 0 до 10: 1-4 – низька оцінка; 5-7 – середня оцінка; 8-10 – висока оцінка.

Обрана кількісна шкала оцінювання зіставляється з її лінгвістичним описом (нечіткою терм-множиною), як це показано, наприклад, в [75]. Приклад зіставлення кількісної шкали оцінювання U з нечіткою терм-множиною наведений в табл. 3.3.

Таблиця 3.3 – Шкала оцінювання

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

Трапецієподібні функції належності нечіткої терм-множини лінгвістичної змінної L, представленої в таблиці 3.3, наведені на рисунку 3.12.

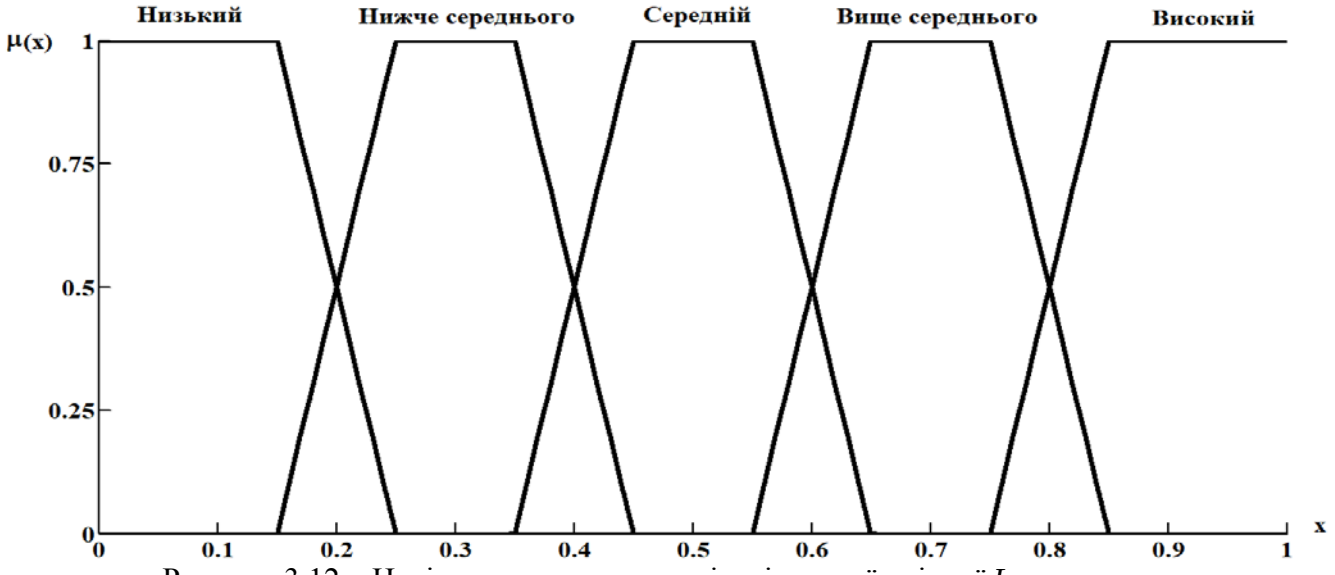

Рисунок 3.12 – Нечітка терм-множина лінгвістичної змінної L

Абсциси нейтральних точок на 01-носії (рис. 3.12) мають координати (0.2, 0.4, 0.6, 0.8). Наведена на рисунку 3.12 шкала оцінювання на трапецієподібних функціях належності нечітких термів є «сірою» шкалою Поспєлова, і лінгвістичний аналіз на її основі є несуперечливим. Наприклад, інтервал [0.15, 0.25] – це зона невизначеності в оцінці, яка може бути описана похилим ребром трапецієподібного нечіткого числа. Перевагою такого опису є його задоволення вимогам «сірої» шкали Поспєлова: наявність нейтральної точки посеред інтервалу невизначеності і монотонне спадання експертної впевненості в класифікації по мірі зростання *X*. Таким вимогам задовольняють не тільки трапецієподібні нечіткі числа. Однак вони відображають факт, що якщо немає ніяких додаткових міркувань про характер убування експертної впевненості, то лінійний вид відповідної функції належності є найбільш раціональним.

