DOI: 10.18372/2225-5036.30.20356

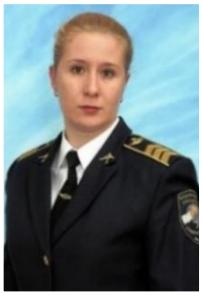
МЕТОД РОЗРАХУНКУ ЗАХИСТУ ІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ НЕЧІТКИХ МНОЖИН

Володимир Ахрамович[1], Олександр Лаптєв[1], Анна Ільєнко [1], Вадим Ахрамович[2]

1. Державний університет «Київський авіаційний інститут»
2. Національна академія статистики, обліку та аудиту

АХРАМОВИЧ Володимир Миколайович, д.т.н., проф.
Рік та місце народження: 1951р., с. Луб'янка Поліського району, Київської обл.
Освіта: Київський політехнічний інститут 1980р.
Посада: професор кафедри кібербезпеки Державний університет «Київський авіаційний інститут»,
Наукові інтереси: кібербезпека, інформаційна безпека, технічний захист інформації,- захист мереж, автоматизація захисту інформації.
Публікації: більше 200 наукових праць, серед них: монографії, наукові статті , підручники та навчально -методичні посібники.
E-mail: 12z@ukr.net
Orcid ID: 0000-0002-0086-9131

ЛАПТЄВ Олександр Анатолієвич, д.т.н., с.н.с.
Рік та місце народження: 1964р., м. Шемонаїна, Казахстан
Освіта: Київське вище військове авіаційне інженерне училище
Посада: доцент кафедри кібербезпеки та захисту інформації Київського національного університету ім.Т.Шевченка
Наукові інтереси: кібербезпека, інформаційна безпека, технічний захист інформації, розробка моделей кіберзахисту від цифрових закладних пристроїв.
Публікації: більше 110 наукових праць, серед них: монографії, наукові статті , підручники та навчально -методичні посібники.
E-mail: alaptev64@ukr.net
Orcid ID: 0000-0002-4194-402X



ІЛЬЄНКО Анна Вадимівна, к.т.н., доцент
Рік та місце народження: 1987р., м. Венспілс, Латвія
Освіта: Національний авіаційний університет, 2009
Посада: завідувач кафедри кібербезпеки Державний університет «Київський авіаційний інститут»
Наукові інтереси: кібербезпека, інформаційна безпека, методи побудови та аналізу криптосистем, захищені інформаційні та комунікаційні системи і технології
Публікації: більше 200 наукових праць, серед них: монографії, посібник, статті у вітчизняних та міжнародних фахових виданнях, навчально-методичні комплекси дисциплін, матеріали і тези доповідей на конференціях, патенти на корисні моделі
E-mail: anna.ilienko@npp.nau.edu.ua
Orcid ID: 0000-0001-8565-1117

АХРАМОВИЧ Вадим Володимирович
Рік та місце народження 1980 р., м. Київ.
Освіта: Київський політехнічний інститут, 1993 р.
Посада: завідувач ком'ютерним центром, Національної академії статистики, обліку та аудиту.
Наукові інтереси: кібербезпека, програмування, програмне та технічне забезпечення захисту інформації, мережі.
Публікації: більше 10 наукових праць, в тому числі - 3 Scopus,
E-mail: 12zstzi@ukr.net
Orcid ID: https://orcid.org/0009-0003-2787-8745

Анотація. *Актуальним завданням аналізу та управління соціальною мережею є вибір такого складу системних елементів, та їх параметрів який забезпечить можливість досягнення максимальної функціональної ефективності в умовах невизначеності. У цій статті проведено дослідження системи захисту соціальної мережі від складових мережі в умовах невизначеності. Основна увага приділяється фазифікації даних, побудові моделей нечітких множин, оцінці ризиків і рівня захищеності мережевих об'єктів. Запропонований підхід дозволяє розробляти ефективні рішення для прийняття управлінських рішень у кібербезпековому контексті. Викладено алгоритм побудови кортежу параметрів захисту та їх моделювання за допомогою функцій належності. Окремо розглянуто методи агрегації результатів і розрахунків за допомогою трапецієподібних та трикутних функцій. Для цього складено: кортеж нечітких множин із складових мережі; проведено його моделювання; розраховані рівні ризиків; рівні захищеності мережі, агрегація результатів, функції належності. Для обрахунків параметрів, використані методи трапеції та трикутника. Розрахунки ілюстровані графічним матеріалом. Результати роботи можуть бути використані адміністраторами мереж, організаціями та державними установами для підвищення ефективності управління кібербезпекою та захисту інформаційних ресурсів.*

