МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Нечітка оцінка якості комплексних систем захисту інформації»

Завідувач випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Барченко Н.Л.**

Студента групи КБ - 71 **Сєдих Ю.М.**

СУМИ 2021

ЗМІСТ

РЕФЕРАТ

Записка: 51 сторінок, 30 рисунків, 24 використаних джерел інформації.

Об’єкт дослідження — Нечітка оцінка якості комплексних систем захисту інформації.

Мета роботи — є розробка моделі оцінювання захищеності ІКС державних органів з використанням методів тестування на проникнення та апарату нечіткої логіки, та розглянути моделі нечіткого логічного виводу.

Результати — в даній роботі було розроблено нечітку модель оцінки якості комплексних систем захисту інформації (КЗСІ). Був проведений математичний опис завдання оцінювання захищеності ІКС. Система критеріїв оцінки задана ієрархічною структурою, яка містить інформацію щодо критеріїв, відношень між ними та множини складових елементів критеріїв. Було розглянуто система нечіткого логічного виведення для оцінки інтегрального показника відповідності. Був розглянутий Fuzzy Logic пакету Matlab, який дозволяє нам створювати системи нечіткого логічного виведення і нечіткої класифікації в рамках середовища MatLab. Також, була розроблена система нечіткого логічного виведення за допомогою Fuzzy Logic пакету Matlab.

ВСТУП

Стрімкий розвиток інформаційних технологій і вдосконалення комп'ютерної техніки вносить істотні зміни в усі сфери діяльності суспільства. Нові інформаційні технології, увірвавшись в наше життя та породили ряд різних проблем, в числі яких і захист інформації (ЗІ).

Проблема безпеки складна, багатогранна і пов'язана з рішенням широкого спектра завдань, орієнтованих як на забезпечення надійності так і на побудову моделей і систем оцінки стану безпеки, організацію експертиз, ефективну реалізацію криптографічних перетворень, безпеку комп'ютерних мереж.

На сучасному, етапі розвитку інформаційних, технологій все частіше для вирішення різних прикладних задач використовують математичний апарат нечітких множин (НМ). Ця тенденція вплинула на створення моделей і систем з нечіткою логікою (НЛ), спрямованих на вирішення завдань у сфері інформаційної безпеки.

Розглядаючи методи оцінки інформаційно-комунікаційних систем, варто зазначити що існує декілька підходів до оцінювання: експертна оцінка, кількісна оцінка, змішаний підхід (CRAMM, RiskWatch) та підхід заснований на нормативних документах .

Найбільш ефективним та поширеним методом є якісна оцінка інформаційних ризиків. Але так як кожен день складність інформаційних процесів не стоїть на одному місці, призводить до того, що одні і тіж методи оцінки ризиків безпеки стають не дієвими з точки зору інформаційної безпеки та витрат ресурсів.

Однією із таких оцінок є нечітка оцінка якості комплексних систем захисту інформації.

З кожним днем зміни які відбуваються в законодавсті нашої країни призводить до того, що Україна переходить до міжнародних стандартів в сфері забезпечення захисту інформації в інформаційно-комунікаційних системах державних органів і об’єктів критичного призначення. Але перехід до новітньої нормативної бази призвів до того, що нормативна база створюється на основі нормативних документі минулих років. З цього виникає потреба розроблення нових підходів до оцінки захищеності ІКС. Одним із таких підходів є застосування методів тестування на проникнення та апарату нечіткої логіки. В даному підході відбувається тестування параметрів комплексу засобів захисту за допомогою загальнодоступних інструментів, які використовуються і зловмисниками. Після завершення даної процедури можливі три варіанти результатів, які описуються нечіткими термами: система відповідає вимогам нормативних документів, система не відповідає вимогам нормативних документів, система частково відповідає вимогам нормативних документів та потребує доопрацювання.

Внаслідок цього постає питання розробки моделі, яка б дозволяла на основі нечіткої бази знань отримати інтегральний показник захищеності.

Метою даної роботи і є розробка моделі нечіткої ієрархічної системи оцінювання профілю захищеності, яка задає множину критеріїв оцінювання та послідовність їх використання. Ця ієрархічна модель дозволяє подати процес оцінювання у явному виді та реалізувати процес перевірки критеріїв із зазначенням ступеню впевненості експерта у релевантності критеріїв оцінювання. Система буде реалізована у середовищі Fuzzy Logic Toolbox пакету прикладних програм Matlab.