Рівень захищеності банку від кібершахрайств опишемо нечіткою ієрархічною моделлю:

$$Y=<G, L, F>, \tag{3.5}$$

де *G* – зважений ієрархічний граф, показаний на рисунку 3.11; *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 банку від кібершахрайств у цілому представимо у вигляді лінгвістичної змінної $L^{(Y)}$ з множиною можливих значень (терм-множиною):

$$L^{(Y)} = \left\{ T_1^{(Y)}, \ ...,T_k^{(Y)},...,T_s^{(Y)} \right\}, \tag{3.6}$$

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

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

$$L^{(i)} = \left\{ T_1^{(i)},...,T_k^{(i)},...,T_s^{(i)} \right\}, \tag{3.7}$$

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:

$$L^{(ij)} = \left\{ T_1^{(ij)},...,T_k^{(ij)},...,T_s^{(ij)} \right\}, \ i = \overline{1,3}; \quad j = \overline{1,M_i}, \tag{3.8}$$

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

З метою 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 $\mu_k(X_{ij})$ з параметрами $\underline{t_k^{(ij)}};\overline{t_k^{(ij)}};a_k^{(ij)};b_k^{(ij)}$ ($k=\overline{1,3}$):

$$\mu_k\left(X_{ij}\right)=\begin{cases} 0, \textit{якщо } X_{ij} \le \underline{t_k^{(ij)}} - a_k^{(ij)} \textit{ або } X_{ij} \ge \overline{t_k^{(ij)}} + b_k^{(ij)} \\ \dfrac{X_{ij} - \left(\underline{t_k^{(ij)}} - a_k^{(ij)}\right)}{a_k^{(ij)}}, \quad \textit{якщо} \quad \underline{t_k^{(ij)}} - a_k^{(ij)} \le X_{ij} \le \underline{t_k^{(ij)}} \\ 1, \quad \textit{якщо} \quad \underline{t_k^{(ij)}} \le \overline{t_k^{(ij)}} \\ \dfrac{\left(\overline{t_k^{(ij)}} + b_k^{(ij)}\right) - X_{ij}}{b_k^{(ij)}}, \textit{якщо} \quad \overline{t_k^{(ij)}} \le X_{ij} \le \overline{t_k^{(ij)}} + b_k^{(ij)} \end{cases} \tag{3.9}$$

Нечітка терм-множина лінгвістичної змінної $L^{(ij)}$ наведена на рисунку 3.13.

