КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.894
УДК 004.056.5

Ільєнко Анна Вадимівна
кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0001-8565-1117
anna.ilienko@npp.kai.edu.ua

Ахрамович Вадим Володимирович
Національна академія статистики, обліку та аудиту, Київ, Україна
ORCID ID: 0009-0003-2787-8745
12zstzi@ukr.net

МЕТОД РОЗРАХУНКУ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Анотація. Актуальним завданням аналізу та управління інформаційною системою корпоративної мережі є вибір такого складу системних елементів, та їх параметрів який забезпечить можливість досягнення максимальної функціональної ефективності в умовах невизначеності. Одним з перспективних підходів до вирішення проблеми оцінки кібербезпеки на об'єктах критичної інфраструктури є використання теорії нечітких множин, наприклад, для оцінки ризиків інформаційної безпеки. На практиці трапляються ситуації, коли на розрахунок кінцевих результатів істотно впливають невідповідності висновків або помилки експертів. У статті проведено дослідження системи захисту корпоративної мережі з урахуванням її архітектурних та функціональних складових в умовах часткової або повної невизначеності Для досягнення поставленої мети було побудовано кортеж нечітких множин, що описують найважливіші аспекти функціонування та захисту корпоративної мережі. У кортеж включено як технічні характеристики (наприклад, інтенсивність інформаційного потоку, рівень захисту, параметри витоку даних, активність фаєрволу, роботу системи резервного копіювання тощо), так і організаційні складові (розмежування доступу, політика автентифікації, ідентифікація користувачів, аудит тощо). Кожен з параметрів отримав відповідну нечітку інтерпретацію у вигляді лінгвістичних змінних: «низький», «середній», «високий» рівень. Для обрахунків параметрів, використані методи трапеції та трикутника. Розрахунки ілюстровані графічним матеріалом. Отримані дані також можуть бути використані для автоматизованого моніторингу стану захищеності мережі, оцінки ефективності впроваджених заходів безпеки, формування рекомендацій щодо підвищення рівня захисту.

Ключові слова: нечіткі множини; корпоративна мережа; кортеж; моделювання; ризики; система захисту; агрегація; функція належності.

ВСТУП

Поняття нечіткої множини — це спроба математичної формалізації нечіткої інформації для побудови математичних моделей. В основі цього поняття лежить уявлення про те, що елементи, які складають дану множину та мають спільну загальну властивість, можуть мати цю властивість різного ступеня і, отже, належати до цієї множини з різним ступенем. За таким підходом вислови типу «такий-то елемент належить даній множині» втрачають сенс, оскільки необхідно вказати «як сильно» або з яким ступенем конкретний елемент задовольняє властивостям даної множини.

Сьогодні нечітка логіка розглядається як стандартний метод моделювання і проектування. У 1997 р. мова нечіткого управління (Fuzzy Control Language) внесена до Міжнародного стандарту програмованих контролерів IEC 1131-7. Системи на нечітких множинах розроблені і успішно упроваджені в таких областях, як: медична діагностика,

технічна діагностика, фінансовий менеджмент, управління персоналом, біржове прогнозування, розпізнавання образів, розвідка копалин, виявлення шахрайств, управління комп'ютерними мережами, управління технологічними процесами, управління транспортом, логістика, пошук інформації в Інтернеті, радіозв'язок і телебачення.

Спектр додатків дуже широкий — від побутових відеокамер, пилососів і пральних машин до засобів наведення ракет ППО і управління бойовими вертольотами і літаками. Як і раніше лідирує Японія, в якій випущено понад 4800 «нечітких» патентів (для порівняння, в США їх близько 1700). Практичний досвід розробки систем на нечітких множинах свідчить, що терміни і вартість їх проектування значно нижчі, ніж при використанні традиційного математичного апарату, при цьому забезпечуються необхідні рівні якості. Отець нечіткої логіки Лотфі Заде якось із цього приводу відмітив, що «майже завжди можна зробити такий же самий продукт без нечіткої логіки, але з нечіткою буде швидше і дешевше».

Засновані на цій теорії методи побудови комп'ютерних нечітких систем суттєво розширюють сфери застосування комп'ютерів. Останнім часом нечітке управління є однією з найактивніших і найрезультативніших областей досліджень застосування теорії нечітких множин. Нечітке управління виявляється особливо корисним, коли технологічні процеси надто складні для аналізу за допомогою загальноприйнятих кількісних методів, або коли доступні джерела інформації інтерпретуються якісно, неточно або невизначено. Експериментально показано, що нечітке управління дає кращі результати, порівняно з одержуваними за загальноприйнятих алгоритмів управління. Нечіткі методи допомагають керувати домівкою та прокатним станом, автомобілем і поїздом, мережами, розпізнавати мову та зображення, проектувати роботів, які мають дотик і зір.