РОЗДІЛ 1 ОРГАНІЗАЦІЯ СИСТЕМ ЗАХИСТУ НА ОСНОВІ ЗАСОБІВ НЕЧІТКОЇ ЛОГІКИ

На сьогоднішній день оцінювання рівня захищеності інформації визначається системою кількісних та якісних показників, які забезпечують розв'язання задачі захисту інформації на основі існуючих в державі норм та вимог. За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання отримання узагальненої оцінки 15 рівня захищеності інформації на основі методології, що враховує як кількісні, так і якісні показники оцінки [6].

Авторами запропона модель нейромережної системи оцінки рівня захищеності інформації, застосовуючи теорію нечітких продукційних моделей (мереж). Інформація про систему, її параметри, входи, виходи та стан системи може бути не надійною, не чітко визначеною та слабоформалізованою. Модель системи є універсальною, достатньо ефективною, описується мовою, близькою до природньої.

Нечіткі продукційні моделі (Rule-Based Fuzzy Models/Systems) є найбільш загальним видом нечітких моделей, які використовуються для опису, аналізу та моделювання складних, слабоформалізованих систем та процесів. Для оцінки рівня захищеності інформації можуть бути застосовані нечіткі продукційні моделі та алгоритми нечіткого висновку на їх основі.

Формально нечіткі продукційні моделі можуть бути представлені у вигляді нечітких продукційних мереж, які по своїй структурі ідентичні багатошаровим нейронним мережам, елементи кожного шару яких реалізують окремий етап нечіткого висновку в нечіткій продукційній моделі.

Запропоновано створювати нечіткі продукційні моделі системи оцінки рівня захищеності інформації адаптивними (з корекцією в процесі та за результатами їх функціонування), а також реалізовувати різні компоненти цих моделей на основі нейромережевої технології.

1.1 Організація систем захисту на основі засобів нечіткої логіки

Методологічний базис - найважливіший компонент теорії захисту. Він складається із сукупності методів і моделей,необхідних і достатніх для досліджень проблеми захисту і решення практичних завдань відповідного призначення. В зв'язку з цим особливої уваги заслуговують завдання оцінки стану безпеки інформації в КС (комплексні системи).

На підставі описаних методів логіко-лінгвіс-тичного підходу моделей і обчислювальних тільних структур пропонується методологія синтезу систем, які використовуються для визначення рівня захищеності інформції в КС. Для однозначності тлумачень дамо визначення рівня безпеки і базового експертного запиту, які використовуються при побудові методології синтезу.

Рівень безпеки - параметр, який характеризує ступінь ефективності проведених заходів і реалізованих СЗІ за поставленому завданню.

Базовий експертний запит - це оцінюючний запит експерта, характерною для певної системи визначення рівня інформації ційної безпеки в КС що до заданої множини характеристик безпеки [5].

Методологія синтезу, заснована на запропонованій Л. Хоффманом загальної послідовності вимірювання рівня безки, містить наступні етапи:

1) Визначення характеристик безпеки інформації

Оцінюючи рівень захищеності інформації, потрібно визначити, які з характеристик безпеки повинні бути забезпечені в оцінюваної КС. Як зазначалося, відомо три характеристики безпеки: конфіденційність, цілісність і

доступність. Практика показує, що в КС, призначених для обробки даних, не для всієї інформації необхідно забезпечення всіх характеристик, наприклад, для відкритої інформації не потрібно забезпечувати конфіденційність. Тому для організації систем оцінки, необхідно визначити необхідний набір характеристик.

2) Аналіз загроз

Здійснюється аналіз можливих загроз Y_j (j=1,i , де i- кількість загроз) інформації та аналізирується їх вплив на раніше визначені характеристики безпеки. Далі визначається безліч загроз, службовців вхідний інформацією для формування експертних запитів. Такими погрозами, наприклад, можуть бути апаратні збої і відмова, логічні бомби, піггібекінг, помилки програмування, які впливають на всі характеристики безпеки [3].