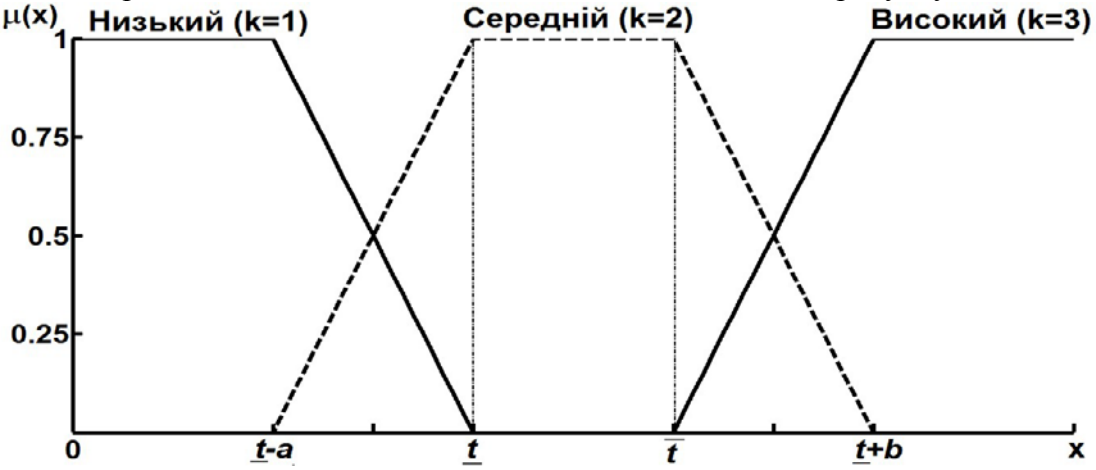

Рисунок 3.13 – Нечітка терм-множина лінгвістичної змінної $L^{(ij)}$

У загальному випадку кількісні значення вхідних факторів X_{ij} (вісь абсцис на рисунку 3.13) 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. 3.12.

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

$$t_{\underline{norm\,k}}^{(ij)} = \frac{\underline{t_k^{(ij)}} - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}{\left(\overline{t^{(ij)}} + b^{(ij)}\right) - \left(\underline{t^{(ij)}} - a^{(ij)}\right)},\ \overline{t_{norm\,k}^{(ij)}} = \frac{\overline{t_k^{(ij)}} - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \tag{3.10}$$

$$a_{norm}^{(ij)} = \frac{\underline{k}}{\underline{a}^{(ij)}}, b_{norm\,k} = \frac{\underline{k}}{b^{(ij)}}. \quad \underline{\quad} \qquad \underline{\quad}$$

$$\left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right) \qquad \left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right)$$

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

$$\underline{t}_{norm\,k}^{(ij)} = \frac{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \underline{t_k^{(ij)}}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \overline{t}_{norm\,k}^{(ij)} = \frac{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \overline{t_k^{(ij)}}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \quad (3.11)$$

$$a_{norm}^{(ij)} = \frac{\underline{k}}{\underline{a}^{(ij)}}, b_{norm\,k} = \frac{\underline{k}}{b^{(ij)}}. \quad \underline{\quad} \qquad \underline{\quad}$$

$$\left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right) \qquad \left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right)$$

В результаті лінгвістична змінна $L^{(ij)} = \left\{ T_1^{(ij)}, \ldots, T_k^{(ij)}, \ldots, T_s^{(ij)} \right\}$ набуває нормованого вигляду $L_{norm}^{(ij)} = \left\{ T_{norm1}^{(ij)}, \ldots, T_{norm\,k}^{(ij)}, \ldots, T_{norm\,s}^{(ij)} \right\}$. Для кількісних значень самих вхідних факторів X_{ij} теж виконується процедура природньої нормалізації або нормалізації Севіджа.

Для того, щоб оцінити рівень захищеності банку від кібершахрайств з використанням ієрархічної структури, представленої на рисунку 3.11, необхідно для кожного рівня ієрархії провести агрегування значень лінгвістичних змінних з пересуванням за напрямом дуг ієрархічного графа від нижніх рівнів ієрархії до верхніх.

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

В якості функції згортки використовуємо OWA-оператор Ягера (OWA – Ordered Weighted Averaging):

$$L_{norm}^{(i)} = \sum_{j=1}^{M_i} \left(L_{norm}^{(ij)} \times \omega^{(ij)} \right) = \sum_{j=1}^{M_i} \left(\left\{ T_{norm1}^{(ij)}, \ldots, T_{norm\,k}^{(ij)}, \ldots, T_{norm\,s}^{(ij)} \right\} \times \omega^{(ij)} \right) =$$

$$= \sum_{j=1} \left\{ T_{norm\,1}^{(ij)} \times \omega^{(ij)}, \ldots, T_{norm\,k}^{(ij)} \times \omega^{(ij)}, \ldots T_{norm\,s}^{(ij)} \times \omega^{(ij)} \right\}, \quad (3.12)$$

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

Оскільки функції належності нечітких термів лінгвістичних змінних $L_{norm}^{(ij)} = \left\{ T_{norm1}^{(ij)}, \ldots, T_{norm\,k}^{(ij)}, \ldots, T_{norm\,s}^{(ij)} \right\}$ мають трапецієподібну форму, то і терми лінгвістичної змінної $L_{norm}^{(i)}$ теж мають трапецієподібну форму.