Постановка проблеми. У сучасному цифровому світі, де технологічний прогрес постійно набирає обертів, кібербезпека корпоративної мережі стає надзвичайно актуальною проблемою. З кожним днем збільшується кількість кіберзагроз, які можуть впливати на локальні мережі, мережі організації, громадян і навіть національну безпеку. Особливої актуальності набувають задачі кібербезпекового оцінювання корпоративної мережі, ефективне вирішення яких залишається викликом для багатьох користувачів, адміністраторів мереж, управлінців відомств та держави в цілому. Необхідно оцінити вплив складових мережі на систему захисту в умовах невизначеності.

Аналіз останніх досліджень і публікацій. Одним з нових та перспективних підходів до вирішення таких задач, заснованих на експертних оцінюваннях, є використання теорії нечітких множин [1]–[9], наприклад, для оцінювання ризиків інформаційної безпеки [5]–[9]. Цей підхід дозволяє моделювати нечіткості та невизначеності в кібербезпековому контексті, надаючи можливість ефективно оцінювати загрози та їхні наслідки. При вирішенні задач експертного оцінювання, заснованого на використанні теорії нечітких множин виникає потреба в фазифікації початкових даних для подальшої їх обробки методами нечіткої логіки [6]–[9]. Оцінка складових корпоративних мереж та їх впливу на систему захисту представлена в роботі [10].

Мета та постановка завдання. Метою даного дослідження є підвищення ефективності оцінювання рівня захищеності корпоративної мережі в умовах невизначеності шляхом застосування теорії нечітких множин. Зростання кількості кіберзагроз, ускладнення структури інформаційних систем та обмеженість точних вхідних даних зумовлюють необхідність використання інноваційних підходів до виявлення, аналізу та управління ризиками інформаційної безпеки. Застосування апарату нечіткої логіки дозволяє моделювати невизначеність і нечіткість, характерні для

кібербезпекового контексту, а також надає змогу ефективно здійснювати експертне оцінювання загроз, їхніх наслідків та ступеня захищеності мережі.

Цей підхід дозволяє моделювати нечіткості та невизначеності в кібербезпековому контексті, надаючи можливість ефективно оцінювати загрози та їхні наслідки. При вирішенні задач експертного оцінювання, заснованого на використанні теорії нечітких множин виникає потреба в фазифікації початкових даних для подальшої їх обробки методами нечіткої логіки.

Необхідно оцінити вплив складових соціальної мережі на систему захисту в умовах невизначеності. Для цього необхідно сформувати кортеж нечітких множин із складових мережі; провести їх моделювання; розрахувати рівні ризиків; рівні захищенності мережі, провести агрегацію результатів, визначити функції належності. Для обрахунків параметрів, використати методи трапеції та трикутника.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Складання кортежа параметрів для корпоративної мережі (СМ)

Кортеж представлений як:

$$<I,Z,Z_p,C_v,C_k,C_{d1},C_{d2},Q_c,R_c,W_c,F_c,A_{dc},V_c,Z_{pc},Z_k,A_{rc},C_c,M_c,I_{dc},A_c,D_c,N_c,S_c> \quad (1)$$

де кожен елемент визначає специфічний аспект захисту інформаційної системи комп'ютера:

I: Потік інформації;

Визначає обсяг або частоту передачі інформації в системі (значення 0…1);

Z: Показник захисту інформації;

Відображає ефективність механізмів захисту (значення 0…1);.

Z_p: Вплив заходів захисту;

Визначає, наскільки заходи безпеки впливають на загальний рівень захисту (значення 0…1);.

C_{d1}:розміри системи та захищеність (значення 0…1);

Впливає на витік інформації;

C_{d2}: розміри системи та захищеність (значення 0…1);

Впливає на захищеність системи;

C_v: Вплив швидкості витоку даних;

Чим більша швидкість витоку, тим більше загроза (значення 0…1);.

C_k: Вплив обсягу даних на ризик витоку;

Більший обсяг даних може призводити до підвищеного ризику (значення 0…1);.

Q_k — коефіцієнт, що відображає контроль цілісності та автентичності даних в мережі (значення 0…1);

R_k: коефіцієнт, що відображає резервне копіювання даних (значення 0…1);

W_k: коефіцієнт, що відображає розмежування доступу до інформації (значення 0…1);

F_k: коефіцієнт, що відображає роботу Firewall (значення 0…1);

A_{dk}: коефіцієнт, що відображає аудит (використовується для спостереження, протоколювання) (значення 0…1);

V_k: коефіцієнт, що відображає антивірусне забезпечення (значення 0…1);

Z_{pk}: коефіцієнт, що відображає збої та відмови компонент програмного забезпечення, які відповідають за роботу мережі (0 або 1);