3) Визначення базового експертного запиту

На підставі кожної сформованої загрози і внутрішніх факторів (які враховують конфігурацію і технологію обробки інформації в оцінюваної КС) з формувачів ВД ФВ $Д_j$ (j=1,i) надходять масиви даних $ВД_{11}$… $ВД_{1k}$, $ВД_{21}$… $ВД_{1m}$, $ВД_{il}$… $ВД_{ip}$, (Де i - кількість загроз в сформованому вище безлічі; k, m і p - кількість складових запиту першої, другої і i-й загроз відповідно), службовці компонентами вектора запиту.

Компонентом вектора запиту може бути, наприклад питання: "Час то Ви оновлюєте резервні копії, які зберігаються за межами організації?", - а внутрішнім фактором може служити, наприклад, домінуюче використання замовленого програмного забезпечення під час обробки інформації в КС.

4) Ранжування ВД

Складові базового експертного запиту упорядковуються за ступенем небезпеки загроз. Ранжування виконується через обчислення $КВ_1$… $КВ_n$ (Де n - кількість компонентів експертного запиту), які використовуються для реалізації нечітких моделей. Ідеальним є випадок, коли всі загрози рівноцінні, однак в

реальному житті існують більш і менш небезпечні. Методи ранжирування дозволяють виявити найбільш небезпечні загрози для того, щоб потім розставити необхідні акценти під час оцінювання [5].

Найбільш зручно використовувати методи ранжирування, побудовані на підставі матриці парного порівняння і дельфійських списків, які дозволяють порівняти два елементи, ігноруючи інші, що істотно полегшує процес прийняття рішення.

5) Формування лінгвістичних термів

Для визначення ЛЗ "Рівень безпеки" (РБ), відповідної кортежу <РБ, $T_{РБ}$, $X_{РБ}$>, необхідно поставити її базове терммножество $T_{РБ} = \{T_i\}$ ((i = l,L, де L - кількість термів, які використовуються в якості нечітких еталонів оцінюваних параметрів) [8].

Базове терммножин такий ЛЗ, наприклад, можна визначити п'ятьма термами:

$$T_{РБ} = \bigcup_{i=1}^{5} T_{РБ} = \{$$ "Низький" (н), "нижче середнього "(нс)," середній "(с)," вищий за середній "(вс)," високий "(в)}

Після визначення термів необхідно задати універсальне безліч $X_{РБ}$ на якому буду, визначені ці нечіткі еталони і відповідно до класифікації побудувати їх ФН.

6) Вибір методу обробки НЧ

Вибір методу грунтується на: можливості обробки певного класу НЧ; параметрах, пов'язаних з швидкодією; економічністю ресурсів; інформативністю отриманого результату. Випадку проведення попередньої експрессоценкі доцільно для виконання операцій використовувати ВМ, що дозволяє (порівняно з іншими методами) зменшити розмірність масивів оброблюваних даних, підвищити швидкість і заощадити використовувані обчислювальні ресурси [6].

7) Вибір нечіткої моделі

Залежно від способу представлення ВД, (шкали), формату ВД і швидкодії вибирається одна з нечітких моделей. Модель НМЛШ дозволяє будувати відносини між оцінюваними параметрами в лінгвістичному вимірі, а НМБШ реалізує безпосередньо кількісну оцінку на безперервній, варіативної N-бальною шкалою. Модель з бальною шкалою менш наочна і точна, але більш швидкодіюча.

8) Обчислення та інтерпретація рівня безпеки інформації

Отриманий Результати інтерпретації через визначений відповідним виміряти ного рівня безпеки еталонних значень, полученньж на етапі формування лінгвістичних термів. Вихідні дані предсталені як в лінгвістичній формі, так і в числовий у вигляді НЧ рівнів. На підставі запропонованої методології синтезу можна будувати як програмні, так і програмно-апаратні системи реального часу, призначені для ефективної оцінки рівня безпеки інформації в КС.

1.2 Система оцінки стану безпеки на лінгвістичних і варіативних бальних шкалах

Система містить підсистеми первинної обробки даних ($ППО_i$, i=1,N) об'єднаних через обчислювальну мережу, і підсистему вторинної обробки (ПВО), що складається з программного і апаратного ядра, інтегрованих інтерфейсним з'єднанням, для забезпечення конфіденційності трафіку і швидкодії обміну даними все підсистеми з'єднуються через криптографічний пристрій (КП).