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

$$L_{norm}^{(Y)} = \sum_{i=1}^{3} \left(L_{norm}^{(i)} \times \omega^{(i)} \right), \tag{3.13}$$

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

Вагові коефіцієнти k_{ij} та k_i в функціях згортки (8)-(9) вершин ієрархічного дерева пропонується розраховувати за схемою Фішберна [76], яка використовується для визначення величини вагових коефіцієнтів, представлених раціональними дробами, за умови, що визначені відношення пріоритетності між критеріями. Знаменниками вказаних раціональних дробів є сума арифметичної прогресії m (кількість критеріїв) перших членів натурального ряду з кроком 1, а чисельниками – спадаючі на 1 елементи натурального ряду від до m до 1.

Наприклад, при m=3 та наявності відношення пріоритетності типу $Y_1 \succ Y_2 \succ Y_3$ вагові коефіцієнти, визначені за схемою Фішберна дорівнюватимуть $k_1 = \frac{3}{6}$, $k_2 = \frac{2}{6}$, $k_3 = \frac{1}{6}$. Тобто, відповідно до схеми Фішберна перевага виражається в спаданні на одиницю чисельника раціонального дробу вагового коефіцієнту критерію, що має слабкіший пріоритет. Зауважимо, що визначення величини вагових коефіцієнтів за схемою Фішберна відповідає максимуму ентропії наявної інформаційної невизначеності щодо вагових коефіцієнтів.

В загальному випадку, коли в системі вагових коефіцієнтів критеріїв присутні як відношення переваги, так і відношення байдужості, визначення вагових коефіцієнтів k_i критеріїв Y_i відповідно до схеми Фішберна здійснюється за наступними рекурентними співвідношеннями:

$$r_{i-1} = \begin{cases} r_i, \text{ якщо } Y_{i-1} \approx Y_i, \\ r_i + 1, \text{ якщо } Y_{i-1} \succ Y_i, \end{cases} \quad r_m = 1, \quad i = m, \ldots, 2. \tag{3.14}$$

$$K = \sum_{i=1}^{m} r_i; \quad k_i = \frac{r_i}{K},$$

де: r_i – ранг критерію Y_i; m – кількість критеріїв; k_i – ваговий коефіцієнт критерію Y_i.

Для ілюстрації в таблиці 3.4 представлені величини вагових коефіцієнтів k_i, розрахованих за схемою Фішберна для різних відношень пріоритетності критеріїв Y_i.

Таблиця 3.4 – Величини вагових коефіцієнтів, розрахованих за схемою Фішберна

Відношення пріоритетності	k_1	k_2	k_3
$Y_1 \approx Y_2 \approx Y_3$	1/3	1/3	1/3
Y_1 f $Y_2 \approx Y_3$	2/4	1/4	1/4
$Y_1 \approx Y_2$ f Y_3	2/5	2/5	1/5
Y_1 f Y_2 f Y_3	3/6	2/6	1/6

Отримані в результаті згортки значення лінгвістичних змінних у вигляді терм-множини (рис. 3.13) розпізнаються за допомогою операцій нечіткої фільтрації за показником можливості [77].

Нехай для досліджуваного банку нечіткі терм-множини нормованих лінгвістичних змінних критеріїв $L_{norm}^{(i)}$ мають вигляд, поданий на рисунку 3.14.