Z_k: коефіцієнт, що відображає збої та відмови компонент апаратного забезпечення, які відповідають за роботу мережі (0 або 1);

A_{rk}: коефіцієнт, що відображає систему мережевого резервування (значення 0…1);

C_k: коефіцієнт, що відображає систему шифрування (значення 0…1);

B_k: коефіцієнт, що відображає розмежування потоків інформації між сегментами мережі (значення 0…1);

E_k: коефіцієнт, що відображає фільтрацію спаму (значення 0…1);

T_k: коефіцієнт, що відображає фізичну безпеку мережі (значення 0…1);

Y_k: коефіцієнт, що відображає підсистему сканування та діагностики (значення 0…1);

U_k: коефіцієнт, що відображає підсистему диспетчеризації процесів контролю і забезпечення цілісності (значення 0…1);

I_d: коефіцієнт, що відображає ідентифікацію користувачів в мережі (значення 0 або 1)

A_k: коефіцієнт, що відображає автентифікацію користувачів в мережі (значення 0 або 1);

D_k: коефіцієнт, що відображає proxy–сервери (значення 0…1);

M_k: коефіцієнт, що відображає міжмережевий екран (значення 0…1).

N_k: коефіцієнт, що відображає мережу VPN (значення 0…1);

S_k: коефіцієнт, що відображає засоби, що виявляють неоднорідності та порушення, які виникають в мережі; (значення 0…1);

K_k: коефіцієнт, що відображає системи виявлення й запобігання вторгненню, наприклад (IDS, IPS) (значення 0…1);

O_k: коефіцієнт, що відображає підмережі захисту (значення 0…1).

З [10] відомо,що:

$$\bar{Z} = \frac{I_d A_k (D_k + M_k + N_k + S_k K_k + Q_k) - (C_{d2} + C_{d1})}{((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_{p1} Z_k)(C_{d2} + C_{d1})} \quad (2)$$

Для виконання аналізу залежності Z від складових параметрів в умовах використання нечітких множин необхідно пройти три етапи: фазифікацію, агрегацію правил і дефазифікацію. Давайте розглянемо кожен з цих етапів з урахуванням нашого кортежа параметрів.

1. Фазифікація

Фазифікація — це перетворення чітких вхідних даних у нечіткі множини за допомогою функцій належності.

Приклад розрахунків:

Задати функції належності:

Для параметрів I,Z,Z_p, що лежать у діапазоні [0;1], можна використати тріангульні функції належності. Наприклад:

Низький (Low): $\mu_{Low}(x) = \begin{cases} 1 - 2x, & 0 \le x \le 0.5 \\ 0, & x > 0 \end{cases}$

Середній (Medium): $\mu_{Medium}(x) = \begin{cases} 2x, & 0 \le x \le 0.5 \\ 2 - 2x, & 0.5 < x > 1 \end{cases}$

Високий (High): $\mu_{High}(x) = \begin{cases} 2x - 1, & 0.5 \le x \le 1 \\ 0, & x < 0.5 \end{cases}$

Фазифікувати вхідні дані:

Для кожного значення параметра (наприклад, I=0.6) обчислити належність кожній нечіткій множині.

2. Агрегація правил

На цьому етапі визначаються правила нечіткого виводу на основі знань про систему. Наприклад:

Приклади правил:

1. Якщо *I* низький і Z_p високий, то *Z* середній.
2. Якщо *I* високий і Z_p середній, то *Z* низький.
3. Якщо *I* середній і Z_p високий, то *Z* високий.

Методи агрегації:

Правила можна об'єднувати методом Макс-Мін (найбільш поширений підхід). Наприклад, якщо I=0.6 (μMedium=0.8) та Z_p=0.8 (μHigh=0.7), для відповідного правила Z середній. Активність правила=min(0.8,0.7)=0.7

Результати агрегації правил можна представити графічно як об'єднання висновків для параметра *Z*.

3. Дефазифікація

Дефазифікація — це перетворення нечіткого вихідного значення у чітке. Найпоширеніші методи:

Центр ваги (Center of Gravity, CoG): $Z = \frac{\int_{\text{універсум}} z * \mu(z)\, dz}{\int_{\text{універсум}} \mu(z)\, dz}$

Максимальна ймовірність: Визначення значення *Z* із найвищою функцією належності. Графічно це відповідає визначенню центру площі нечіткої множини *Z*.

Розрахунок і графіки:

Для розрахунків залежності *Z* потрібно:

1. Виконати фазифікацію вхідних параметрів (обчислення μLow,μMedium,μHigh для кожного значення).
2. Побудувати нечітку базу знань із правил.
3. Провести агрегацію (графічно показати перетини множин).
4. Виконати дефазифікацію для отримання *Z*.