Ключові слова*: нечіткі множини, складові соціальної мережі, кортеж, моделювання, ризики, система* ***захисту,*** *агрегація, функція належності.*

Постановка проблеми

У сучасному цифровому світі, де технологічний прогрес постійно набирає обертів, кібербезпека мереж стає надзвичайно актуальною проблемою. З кожним днем збільшується кількість кіберзагроз, які можуть впливати на організації, громадян і навіть національну безпеку. Особливої актуальності набувають задачі кібербезпекового оцінювання на мережевих об'єктах, 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 [1-4], наприклад, для оцінювання ризиків інформаційної безпеки [5]. 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 [5]. Оцінка складових соціальних мереж (довіри, репутації, взаємодії, взаємовпливу) представлена в роботах [6-9].

Мета та постановка завдання

Зрозуміло, що зростання кількості кіберзагроз мережам, в тому числі, соціальним, вимагає нових інноваційних підходів до їхнього виявлення та управління. Використання теорії нечітких множин є одним із способів досягнення цієї мети та може допомогти користувачам, адміністраторам мереж, управлінцям, організаціям збільшити ефективність їхніх кібербезпекових заходів.

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.

Математична теорія нечітких множин (fuzzy sets) і нечітка логіка (fuzzy logic) є узагальненнями класичної теорії множин і класичної формальної логіки. Підвищення ефективності мережевих систем, підтримки прийняття рішень та управління в реальному часі в умовах невизначеності пов'язане з розробкою нових методів для обробки нечіткої інформації та великих масивів даних, приймаючи до уваги динамічну природу сигналів від реальних об'єктів. Основною характеристикою нечіткої множини є її функція належності, яка ставить у відповідність кожному елементу універсальної множини число з інтервалу [0, 1], що означає ступінь належності. Поняття функції належності є узагальненням поняття характеристичної функції чіткої множини, яка оперує значеннями {0, 1}. Тому основні властивості та операції над нечіткими множинами являють собою узагальнення відповідних властивостей та операцій класичної теорії множин. Подальше узагальнення поняття функції належності привело до появи нечітких множин типу 2 та множин вищих порядків. Узагальнена нечітка множина визначається функціями належності, в ролі значень яких також виступають нечіткі множини.

Проте побудова моделей на основі узагальнених нечітких множин пов'язана зі значною обчислювальною складністю, тому на практиці використовується їх інтервальне подання. Апарат інтервальних нечітких множин оперує лише крайніми точками інтервалу зміни значення функції належності, і не враховує особливостей розподілу, що виникає в межах цього інтервалу. Таке спрощення значно знижує кількість обчислювальних ресурсів, необхідних для побудови нечіткого логічного висновку; при цьому на якості функціонування системи це майже не відбивається. У США розвиток нечіткої логіки йде шляхом створення систем, що потрібні великому бізнесу і військовим. Нечітка логіка застосовується при аналізі нових ринків, біржовій грі, оцінці політичних рейтингів, виборі оптимальної цінової стратегії, оцінці рівня зрілості процесів захисту інформації і т. ін. З'явилися і комерційні системи масового застосування.

Початком практичного застосування теорії нечітких множин вважають 1973 р., коли Мамдані (Mamdani) і Ассиліан (Assilian) з Лондонського коледжу Королеви Мері побудували перший нечіткий контролер для лабораторної моделі парового двигуна. Концепцію першого нечіткого контролера складають ідеї нечіткого логічного виводу і нечіткого алгоритму, викладені Заде в 1973 р. Перший промисловий нечіткий контролер запрацював в кінці 1970-х років в Данії – Холмблад (Holmblad) і Остергард (Ostergaard) впровадили нечітку логіку в управління процесом випалення цементу. У 1980-х роках

європейські і американські інженерні і наукові співтовариства вельми скептично сприйняли нову теорію. Зате на Сході нечітка логіка пішла «на ура». Для людей, вихованих на східній філософії, з її неоднозначними і розпливчатими категоріями, нечітка логіка відразу стала своєю, рідною.

