

НЕЧІТКІ МНОЖИНИ В ЗАДАЧАХ ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

Досліджено захист інформації за допомогою нечітких множин, розглянуто використання нечітких множин в захисті інформації.

Ключові слова:

Нечіткі множини; множини; захист; інформація; доступ; адаптивність.

Abstract

Protection of information with the help of fuzzy sets was studied, the use of fuzzy sets in information protection was considered.

Keywords:

Fuzzy sets; plurals; protection; information; access; adaptability.

В сучасному світі, де обсяги даних швидко зростають, потрібно їх захищати від шахраїв. Існує безліч різних видів захисту інформації, але пропонується розглянути використання нечітких множин для побудови систем захисту. Цей підхід дозволяє ефективно моделювати неоднозначність та невизначеність в обробці даних, що є невід'ємним аспектом сучасного кіберпростору.

Що ж таке нечітка множина? Розглянемо детальніше з цим твердженням. Нечіткі множини є математичною концепцією, яка дозволяє моделювати нечіткість, неоднозначність та невизначеність у даних. Ця теорія виникла в середині 1960-х років завдяки відомому математику Лотфі Заде. Її основна ідея полягає в тому, щоб розширити класичні множини, де елементи можуть або входити, або не входити, додавши ступінь належності елементів в множину, що може приймати значення від 0 до 1.

Нечіткі множини можуть бути задані двома основними способами [1]:

1. У формі списку з явним переліком всіх елементів і відповідних їм значень функції належності, що утворюють розглянуту нечітку множину[1]. При цьому найчастіше елементи з нульовими значеннями функції належності просто не вказуються в даному списку[1]. Цей спосіб підходить для задання нечітких множин зі скінченим дискретним носієм і невеликим числом елементів [1].
2. Аналітично у формі математичного виразу для відповідної функції належності[1]. Цей спосіб може бути використаний для задання довільних нечітких множин як зі скінченим, так і з нескінченим носієм [1].

Для ефективного визначення стану безпеки інформації, що зберігається та перетворюється в комп'ютерній системі, необхідно використовувати спеціальні інтелектуальні технології [2].

Нечіткі множини можна використовувати для захисту інформації ось в таких методах:

1. Адаптивність: Використання нечітких множин для розроблення систем, які будуть адаптуватися до нових загроз, а також до нових змін у системах.
2. Доступ: За допомогою нечітких множин можна контролювати рівні доступу користувачів чи працівників до систем.
3. Розпізнавання вторгнень: За допомогою нечітких множин можна моделювати атаки чи поведінки «користувачів».

Побудова нечітких моделей для оцінювання рівня захисту інформації в комп'ютерних системах може включати в себе використання експертних знань і методів, таких як матриця СААТІ (Суперечливості, Аналогії, Абстракції, Трансформації, Інтеграції).

Включення експертів у процес оцінювання рівня захисту є одним із ключових етапів. Експерти зазвичай надають цінні знання про потенційні загрози, слабкі місця та заходи захисту [3]. Матриця СААТІ - це інструмент, який допомагає експертам вирішувати проблеми або приймати рішення. За її допомогою можна розглядати проблему з різних точок зору, розглядаючи нові зміни, альтернативи для знаходження оптимального рішення. Основна ідея полягає в тому, щоб ранжувати альтернативи за допомогою парних порівнянь за кожним критерієм. Для цього використовується числова шкала, наприклад, від 1 до 9, де 1 означає, що два варіанти мають рівну важливість, а 9 означає, що один варіант значно важливіший за інший (таб.1.1).

Оцінка значимості	Якісна оцінка	Примітки
1	Однакова значимість	Альтернативи мають однаковий ранг
3	Слабка перевага	Перевага однієї альтернативи перед іншою (менш переконливою)
5	Сильна перевага	Існують надійні докази істотних переваг однієї альтернативи
7	Очевидна перевага	Існують переконливі докази в користь однієї альтернативи
9	Абсолютна перевага	Докази на користь переваги однієї альтернативи більші ніж над іншою альтернативою
2, 4, 6, 8	Проміжні значення	Використовуються, якщо необхідний компроміс

Таблиця 1.1 – Числова шкала значимості

Результатом попарних порівнянь альтернатив є матриця попарних порівнянь альтернатив $A_1 \dots A_n$ виду :

	A_1	A_2	...	A_j	...	A_n
A_1	a_{11}	a_{12}	...	a_{1j}	...	a_{1n}
A_2	a_{21}	a_{22}	...	a_{2j}	...	a_{2n}
...
A_i	a_{i1}	a_{i2}	...	a_{ij}	...	a_{in}
...
A_n	a_{n1}	a_{n2}	...	a_{nj}	...	a_{nn}

Рис.1 – Результат попарних порівнянь

Наприклад, на основі виявлених суперечностей експертами можна визначити нечіткі категорії для рівня захисту та встановити правила, які будуть враховувати аналогії в системі безпеки.

Висновки

Отже, нечіткі множини – це інструмент, який дає багато можливостей не тільки для дискретної математики, а й для захисту інформації. Саме використання нечітких множин у захисті інформації є показником новітнього способу. Їх використання дозволяє створити системи, які здатні ефективно працювати з різноманітністю та невизначеністю даних, що є важливим умовою для забезпечення високого рівня безпеки в сучасному світі інформаційних технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Н. Р. Кондратенко, А. В. Остапенко-Боженова .РОЗДІЛИ ДИСКРЕТНОЇ МАТЕМАТИКИ ДЛЯ ЗАДАЧ ЗАХИСТУ ІНФОРМАЦІЇ.Вінниця ВНТУ 2022
2. НЕЧІТКЕ МОДЕЛЮВАННЯ В ЗАДАЧАХ ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ Н. Р. Кондратенко, к.т.н., доцент1 ; О. О. Манасва, магістрантка2 ; О. В. Чеборака, к.т.н., ст. викладач3 ; Вінницький національний технічний університет 1 kondrn@yandex.ru, 2 sleecery@meta.ua, 3 alch_666@yahoo.com
3. Кондратенко Н.Р. Особенности застосування функцій належності типу-2 в системах нечіткої логіки. Наукові вісті НТТУ "КПІ". 2016. №2. С.43-50. doi.org/10.20535/1810-0546.2016.2.51636

Москаленко Аліна Євгенівна- студентка групи 1BKS-226, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: moskalenkoalina56@gmail.com

Кондратенко Наталія Романівна – професор кафедри Захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: kondrn2014@gmail.com

Moskalenko Alina Evgeniivna- student of group 1BKS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: moskalenkoalina56@gmail.com

Nataliya Romanivna Kondratenko is a professor at the Department of Information Protection, Vinnytsia National University Technical University, Vinnytsia, Ukraine, e-mail: kondrn2014@gmail.com