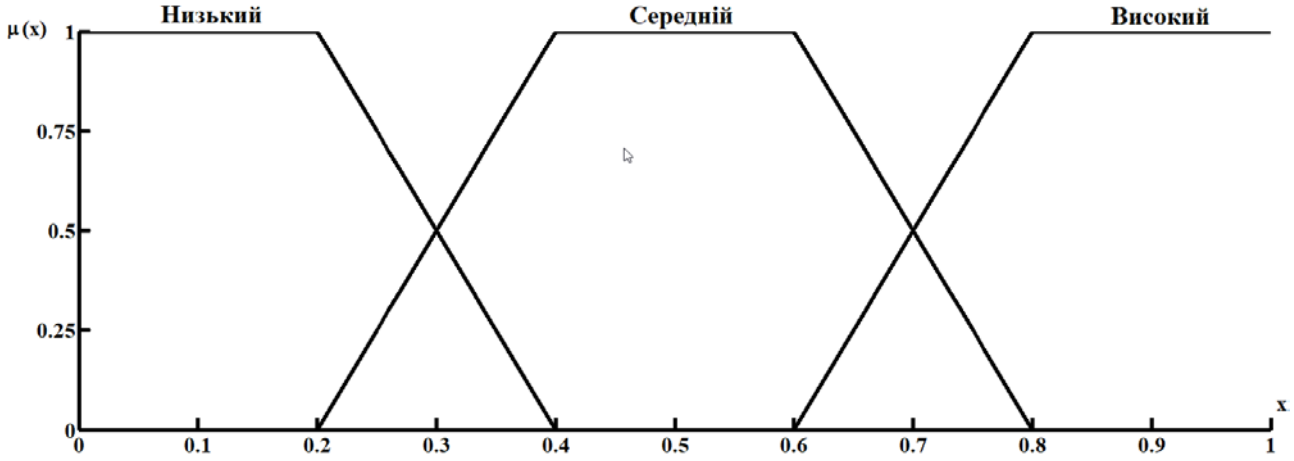

Рисунок 3.14 – Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(i)}$

Абсциси нейтральних точок на 01-носії (рис. 3.14) мають координати (0.3, 0.7).

Нехай нормоване значення критерію захищеності інформаційно-телекомунікаційної системи банку $L_{norm}^{(1)} = 0{,}5$; критерію надійності персоналу банку $L_{norm}^{(2)} = 0{,}9$; критерію якості інформації для прийняття рішень $L_{norm}^{(3)} = 0{,}7$. Виконаємо згортку критеріїв $L_{norm}^{(i)}$ в комплексний показник $L_{norm}^{(Y)}$ з рівнями значущості $k_1 = 0{,}5;\quad k_2 = 0{,}3;\quad k_3 = 0{,}2.$ Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(Y)}$ наведена на рисунку 3.15.