У Японії перший нечіткий контролер розробив Сугено (Sugeno) в 1983 р. за замовленням фірми Fuji El. для системи очищення води. Чотири роки опісля фірма Hitachi розробила нечітку систему управління рухом електропоїзду в метро м. Сендай. На 1990 р. в Японії було зареєстровано 30 патентів, пов'язаних з нечіткою логікою. На початку 1990-х років японці поставили нечітку логіку «на конвеєр» – почалося серійне виробництво побутових приладів з нечітким управлінням: камери з автоматичним фокусуванням (Canon), кондиціонери повітря (Mitsubishi), пральні машини (Panasonic і Matshushita).

Що стосується вітчизняного ринку комерційних систем на основі нечіткої логіки, то його формування почалося в середині 1995 року. Найбільш популярні в замовників такі пакети:

- CubiCalc 2.0 RTC – одна з найбільш могутніх комерційних експертних систем на основі нечіткої логіки, що дозволяє створювати власні прикладні експертні системи;

- CubiQuick – дешева «університетська» версія пакету CubiCalc;

- RuleMaker – програма автоматичного витягу нечітких правил із вхідних даних;

- FuziCalc – електронна таблиця з нечіткими полями, що дозволяє робити швидкі оцінки при неточно відомих даних без нагромадження похибки;
- OWL - пакет, що містить вихідні тексти усіх відомих видів нейронних мереж, нечіткої асоціативної пам'яті і т.д.

Використання сучасних комп'ютерних технологій суттєво розширює можливості дослідження методів теорії нечітких множин та нечіткої логіки, зокрема обчислювальні середовища FuzzyTECH та MATLAB забезпечують можливість використання блочно-структурних моделей для дослідження різних типів систем прийняття рішень та управління в умовах невизначеності.

Актуальним завданням аналізу та синтезу соціальної мережі є вибір такого складу системних елементів, та їх параметрів який забезпечить можливість досягнення максимальної функціональної ефективності в умовах невизначеності. Зокрема, це завдання виникає при синтезі мережі, представленою сукупністю взаємодіючих складових елементів. Необхідно вибрати такі складові елементи та їх параметри, які будуть найбільш адекватно відповідати виробничим умовам. Підхід, заснований на нечіткості вимог, забезпечує взаємозамінність альтернатив і можливість їх оптимального вибору. Число характеристичних параметрів складових мережі може перевищувати кілька десятків, а їх значення в альтернативних видах найчастіше суперечать пропонованим вимогам. Тому вибір складових елементів, здатних забезпечити досягнення найкращих показників ефективності, вимагає застосування рішень на основі нечітких множин.

Виклад основного матеріалу дослідження

1. **Розв'язання задачі визначення стану системи захисту на основі кортежа та нечітких множин**

Виконаємо наступні кроки:

1. Складання кортежа параметрів

Кортеж представлений як:

$$<I,Z,Z_p,C_v,C_k,D_i,C_{d1},C_{d2}>,$$

де кожен елемент визначає специфічний аспект захисту інформаційної системи.

I **: Потік інформації.** Визначає обсяг або частоту передачі інформації в системі.

Z **: Показник захисту інформації**. Відображає ефективність механізмів захисту.

Z_p **: Вплив заходів захисту**. Визначає, наскільки заходи безпеки впливають на загальний рівень захисту.

C_v **: Вплив швидкості витоку даних**. Чим більша швидкість витоку, тим більше загроза.

C_k **: Вплив обсягу даних на ризик витоку**. Більший обсяг даних може призводити до підвищеного ризику.

D_i **: Втрата довіри між користувачами**. Впливає на загальну стійкість системи.

C_{d1} **: Розміри системи та захищеність**. Впливає на витік інформації.

C_{d2} **: Розміри системи та захищеність**. Впливає на захищеність системи

2. Моделювання нечітких множин

Кожен параметр можна представити у вигляді нечітких множин:

Low (низьке значення);

Medium (середнє значення);

High (високе значення).

Для кожної множини задається **функція належності** ($\mu(x)$, яка відображає ступінь належності параметра до конкретної категорії.

Функції належності (приклади):

Low: $\mu(x) = 1\text{-}x$, $x \in [0,1]$. Значення $\mu(x)$ зменшується з ростом x.

Medium: $\mu(x) = \max\left(1 - |x - 0.5| \cdot 2.0\right)$. Найвища належність для $x = 0.5x$, лінійно зменшується до 0 на межах $[0,1]$.

High: $\mu(x) = x$, $x \in [0,1]$. Значення $\mu(x)$ збільшується зі збільшенням x.