Підсистеми $ППО_i$ містять інтерфейсні блоки (ІБ) моделей НМЛШ і НБМШ, блок настройки шкали (БНШ), інтерпретатори лінгвістичної і бальною шкал (ІЛШ і ІБШ відповідно), а також блок збору локальних даних (БСЛД, призначений для зберігання інформації, отриману, наприклад, в результаті відповідей користувачів на експертний запит [5].

Користувачеві пропонується використовувати одну з шкал оцінки: лінгвістичну або бальну, підготовлену за допомогою БНШ. Інтерпретатори шкал формують результат для подальшої обробки з урахуванням вибору однієї з нечітких моделей. Для моделей НМЛШ і НМБШ - це відповідно формування НЧ Z_t , t = 1,N і кількості балів X_j^* (j = 1,n) по кожному з компонентів запиту [4].

Логіко-лінгвістична нечітка підсистема (ЛЛПН), яка складає основу програмного ядра, містить:

- блок формування вихідних даних (БФВД), отриманих на підставі інформації від систем $ППО_i$;
- блок ранжирування вихідних даних (БРВД) експертного запиту, в якому обчислюються КВ PN_j;
- формувач еталонів параметрів (ФЕП), призначений для побудови ФП μ_i, i = 1, L еталонних НЧ на підставі прийнятих експертами рішень про кількість і вигляді еталонів;
- керуючий блок (КБ), що дозволяє за допомогою керуючих впливів здійснювати обробку по одній з нечітких моделей.

Блок НМЛШ визначає показник рівня захищеності даних і отриманих вихідних даних.

Блок НМБШ виконує перерахунок параметра X_j^* , j = 1,n (кількість балів) до відповідного елемент універсальної множини U_j^* і обчислення ФП μ_i^j (U_j^*), а також формує показник рівня безпеки інформації μ_S (X_j^*). [3]

Блок формування результатів (БФР) визначає виміряний рівень безпеки інформації. Функцію архіву системи виконує блок перетворення і накопичення даних (БПНД), призначений для архівного зберігання всіх отриманих даних, на підставі яких за допомогою блоку відображення та аналізу (БВА) можна простежити динаміку зміни виміряного рівня безпеки інформації.

Основу апаратного ядра складають високопродуктивні обчислювальні структури, призначені для підвищення швидкодії роботи всієї системи оцінки, Зазначені структури представляють собою нечіткі обчислювачі $НВ_1$, $НВ_2$, і $НВ_3$, (пов'язані з інтерфейсним з'єднанням через шинні формувачі), які виконують НАО по методам ЛАЛМ, ВМ і АУМ відповідно і містять масив ММУ, Осередки, структурних схем яких призначений для видалення і зберігання компонентів НЧ з можливістю попередньої установки для завдання критерію сортування [6].

Для ефективної реалізації НАО методами ВМ і АУМ використовується ММС. Це пристрій виконує максмінную композицію двох НЧ, об'єднуючи, сортуючи і відсікаючи отримані компоненти для приведення результату до розмірності ВД.

1.3 Алгоритмічне забезпечення системи оцінки

Для забезпечення функціонування систем оцінки стану безпеки необхідна алгоритмічна база, яка містить ряд нечітких алгоритмів, які за визначенням є послідовністю нечітких операторів (що містять, принаймні, одне НЧ, функцію, відношення, змінну або інші розмиті поняття), що призводять до нечіткого (в повному обсязі певного) вирішення поставленого завдання.

Ці алгоритми виконують обробку нечітких ВД і використовуються, наприклад, для побудови систем оцінки рівня ризику втрати певних ІР. До них відносяться алгоритми:

- формування L_j і LS для НМЛШ;
- визначення d (X, Y) і d_{min} для НМЛШ;
- обчислення ФП нечіткого терма і показника ризику для НМБШ;
- виконання НАО за методом ЛАЛМ.

Найбільш вагоме значення при побудові систем оцінки рівня ризику втрати ІР використовує алгоритм, який реалізує НАО по метолу ЛАЛМ [3].

1.4 Методологія синтезу систем оцінки рівня гарантій

На особливу увагу під час проведення експертизи ТЗІ на АТС заслуговує питання перевірки виконання нормативних гарантій захищеності інформації з метою оцінки УД до коректності реалізації системи ТЗІ.