Для проведення розрахунків і побудови графіків залежності *Z* від вхідних параметрів (на основі нечітких множин), я запропоную використовувати Python. Основні кроки включають:

4. **Фазифікацію:** Розрахунок функцій належності для вхідних параметрів.
2. **Агрегацію правил:** Визначення логіки взаємодії параметрів I, Z_p, C_{d1}, C_{d2}, та їх впливу на *Z*.
3. **Дефазифікацію:** Визначення чіткого значення *Z* на основі отриманих результатів.
4. **Візуалізацію:** Побудова графіків для кожного етапу.

Створено код для розрахунку та побудови графіків фазифікації (рис.1), агрегації правил і дефазифікації (рис. 2) залежності *Z* від параметрів I та Z_p. Ви можете виконати цей код у Python (необхідні бібліотеки: numpy, matplotlib, scikit-fuzzy).

1. Фазифікація. На рис. 1 представлене схематичне зображення процесу перетворення вхідних даних у нечіткі множини.

На вході: чіткі параметри (наприклад, I,Z_p,C_{d1},C_{d2},… у вигляді лінгвістичних змінних). **Процес:** Зображення системи функцій належності, де кожен параметр оцінюється як нечітка множина (наприклад, «низький», «середній», «високий»). Вибрати функції належності (трикутні, трапецієподібні, гауссові тощо) для кожного параметра. **Вихід:** Нечіткі значення для кожного коефіцієнта (рис. 1,2).

2. Дефазифікація. На рис. 2 представлене зворотний процес — перетворення нечітких множин у чіткі значення.

На вході: Нечіткі множини з різними рівнями належності**. Процес:** Механізм вибору чіткого значення (методи: центр ваги, середнє значення, метод найбільшого піку). **Вихід**: Графічне представлення чітких результатів для кожного параметра.

Далі наведемо фрагмент коду для розрахунку та побудови графіків фазифікації мовою програмування Python. Для реалізації було використано бібліотеки numpy — для

числових розрахунків; skfuzzy — для роботи з нечіткою логікою та matplotlib.pyplot — для побудови графіків. Даний код дає змогу реалізувати повноцінну систему нечіткого виводу (fuzzy inference), яка: приймає вхідні дані (I і Z_p); визначає, до яких нечітких множин вони належать; застосовує логічні правила; агрегує результати; видає чітке значення захисту Z. Результати моделювання представлені на рис. 1.

```
Fuzzy Analysis Z
import numpy as np
import skfuzzy as fuzz
import matplotlib.pyplot as plt

# 1. Визначення універсумів і функцій належності
x_I = np.linspace(0, 1, 100)   # Універсум для потоку інформації I
x_Zp = np.linspace(0, 1, 100)  # Універсум для впливу заходів захисту Zp
x_Z = np.linspace(0, 1, 100)   # Універсум для показника захисту Z

# Функції належності для I (Low, Medium, High)
I_low = fuzz.trimf(x_I, [0, 0, 0.5])
I_medium = fuzz.trimf(x_I, [0.2, 0.5, 0.8])
I_high = fuzz.trimf(x_I, [0.5, 1, 1])

# Функції належності для Zp (Low, Medium, High)
Zp_low = fuzz.trimf(x_Zp, [0, 0, 0.5])
Zp_medium = fuzz.trimf(x_Zp, [0.2, 0.5, 0.8])
Zp_high = fuzz.trimf(x_Zp, [0.5, 1, 1])

# Функції належності для Z (Low, Medium, High)
Z_low = fuzz.trimf(x_Z, [0, 0, 0.5])
Z_medium = fuzz.trimf(x_Z, [0.2, 0.5, 0.8])
Z_high = fuzz.trimf(x_Z, [0.5, 1, 1])

# 2. Побудова графіків функцій належності
fig, axs = plt.subplots(1, 3, figsize=(15, 5))

axs[0].plot(x_I, I_low, ‘b’, label=‘Low’)
axs[0].plot(x_I, I_medium, ‘g’, label=‘Medium’)
axs[0].plot(x_I, I_high, ‘r’, label=‘High’)
axs[0].set_title(‘Membership Functions for I’)
axs[0].legend()

axs[1].plot(x_Zp, Zp_low, ‘b’, label=‘Low’)
axs[1].plot(x_Zp, Zp_medium, ‘g’, label=‘Medium’)
axs[1].plot(x_Zp, Zp_high, ‘r’, label=‘High’)
axs[1].set_title(‘Membership Functions for Zp’)
axs[1].legend()

axs[2].plot(x_Z, Z_low, ‘b’, label=‘Low’)
axs[2].plot(x_Z, Z_medium, ‘g’, label=‘Medium’)
```

```
axs[2].plot(x_Z, Z_high, ‘r’, label=‘High’)
axs[2].set_title(‘Membership Functions for Z’)
axs[2].legend()

plt.tight_layout()
plt.show()

# 3. Нечітка логіка правил
# Вхідні значення для прикладу
I_level = 0.6
Zp_level = 0.7

# Фазифікація вхідних значень
I_low_level = fuzz.interp_membership(x_I, I_low, I_level)
I_medium_level = fuzz.interp_membership(x_I, I_medium, I_level)
I_high_level = fuzz.interp_membership(x_I, I_high, I_level)

Zp_low_level = fuzz.interp_membership(x_Zp, Zp_low, Zp_level)
Zp_medium_level = fuzz.interp_membership(x_Zp, Zp_medium, Zp_level)
Zp_high_level = fuzz.interp_membership(x_Zp, Zp_high, Zp_level)

# Застосування правил
rule1 = np.fmin(I_low_level, Zp_high_level)  # If I is Low and Zp is High, then Z is Medium
rule2 = np.fmin(I_medium_level, Zp_medium_level)  # If I is Medium and Zp is Medium,
then Z is High
rule3 = np.fmin(I_high_level, Zp_low_level)   # If I is High and Zp is Low, then Z is Low

# Агрегація результатів
Z_activation_medium = np.fmin(rule1, Z_medium)
Z_activation_high = np.fmin(rule2, Z_high)
Z_activation_low = np.fmin(rule3, Z_low)

aggregated = np.fmax(Z_activation_low, np.fmax(Z_activation_medium, Z_activation_high))

# 4. Дефазифікація
Z_defuzzified = fuzz.defuzz(x_Z, aggregated, ‘centroid’)

# Побудова графіка результату
plt.figure(figsize=(8, 5))
plt.plot(x_Z, Z_low, ‘b’, linestyle=‘--’, label=‘Low’)
plt.plot(x_Z, Z_medium, ‘g’, linestyle=‘--’, label=‘Medium’)
plt.plot(x_Z, Z_high, ‘r’, linestyle=‘--’, label=‘High’)
plt.fill_between(x_Z, 0, aggregated, alpha=0.5, label=‘Aggregated’, color=‘orange’)
plt.axvline(Z_defuzzified, color=‘k’, linestyle=‘:’, label=f’Defuzzified (Z) =
{Z_defuzzified:.2f}’)
plt.title(‘Aggregated Membership and Defuzzification’)
plt.legend()
plt.show()
```