3. Розрахунок рівня ризику

Визначення ризику базується на універсальній множині значень $x = [0,1]$ і нечітких множинах:

Низький ризик: Low

Середній ризик: Medium

Високий ризик: High

Приклад:

Якщо x — значення ризику (наприклад, оцінене як відношення інцидентів до загального обсягу даних), обчислюємо функції належності:

$\mu(x)Low = 1\text{-}x$;

$\mu(x)Medium = \max\left(1 - |x - 0.5| \cdot 2.0\right)$;

$\mu(x)High = x$.

Результати:

Значення $x = 0.2x$:

$\mu(x)Low(0.2) = 0.8$, $\mu(x)Medium(0.2) = 0.6$,

$\mu(x)High(0.2) = 0.2$

Висновок: Переважає низький ризик.

Значення $x = 0.7x$:

$\mu(x)Low(0.7) = 0.3$, $\mu(x)Medium(0.7) = 0.6$,

$\mu(x)High(0.7) = 0.7$

Висновок: Переважає високий ризик.

4. Оцінка загального рівня захищеності

На основі нечітких правил і результатів для кожного параметра $(Z, Z_p, ..., C_{d2})$, будуємо графік рис. 1.

Наприклад: Якщо Z **High**, а C_v **Low**, то система добре захищена. Якщо D_i **High** і C_{d1} **Low**, то загальний рівень захищеності низький.

5. Агрегація результатів

Для агрегування використовуємо **метод центру ваги**:

$$R = \sum i\mu_i(x) \cdot x_i$$

де $i\mu_i(x)$ — функція належності для параметра i, а x — значення параметра.

Висновок:

1.Формалізували кортеж.

2.Задали нечіткі множини для кожного параметра.

3.Обчислили рівні ризику.

На основі правил нечіткої логіки оцінили стан системи захисту.

Графік показує функції належності для трьох нечітких множин, що використовуються для оцінки параметрів системи захисту:

1. **Low (Низький рівень)**:

Значення функції належності ($\mu(x)Low(x)$ зменшується зі збільшенням x. Високий ступінь належності спостерігається для малих значень параметра.

2. **Medium (Середній рівень)**:

Найвищий ступінь належності ($\mu(x)Medium$ для значень, близьких до 0.5. Ступінь належності поступово зменшується до 0 при крайніх значеннях x=0, x=1.

3. **High (Високий рівень)**:

Значення функції належності ($\mu(x)High$ зростає зі збільшенням x. Високий ступінь належності характерний для великих значень параметра.

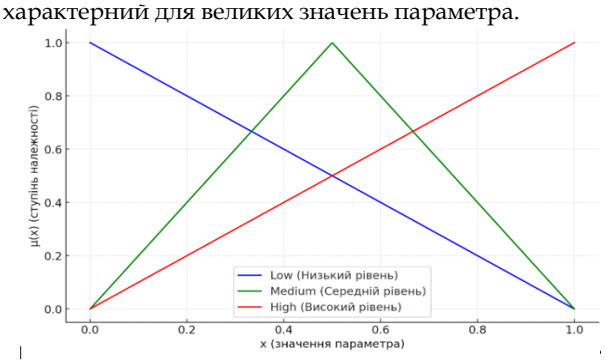


Рис. 1. Функції належності від параметрів захисту

Інтерпретація: Для кожного параметра кортежа $(Z, Z_p, ..., C_{d2})$ значення x визначає, наскільки цей параметр належить до категорій *Low*, *Medium* або *High*.

6. Функції належності

Функції належності дозволяють враховувати невизначеність у значеннях параметрів і дають можливість моделювати їхній вплив на загальний стан системи Для представлення задачі через метод трапецій або трикутника з цими параметрами, можна уявити графічне відображення залежності між елементами кортежу. Припустимо, що значення кожного параметра $<I, Z, Z_p, C_v, C_k, D_i, C_{d1}, C_{d2}>$ залежить від певної функції $f(x)$, де x — це загальний індикатор часу, обсягу чи іншого фактора.

План реалізації:

1. **Метод трапецій**: Використаємо інтегрування для оцінки загального показника захисту системи. Побудуємо площу під кривою для кожного елемента кортежу.

2. **Метод трикутника (середніх прямокутників)**: Для оцінки внеску кожного параметра у загальний показник розглянемо середні значення функції.