Однак при практичному використанні існуючих стандартів експерти не завжди можуть чітко детермінувати оцінювані параметри, оскільки їх часто представляє в якісній формі. До того ж, методика якісного оцінювання АТС описана лише в загальному і немає реального інструменту для її конкретної реалізації.

Тому, особливий інтерес представляють моделі і системи, які дозволяють ефективно проводити експертизу (з урахуванням якісної оцінки), а також здійснювати вибір найкращого варіанту АТС, використовуючи інтегроване значення УГ захищеності ІР отримане на базі методів і моделей НМ. Такі системи дозволяють визначати УГ забезпечення захищеності ІР і вибирати альтернативи на підставі експертних оцінок еталонів параметрів і нечітко визначених ВД розробників і експертів, представлених різними показниками як в кількісному, так і в лінгвістичній формі.

Оцінка на програмно-керованих АТС

На програмно-керованих АТС оцінюванню підлягають коректність реалізації СТЗІ і РД до коректності її реалізації, куди входить і оцінка ДО. Процес оцінювання РД складається в основному в послідовному перегляді результатів і умов розробки, виготовлення випробувань, що оцінюється АТС на відповідність заданим в критеріям довіри. Перелік, зміст і форма необхідних для аналізу документів, рівень деталізації, обгрунтувань і доказів, прикладених заявником до

різних аспектів реалізованої на АТС СТЗІ, однозначно залежать від заявленого УД до коректності реалізації системи захисту. Ця залежність відображена у відповідних вимогах.

Гарантії специфіковані п'ятьма аспектами:

- гарантії безпеки середовища персоналу;
- гарантії стандартизації технологічного середовища (тс);
- гарантії забезпечення наочності і керованості ТЗ;
- гарантії забезпечення конфіденційності і цілісності ІР ТЗ;
- uарантія якості ДЗ.

1.5 Системи оцінки для проведення експертиз технічного захисту інформації

Згідно методологій, які ґрунтуються на логіко-лінгвістичному підході і запропонованих методах і моделях НМ, розроблена система оцінки УГ захищеності інформації в АТС і система вибору найкращого варіанту АТС щодо вимог нормативних документів з безпеки ІР АТС [5].

Структурна схема системи оцінки УГ містить: модуль обробки первинних параметрів (МОПП), модуль формування нечітких даних (МФНД), блок формування ОК (БФОК), блок встановлення відповідності (БУС) і блок формування результуючого УГ (БФР) [5].

Модуль МОПП служить для підготовки даних, заснованих на судженнях експертів для МФНД, і містить:

- блок первинних параметрів (ПП), що вводяться експертом;
- блок вибору методу формування ФП (ВМФП), де в залежності від кількості фахівців, які проводять експертизу, визначається метод формування ФП нечітких оцінок (МО або МНП);

- базу даних (БД), що містить специфікації оцінюваних аспектів, таких, як безпека середовища персоналу, якість, ДО, стандартизація ТС, забезпечення конфіденційності і цілісності ІР ТЗ, забезпечення наочності і керованості ТЗ;