ISSN 2663 - 4023

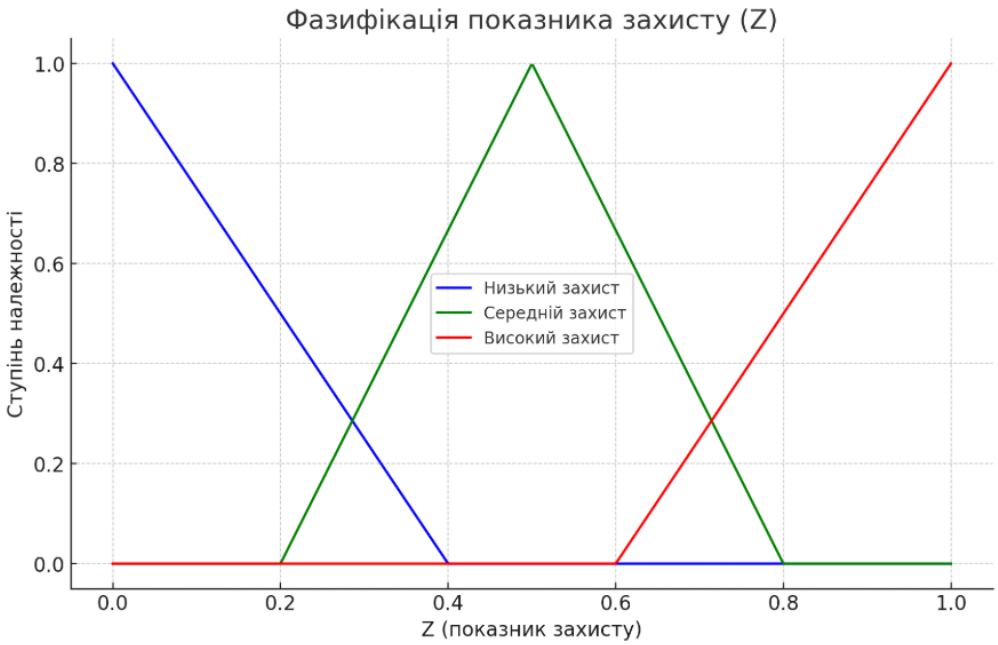

Рис. 1. Фазифікація показника Z

Далі наведемо програмний код для розрахунку та побудови графіків дефазифікації мовою програмування Python. Для реалізації було використано бібліотеки numpy — для роботи з масивами; matplotlib.pyplot — для побудови графіків; skfuzzy.control — модуль нечіткої логіки; skfuzzy — модуль для створення функцій належності. Нижче наведений програмний код реалізує нечітку логічну систему (fuzzy logic system) для моделювання рівня захисту (Z) на основі чотирьох вхідних параметрів: C_{d1}, C_{d2}, Z_p, Q_k, і будує графіки функцій належності, а також 3D-графік дефазифікованого результату. Результати моделювання представлені на рис. 2.