Формалізація. Приклад функції

$$Z = \frac{(C_v + C_k) \cdot D_i}{(C_{d1} + C_{d2}) \cdot Z_p}$$

для кожного елемента (умовно). Проведемо чисельне інтегрування для обчислення загальної ефективності системи. Потім візуалізуємо графіки (рис.2).

На графіках показані результати для кожного параметра $I, Z, Z_p, C_v, C_k, D_i, C_{d1}, C_{d2}$ при застосуванні:

1. **Методу трапецій**:

2. Площа під функцією f(x), що відповідає кожному параметру, обчислена методом трапецій. Це забезпечує більш точне наближення інтегралів.

3. **Методу трикутника (середніх прямокутників)**:

4. Використовується середнє значення функції для кожного інтервалу, що дає інший підхід до оцінки внеску параметрів.

Обидва підходи ілюструють інтегральний внесок кожного елемента в загальний показник ефективності або захищеності системи.

Щоб обчислити загальний показник Z за формулою:

$$Z = \frac{(C_v + C_k) \cdot D_i}{(C_{d1} + C_{d2}) \cdot Z_p},$$

ми використаємо чисельний підхід: метод трапецій або трикутника. Ось як це буде зроблено:

1. Алгоритм обчислення: Розіб'ємо область x на n підінтервалів. Для кожного параметра $C_v, C_k, D_i, C_{d1}, C_{d2}$ задаємо функції $f(x)$, які визначають їх залежність від часу або інших змінних.

• Обчислимо інтеграл для обчислення Z за допомогою обраного методу.

2. Метод трапецій:

Формула інтегрування:

$$\int abf(x)dx \approx h2\left[f(a) + 2\sum i\right] = 1n - 1f(x_i) + f(b)$$

3. Метод трикутника (середніх прямокутників):

Формула:

$$\int abf(x)dx \approx h\sum i = 1nf\left(x_i^*\right),$$

де $x_i^* \cdot x\_$ — середина і-го підінтервалу. Реалізуємо це чисельно і побудуємо графік. На графіку (рис. 3) представлені результати обчислення показника Z за формулою:

$$Z = \frac{(C_v + C_k) \cdot D_i}{(C_{d1} + C_{d2}) \cdot Z_p}, \text{ використовуючи:}$$

1. **Метод трапецій** — надає точніше наближення за рахунок врахування криволінійності функцій.

2. **Метод трикутника (середніх прямокутників)** — простіший метод, що використовує середні значення параметрів.

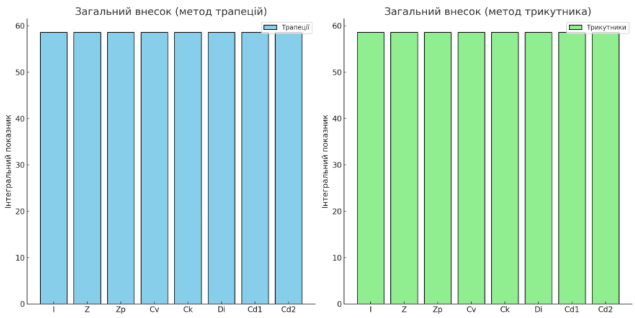


Рис.2. Інтегральний показник загального внеску складових

Результати показують, як вибір чисельного методу впливає на обчислення інтегрального показника Z.

Метод трапеції (Trapezoidal Membership Function):

Функція належності для кожного рівня Z має вигляд трапеції, визначеної чотирма параметрами (*a,b,c,d*).

Для кожного рівня Z межі *(a,b,c,d)* обрані так:

Low: (0, 0.2, 0.3, 0.4)

Medium: (0.3, 0.4, 0.6, 0.7)

High: (0.6, 0.7, 1, 1)

$$\mu(x) = \begin{cases} 0, & x < a \text{ або } x > b \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \dfrac{d-x}{d-c}, & c \le x \le d \end{cases}$$

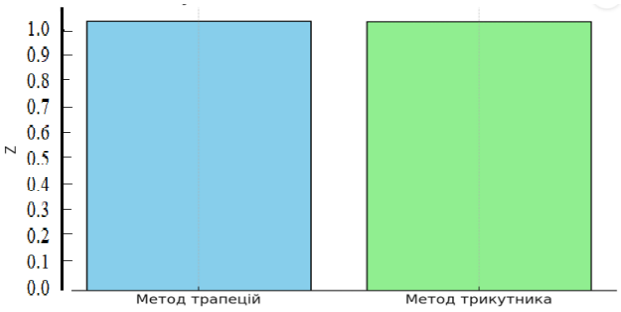


Рис. 3. Результати обчислення показника Z

2. Метод трикутника (Triangular Membership Function):