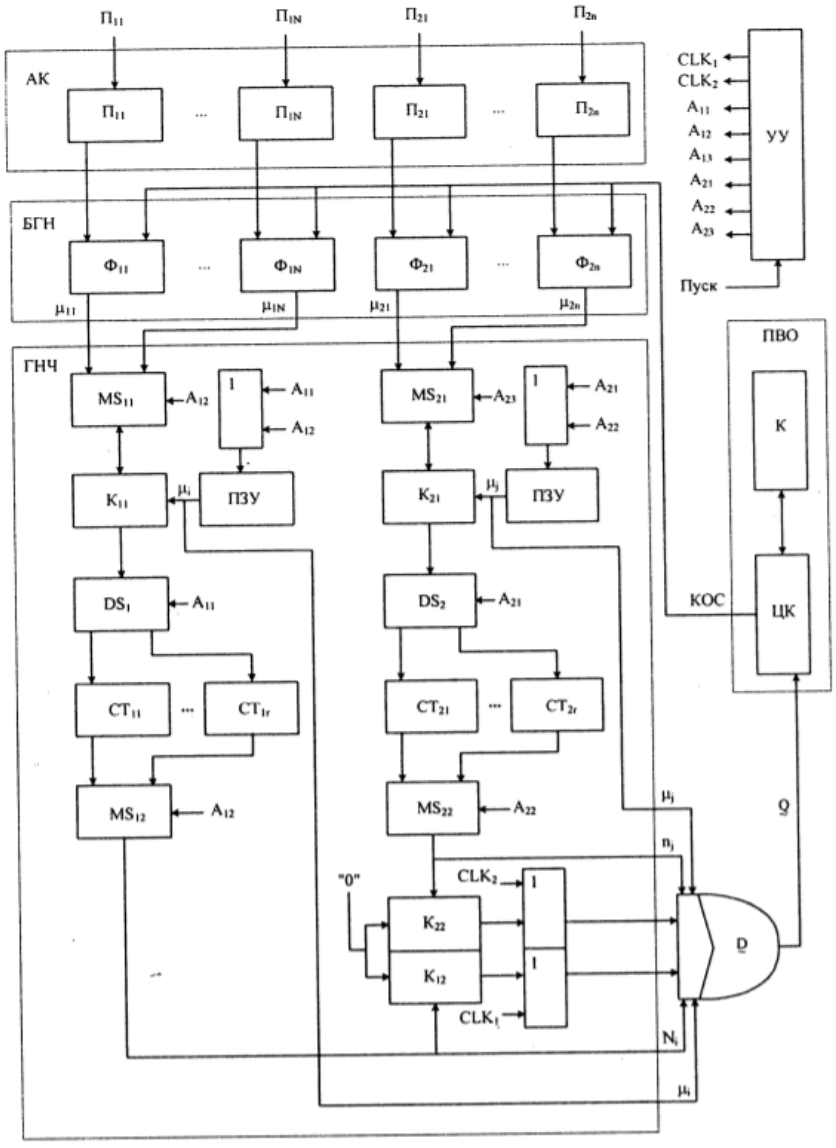

Рисунок 1. Структурна схема СОК

РОЗДІЛ 2 НЕЧІТКА ІЄРАРХІЧНА ОЦІНКА ЯКОСТІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Зміни які відбуваються кожного дня з розвитком інформаційних технологій, безпека інформації відіграє важливу роль в становленні програмного продукту.

Одним із варіантів вирішення даної проблеми є застосування методів тестування на проникнення та апарату нечіткої логіки. Під час даної процедури відбувається тестування параметрів комплексу засобів захисту за допомогою загальнодоступних інструментів, які використовуються і зловмисниками. Для проведення оцінки методом експертного оцінювання захищеності системи використовують нормативні документи, як вітчізняні так і іноземні.

Найбільш популярними міжнародними стандартами оцінки системи захисту інформації є використання стандарту ISO/IEC 15408.

Варто сказати, що відповідно до документу планове оцінювання захищеності методом тестування на проникнення повинно здійснюватися не менше одного разу на п’ять років. Проте через обмежену кількість фахівців відповідне оцінювання проводиться лише в деяких державних органах і вкрай рідко. Крім того, в вільному доступі відсутні будь-які методики, інструкції, тощо, які регламентують проведення процедури тестування на проникнення.

Проте незважаючи на різні підходи до оцінювання захищеності інформаційно-комунікаційних систем (ІКС), варто зазначити, що кожен день фахівці в сфері кібербезпеки знаходять нові вразливості в програмному забезпеченні комп’ютерних систем.

Тому навіть при якісному врахуванні всіх сучасних загроз, виборі програмних (апаратних) засобів захисту, їх коректного налаштуванні на момент

завершення процедури оцінки, система захисту з великою вірогідністю буде мати деякі вразливості.

У зв'язку зі стрімким розвитком способів, методів і інструментарію отримання несанкціонованого доступу до інформаційних систем, необхідно використовувати методи оцінки, які б з одного боку дозволяли оцінити реальний стан захищеності ІКС, а з іншого боку дозволяли підтвердити або спростувати відповідність системи захисту ІКС вимогам національного законодавства.

Тестування на проникнення – це метод оцінювання захищеності ІКС, шляхом моделювання дій зловмисників для отримання доступу до конфіденційної інформації, що в ній циркулює, порушення її цілісності або доступності. Якісно проведене тестування дозволяє визначити рівні захищеності ІКС та наявності в ній вразливостей, ідентифікувати найбільш вірогідні шляхи порушення встановленої політики безпеки і визначити наскільки якісно працює комплекс засобів захисту такої системи [24].