Defuzzification Graphs

```
import numpy as np
import matplotlib.pyplot as plt
from skfuzzy import control as ctrl
import skfuzzy as fuzz

# 1. Визначення нечітких змінних
# Вхідні параметри
Cd1 = ctrl.Antecedent(np.arange(0, 1.1, 0.1), 'Cd1')
Cd2 = ctrl.Antecedent(np.arange(0, 1.1, 0.1), 'Cd2')
Zp = ctrl.Antecedent(np.arange(0, 1.1, 0.1), 'Zp')
Qk = ctrl.Antecedent(np.arange(0, 1.1, 0.1), 'Qk')

# Вихідна змінна
Z = ctrl.Consequent(np.arange(0, 1.1, 0.1), 'Z')

# 2. Функції належності для вхідних параметрів
Cd1['low'] = fuzz.trimf(Cd1.universe, [0, 0, 0.5])
```

```
Cd1[‘medium’] = fuzz.trimf(Cd1.universe, [0, 0.5, 1])
Cd1[‘high’] = fuzz.trimf(Cd1.universe, [0.5, 1, 1])

Cd2[‘low’] = fuzz.trimf(Cd2.universe, [0, 0, 0.5])
Cd2[‘medium’] = fuzz.trimf(Cd2.universe, [0, 0.5, 1])
Cd2[‘high’] = fuzz.trimf(Cd2.universe, [0.5, 1, 1])

Zp[‘low’] = fuzz.trimf(Zp.universe, [0, 0, 0.5])
Zp[‘medium’] = fuzz.trimf(Zp.universe, [0, 0.5, 1])
Zp[‘high’] = fuzz.trimf(Zp.universe, [0.5, 1, 1])

Qk[‘low’] = fuzz.trimf(Qk.universe, [0, 0, 0.5])
Qk[‘medium’] = fuzz.trimf(Qk.universe, [0, 0.5, 1])
Qk[‘high’] = fuzz.trimf(Qk.universe, [0.5, 1, 1])

# 3. Функції належності для вихідного параметра
Z[‘low’] = fuzz.trimf(Z.universe, [0, 0, 0.5])
Z[‘medium’] = fuzz.trimf(Z.universe, [0, 0.5, 1])
Z[‘high’] = fuzz.trimf(Z.universe, [0.5, 1, 1])

# 4. Нечіткі правила
rule1 = ctrl.Rule(Cd1[‘low’] & Cd2[‘low’], Z[‘high’])
rule2 = ctrl.Rule(Cd1[‘medium’] | Cd2[‘medium’], Z[‘medium’])
rule3 = ctrl.Rule(Cd1[‘high’] & Cd2[‘high’], Z[‘low’])
rule4 = ctrl.Rule(Zp[‘high’] & Qk[‘high’], Z[‘high’])
rule5 = ctrl.Rule(Zp[‘low’] | Qk[‘low’], Z[‘low’])

# 5. Контролер
protection_ctrl = ctrl.ControlSystem([rule1, rule2, rule3, rule4, rule5])
protection_simulation = ctrl.ControlSystemSimulation(protection_ctrl)

# 6. Вхідні значення для тесту
protection_simulation.input[‘Cd1’] = 0.7
protection_simulation.input[‘Cd2’] = 0.6
protection_simulation.input[‘Zp’] = 0.2
protection_simulation.input[‘Qk’] = 0.9

# Обчислення
protection_simulation.compute()
print(f"Рівень захисту Z : {protection_simulation.output[‘Z’]:.2f}")

# 7. Побудова графіків
fig, axes = plt.subplots(2, 2, figsize=(10, 8))
Cd1.view(ax=axes[0, 0])
Cd2.view(ax=axes[0, 1])
Zp.view(ax=axes[1, 0])
Qk.view(ax=axes[1, 1])
plt.tight_layout()
```