Функція належності для кожного рівня Z має вигляд трикутника, визначеного трьома параметрами *(a,b,c):*

$$\mu(x)=\begin{cases}0, & x<a \text{ або } x>c\\ \dfrac{x-a}{b-a}, & a\le x\le b\\ \dfrac{c-x}{c-b}, & b\le x\le c\end{cases}$$

Для кожного рівня *Z* межі *(a,b,c)* обрані так:

Low: (0, 0.3, 0.6)

Medium: (0.4, 0.6, 0.8)

High: (0.7, 0.9, 1)

Побудова графіків:

Графіки показують, як значення *Z* від *0* до *1* впливають на ступінь належності ($\mu(x)$ до кожного рівня.

Трапецієподібні функції відображають поступовий перехід між рівнями.

Трикутні функції є більш різкими і підкреслюють точковий перехід між рівнями.

На основі цих функцій побудовані дві серії графіків для порівняння рис. 4.

Результати розрахунку *Z*:

Ось розрахунки для кожного випадку на основі формули:

$$Z=\frac{(C_v+C_k)\cdot D_i}{(C_{d1}+C_{d2})\cdot Z_p}$$

Випадок Low:

Параметри:

$C_v=0.2, C_k=0.2, D_i=0.3, C_{d1}=0.4, C_{d2}=0.3, Z_p=0.5$

Підставляємо:

$Z=(0.2+0.2)\cdot 0.3/(0.4+0.3)\cdot 0.5=0.4\cdot 0.30/0.7\cdot 0.5=$
$=0.120/0.35=0.34$

Випадок Medium:

Параметри: $C_v=0.5, C_k=0.5, D_i=0.5, C_{d1}=0.5, C_{d2}=0.5, Z_p=0.8$

Підставляємо:

$Z=(0.5+0.5)\cdot 0.50/(0.5+0.5)\cdot 0.8=0.625$

Випадок High:

Параметри:

$C_v=0.8, C_k=0.7, D_i=0.9, C_{d1}=0.6, C_{d2}=0.8, Z_p=1.$

Підставляємо:

$Z=(0.8+0.7)\cdot 0.90/(0.6+0.8)\ 1=1,35/1,4=0,96$

Висновки:

Low: *0.34*

Medium: *0.625*

High: *0.96*

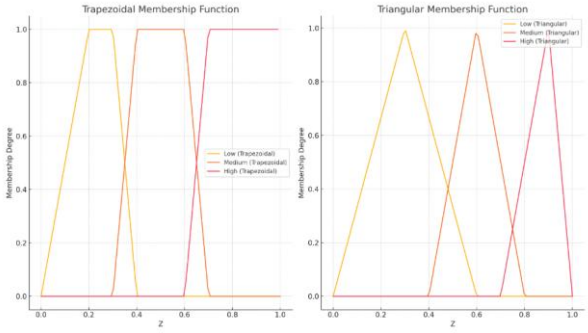


Рис. 4. Вплив значень Z на ступінь належності (μ(x) до кожного рівня

На графіках можна побачити функції належності для кожного рівня *Z*, використовуючи методи трапеції (ліворуч) та трикутника (праворуч). Ці функції відображають, як значення *Z* співвідноситься з рівнем захисту (Low, Medium, High).

Висновки

З рис. 1 видно, як саме показники складових мережі впливають на систему захисту. Чим більший рівень показників тим вище показник захисту інформації.

З рис. 2 ,3 (метод трапецій та трикутника) слідує, що показники складових захисту значно впливають на захист інформації.

На рис. 4 представлено вплив значень Z на ступінь належності ($\mu(x)$ до кожного рівня. Чим більше перекриття, тим більше сумарне значення початкових інтервалів, що відображаються у верхній основі трапеції для яких $\mu(t_1)=1$. Цей підхід дозволяє візуалізувати ступінь впевненості експерта в належності значень до обраного прийнятного показника захисту інформації в мережі та відобразити цю впевненість на підставі графіків і відповідних розрахунків, що наведені в статті. Таким чином, запропонований метод розрахунку показника захисту в якому за рахунок реалізації процедур визначення показника захисту для отримання трикутних та трапецієподібних показників, що відображають значення впливу складових мережі. Розроблений метод надалі може ефективно використовуватись для вирішення задач кібербезпекового оцінювання на мережевих об'єктах.