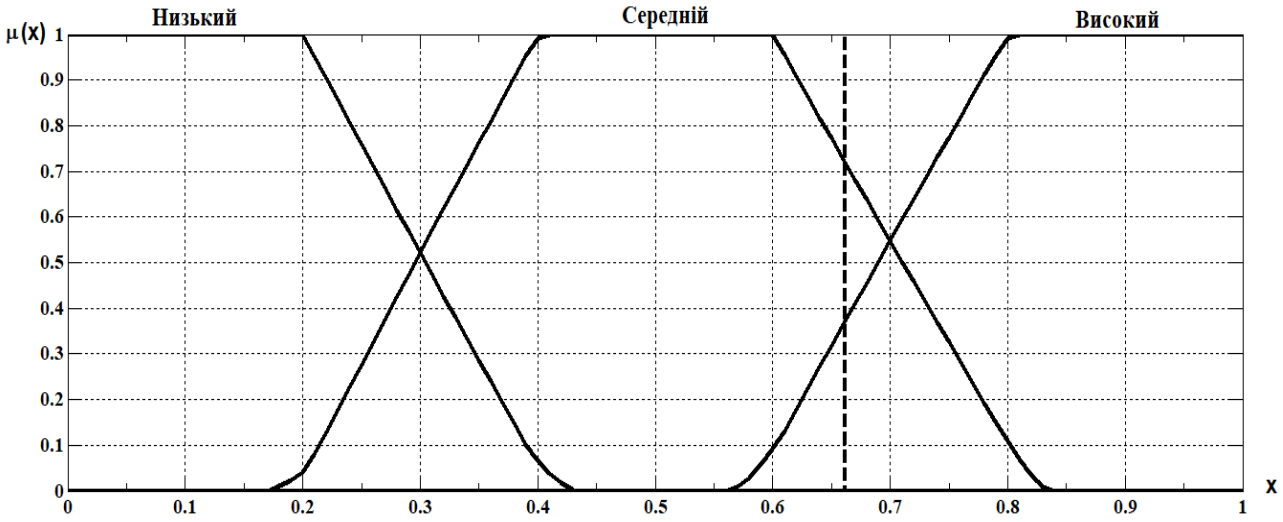

Рисунок 3.15 – Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(Y)}$

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

3.4 Динамічний підхід щодо моделювання процесу боротьби з кібератаками у сфері електронного банкінгу

Відсутність належної уваги до безпеки проведення онлайн-операцій може зробити їх уразливими для злочинців.

Сьогодні більшість фінансових операцій здійснюються через Інтернет. Розвиток електронної комерції призвів до того, що ці тенденції поширилися і на банківський сектор. З початку 80-х термін «електронний банкінг» увійшов в економічну термінологію.

З надходженням коштів через Інтернет-канали зв'язку, шахраї, які придумують все нові і нові схеми кібератак, стали активнішими. З появою нових кібератак з'являються нові протидіючі інструменти.

Вивчення цього питання хоча і є актуальним, але, на жаль, знаходиться на базовому рівні. Це пов’язано з тим, що, в першу чергу, вся інформація про кібератаки, які здійснюються в банківському секторі, є конфіденційною.

У той же час теоретично і практично виправдано, що поява нових шахрайських схем призводить до розробки нових інструментів боротьби з ними. Таким чином, існує своєрідна гонка, яка може тривати назавжди.

Таким чином, перед вченими стоїть завдання вивчити динаміку виникнення кібератак у банківському секторі та розробити інструменти протидії шахрайству в електронному банку.

Інноваційний розвиток економіки будь-якої країни залежить від спрямованості суспільства до інформаційного простору. На сьогодні головним напрямком інновацій у бізнесі є передача комерційної діяльності в Інтернет-просторі. Щороку від 30% до 70% бізнесу в будь-якій країні (незалежно від рівня розвитку) переходить в онлайн сферу. Тобто компанії все частіше використовують системи електронної комерції для ведення бізнесу.

Початок Інтернет економіки може бути пов’язаний з проривом під час появи системи Всесвітньої павутини в середині 1990-х. Сьогодні для опису економічних відносин в Інтернеті використовується поняття «електронна комерція», яке є частиною Інтернет економіки. Таким чином, Організація економічного співробітництва та розвитку дає таке визначення цього терміна (у широкому розумінні): будь-яка форма ділових відносин, де взаємодія між суб'єктами відбувається за допомогою Інтернет-технологій [78].

Кузьменко Ольга Віталіївна,
Яровенко Ганна Миколаївна,
Лєонов Сергій Вячеславович

СУЧАСНІ ІНСТРУМЕНТИ БОРОТЬБИ З КІБЕРШАХРАЙСТВАМИ У БАНКАХ

Монографія
За загальною редакцією О. В. Кузьменко, Г. М. Яровенко

Відповідальний за випуск О. В. Кузьменко

Підписано до друку 16.11. 2018.
Формат 60х84/16. Папір офсетний. Друк офсетний.
Умовн. друк. арк. 9,98. Обл.-вид. арк. 9,86
Наклад 300 прим. Вид. №128/218.

Видавець і виготовлювач: видавництво «Ярославна», Україна,
40030, м. Суми, вул. Горького, 2,

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру
ДК № 332 від 09.02.2001 р.