ISSN 2663 - 4023

```
plt.show()

# Вхідні функції належності
Z.view()
plt.show()

# 8. Графік залежності Z від двох параметрів
x = np.linspace(0, 1, 100)
y = np.linspace(0, 1, 100)
X, Y = np.meshgrid(x, y)
Z_values = np.zeros_like(X)

for i in range(X.shape[0]):
    for j in range(X.shape[1]):
        protection_simulation.input['Cd1'] = X[i, j]
        protection_simulation.input['Cd2'] = Y[i, j]
        protection_simulation.input['Zp'] = 0.8  # Фіксоване значення
        protection_simulation.input['Qk'] = 0.9  # Фіксоване значення
        protection_simulation.compute()
        Z_values[i, j] = protection_simulation.output['Z']

fig = plt.figure(figsize=(10, 7))
ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(X, Y, Z_values, cmap='viridis')
ax.set_xlabel('Cd1')
ax.set_ylabel('Cd2')
ax.set_zlabel('Z')
plt.title('Залежність Z від Cd1 та Cd2')
plt.show()
```

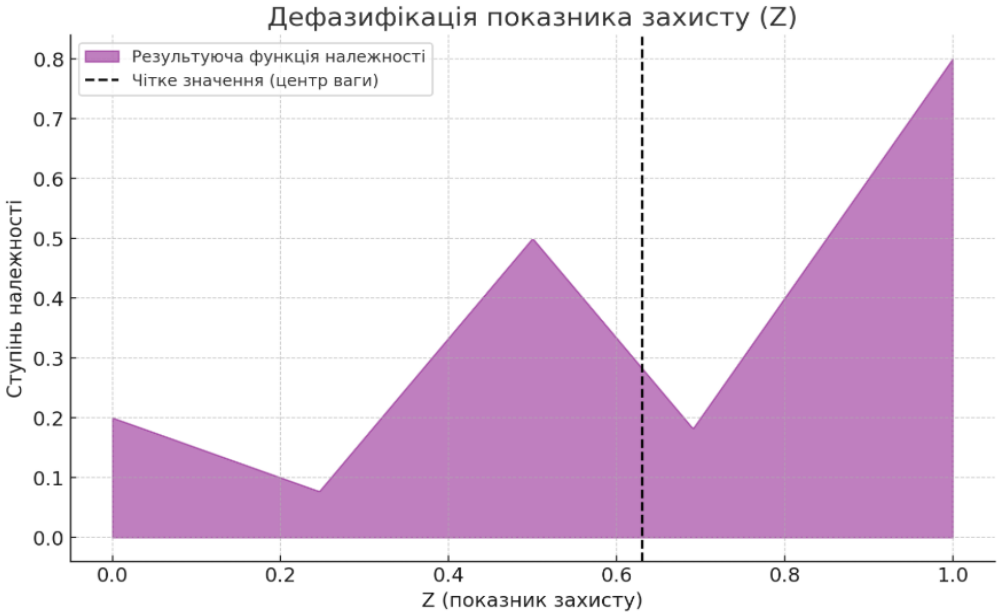

Рис. 2. Дефазифікація показника захисту Z

ВИСНОВКИ

У даній роботі було запропоновано метод оцінювання рівня захисту корпоративної мережі в умовах невизначеності з використанням апарату теорії нечітких множин. Проведено побудову кортежу параметрів, що характеризують різні аспекти функціонування мережі, та здійснено їхнє моделювання з урахуванням факторів ризику, ефективності засобів захисту, впливу архітектури та стану компонентів інфраструктури.

На основі нечітких множин реалізовано три основні етапи: фазифікація, агрегація правил та дефазифікація, які дозволили отримати кількісне значення рівня захисту мережі (Z) при наявності, нечіткої або суперечливої інформації. У моделюванні застосовано трикутні функції належності для основних параметрів, а також побудовано графічне відображення процесів фазифікації та дефазифікації. Результати досліджень засвідчили доцільність та ефективність використання нечіткої логіки для задач оцінювання інформаційної безпеки, особливо в умовах відсутності повних або точних даних. Запропонований метод створює основу для формування інтелектуальних систем підтримки прийняття рішень у сфері кібербезпеки корпоративних мереж, які здатні адаптуватися до динамічних умов сучасного інформаційного середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., & Tkachuk, S. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. *Eastern-European Journal of Enterprise Technologies*, *111*(3/9), 63–83.
2. Yevseiev, S. P., Shmatko, O. V., & Romashchenko, N. V. (2019). An algorithm for assessing the degree of information security risk based on a fuzzy set approach. *Suchasni Informatsiini Systemy – Modern Information Systems*, *3*(2), 73–79.
3. Kochetkov, O. V., Gaur, T. O., & Mashin, V. M. (2019). Enterprise information security risk assessment system based on fuzzy logic. *Scientific Works of O.S. Popov ONAZ, (1)*, 97–104.
4. Korchenko, A. O. (2019). *Methods for identifying anomalous states for intrusion detection systems: Monograph*. Kyiv: TsP “Komprint”.
5. Korchenko, O. H., Kazmirchuk, S. V., & Akhmetov, B. B. (2017). *Applied systems for assessing information security risks: Monograph*. Kyiv: TsP “Komprint”.
6. Korchenko, A. H. (2006). *Construction of information protection systems on fuzzy sets: Theory and practical solutions*. Kyiv: MK-Press.
7. Korchenko, O. H., Kazmirchuk, S. V., & Akhmetov, B. B. (2017). *Applied systems for assessing information security risks: Monograph*. Kyiv: TsP “Komprint”.
8. Korchenko, A., Arkhipov, A., & Kazmirchuk, S. (2013). *Analysis and assessment of information security risks: Monograph*. Kyiv: Lazurit-Polygraph LLC.
9. Akhramovych, V., & Akhramovych, V. (2025). A method for calculating the indicator of computer information protection under conditions of uncertainty. *Information Technology and Security*, *13*(1(24)), 55–68. https://doi.org/10.20535/2411-1031.2025.13.1.328898
10. Akhramovych, V. (2025). A method for researching quantitative indicators of the corporate network protection system. *Cybersecurity: Education, Science, Technology*, *4*(28), 176–197.
11. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
12. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
13. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Anna Ilyenko
Candidate of Technical Sciences, Associate Professor,
Head of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-8565-1117
anna.ilienko@npp. kai.edu.ua