Список літератури

[1] Korchenko A., Breslavskyi V., Yevseiev S., Zhumangalieva N., Zvarych A., Kazmirchuk S., Kurchenko O., Laptiev O., Sievierinov O., Tkachuk S., Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency, EasternEuropean Journal of Enterprise Technologies, 2021. Vol.111. №.3/9. pp. 63-83.

[2] Євсеєв С.П., Шматко О. В., Ромащенко Н.В., Алгоритм оцінювання ступеня ризику інформаційної безпеки, що базується на нечіткомножинному підході, Сучасні інформаційні системи, 2019. Т. 3, № 2. С. 73-79.

[3] Кочетков О.В., Гаур Т.О., Машін В.М., Система оцінки ризиків інформаційної безпеки підприємства на основі

нечіткої логіки, Наукові праці ОНАЗ ім. О.С. Попова. 2019., № 1. С. 97-104.

[4] Корченко А.О., Методи ідентифікації аномальних станів для систем виявлення вторгнень, Монографія, Київ, ЦП «Компринт», 2019, 361 с.

[5] Корченко О.Г., Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017, 435 с.

[6] Ахрамович В.М. Модель взаємовідносин користувачів в соціальних мережах/ Сучасний захист інформації. К. ДУТ: 2019 .№3. с. 42-50.

[7] Ахрамович В.М. Моделі довіри та репутації користувачів в соціальних мережах. Сучасний захист інформації, 2019. №4 с. 45-51. https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf.

[8] Ахрамович В.М. Зв'язок та вплив користувачів в соціальних мережах/ Colloquium-journal (Warszawa, Polska). №3 (55), 2020 /Część 1. Pp. 21-25. http://www.colloquium-journal.org.

[9] Sobchuk, V., Asrorov, F., Perehuda, O., Laptiev, O., Lukova-Chuiko, N. The limited solutions method for telecommunications network information security models/ 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, P. 126–131

УДК 004.056.5(045)

Akhramovych V., Laptiev O., Ilienko A., Akhramovych V. Method for calculating information protection in social networks in the conditions of fuzzy sets

Abstract. *The current task of analyzing and managing a social network is to select such a composition of system elements and their parameters that will ensure the possibility of achieving maximum functional efficiency under conditions of uncertainty. This article studies the system for protecting a social network from network components under conditions of uncertainty. The main attention is paid to data fuzzification, building fuzzy set models, assessing risks and the level of security of network objects. The proposed approach allows developing effective solutions for making management decisions in the cybersecurity context. An algorithm for building a tuple of protection parameters and modeling them using membership functions is presented. Methods for aggregating results and calculations using trapezoidal and triangular functions are separately considered. For this purpose, the following were compiled: a tuple of fuzzy sets from network components; its modeling was carried out; risk levels were calculated; network security levels, aggregation of results, membership functions. Trapezoidal and triangular methods were used to calculate parameters. The calculations are illustrated with graphic material. The results of the work can be used by network administrators, organizations and government agencies to improve the efficiency of cybersecurity management and protection of information resources.*

Keywords: *fuzzy sets, social network components, tuple, modeling, risks, protection system, aggregation, membership function.*

Ахрамович Володимир Миколайович, д.т.н, проф., професор кафедри кібербезпеки Державний університет: «Київський авіаційний інститут».

Akhramovych Volodymyr, Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity State University «Kyiv Aviation Institute».

Лаптєв Олександр Анатолієвич, д.т.н., с. н. с., доцент кафедри кібербезпеки та захисту інформації Київського національного університету ім.Т.Шевченка.

Laptiev Oleksandr, Doctor of Technical Sciences, Senior Researcher, Associate Professor of the Department of Cybersecurity and Information Protection of the Taras Shevchenko National University of Kyiv.

Ільєнко Анна Вадимівна, к.т.н., доцент, завідувач кафедрою кібербезпеки Державний університет: «Київський авіаційний інститут».

Ilienko Anna, Ph.D., Associate Professor, Head of the Department of Cybersecurity State University «Kyiv Aviation Institute».

Ахрамович Вадим Володимирович, завідувач комп'ютерним центром Національної академії статистики, обліку та аудиту.

Akhramovych Vadym, Head of the Computer Center of the National Academy of Statistics, Accounting and Audit.