Vadym Akhramovych
National Academy of Statistics, Accounting and Audit, Kyiv, Ukraine
ORCID ID: 0009-0003-2787-8745
12zstzi@ukr.net

A METHOD FOR CALCULATING THE PROTECTION OF A CORPORATE NETWORK UNDER CONDITIONS OF UNCERTAINTY

Abstract. A relevant task in the analysis and management of a corporate network information system is to select such a configuration of system elements and their parameters that ensures the highest possible functional efficiency under conditions of uncertainty. One of the promising approaches to solving the problem of cybersecurity assessment for critical infrastructure objects is the use of fuzzy set theory, for example, for assessing information security risks. In practice, situations often arise in which the final calculation results are significantly influenced by inconsistencies in conclusions or errors made by experts.This paper investigates the protection system of a corporate network, taking into account its architectural and functional components under conditions of partial or complete uncertainty. To achieve this goal, a tuple of fuzzy sets was constructed to describe the most important aspects of the corporate network's operation and security. The tuple includes both technical characteristics (e.g., information flow intensity, security level, data leakage parameters, firewall activity, operation of the backup system, etc.) and organizational components (access control, authentication policy, user identification, auditing, etc.). Each parameter was given an appropriate fuzzy interpretation in the form of linguistic variables: "low," "medium," and "high" levels.For parameter calculations, trapezoidal and triangular methods were applied. The calculations are illustrated with graphical material. The obtained data can also be used for automated monitoring of the network's security state, evaluation of the effectiveness of implemented security measures, and formulation of recommendations for improving the level of protection.

Keywords: fuzzy sets; corporate network; tuple; modeling; risks; protection system; aggregation; membership function.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., & Tkachuk, S. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. *Eastern-European Journal of Enterprise Technologies*, *111*(3/9), 63–83.
2. Yevseiev, S. P., Shmatko, O. V., & Romashchenko, N. V. (2019). An algorithm for assessing the degree of information security risk based on a fuzzy set approach. *Suchasni Informatsiini Systemy – Modern Information Systems*, *3*(2), 73–79.
3. Kochetkov, O. V., Gaur, T. O., & Mashin, V. M. (2019). Enterprise information security risk assessment system based on fuzzy logic. *Scientific Works of O.S. Popov ONAZ, (1)*, 97–104.
4. Korchenko, A. O. (2019). *Methods for identifying anomalous states for intrusion detection systems: Monograph*. Kyiv: TsP "Komprint".
5. Korchenko, O. H., Kazmirchuk, S. V., & Akhmetov, B. B. (2017). *Applied systems for assessing information security risks: Monograph*. Kyiv: TsP "Komprint".
6. Korchenko, A. H. (2006). *Construction of information protection systems on fuzzy sets: Theory and practical solutions*. Kyiv: MK-Press.
7. Korchenko, O. H., Kazmirchuk, S. V., & Akhmetov, B. B. (2017). *Applied systems for assessing information security risks: Monograph*. Kyiv: TsP "Komprint".

8. Korchenko, A., Arkhipov, A., & Kazmirchuk, S. (2013). *Analysis and assessment of information security risks: Monograph*. Kyiv: Lazurit-Polygraph LLC.
9. Akhramovych, V., & Akhramovych, V. (2025). A method for calculating the indicator of computer information protection under conditions of uncertainty. *Information Technology and Security*, *13*(1(24)), 55–68. https://doi.org/10.20535/2411-1031.2025.13.1.328898
10. Akhramovych, V. (2025). A method for researching quantitative indicators of the corporate network protection system. *Cybersecurity: Education, Science, Technology*, *4*(28), 176–197.
11. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
12. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
13. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.