Отже, ми маємо концептуальні проблеми в оцінюванні захищеності ІКС, які підключені до мережі Інтернет. Можливим варіантом вирішення даної проблеми є розробка математичної моделі, яка дозволить при використанні методу тестування на проникнення з одного боку отримати деякий числовий коефіцієнт ступеню захищеності ІКС, а з іншого підтвердити або спростувати реалізацію профілю захищеності, що був визначний на етапі розробки системи захисту інформації.

Оцінювання програмного продукту відноситься до задачі класифікації, яка може бути розв'язана за допомогою методів інтелектуального аналізу даних у тому числі методів, побудованих на основі машинного навчання та розпізнавання образів. Оскільки при оцінюванні використовується якісна шкала виміру, то одним із перспективних підходів до вирішення цієї задачі є застосування ієрархічної структури критеріїв оцінювання та методів логічного виведення для

нечітких ієрархічних систем. Загальна схема таких методів складається з таких дій:

- фазифікація результатів перевірки необхідних умов та тестувань на проникнення;
- процедура нечіткого логічного виведення послідовно для кожного рівня ієрархії;
- оцінка критеріїв за принципом термометра ;
- дефазифікація результатів оцінювання.

На етапі фазифікації вхідних змінних для кожної лінгвістичної змінної визначаються відповідні лінгвістичні терми, а для кожного терма визначається функція приналежності. На цьому етапі встановлюється відповідність між вхідною змінною та функцією приналежності відповідного терма. Після завершення етапа фазифікації для всіх вхідних лінгвістичних змінних повинні бути визначенні конкретні значення функції приналежності.

Наступний етап це процедура нечіткого логічного виведення або безпосередньо нечітке виведення. На цьому етапі оцінюється значення істиності для кожного правила на основі нечітких операцій. Використовуючи один із способів побудови нечіткої імплікації, можемо отримати нечітку змінну. В логічному виведенні з використанням продукцій, вихідна функція приналежності масштабується за допомогою обчисленої степені істинності передумови правила [22].

Наступний етап, етап дефазифікація він є необов’язковим порівняно с іншими. Він застосовується тоді, коли корисно перетворювати нечіткий набір значень вивідних лінгвістичних змінних у точні значення.

Алгоритм нечіткого логічного виведення має такий вигляд.

1. Фіксується вектор значень вхідних змінних.

2. Визначається значення функцій належності термів-оцінок вхідних змінних.

3. Обчислюються функції належності термів-оцінок вихідної величини, яка відповідає вектору значень вхідних змінних.

4. Визначається оцінка, функція належності якої максимальна.

Найбільше розповсюдження є два підходи до визначення оптимального варіанту побудови КСЗІ організацій. Перший з них ґрунтується на перевірці відповідності рівня захищеності інформації в організації вимогам одного зі стандартів (законодавчих актів) у галузі інформаційної безпеки. Основний недолік першого підходу полягає в тому, що коли рівень захищеності інформації чітко не визначений визначити найбільш ефективний варіант побудови КСЗІ організації достатньо складно. Другий підхід пов'язаний з використанням методів та моделей оптимізації складних систем для визначення оптимального варіанту побудови КСЗІ. У зв’язку з цим розробка відповідних методів та моделей оптимізації показників систем захисту інформації (СЗІ) отримує особливу актуальність.

Кінцевою метою при оптимізації показників КСЗІ є забезпечення необхідного рівня інформаційної безпеки організації за різних умов конкурентної боротьби. Завдання ускладнюється тим, що пошук доводиться вести в умовах невизначеності, коли дії суперника нам не відомі і, в кращому разі, можуть бути оцінені з певною долею ймовірності. При відсутності статистичних даних, що характерно для комерційних структур, вибір параметрів розрахунку і функціональних залежностей, які входять в математичну модель, ведеться на основі експертних оцінок і вимагає розробки відповідних методів та методик.

Вирішення зазначених завдань вимагає включення до складу процедур спеціальних оптимізаційних моделей встановлюють залежність між показниками кінцевого ефекту функціонування системи і сукупності ї параметрів. Саме такий підхід може бути покладений в основу оптимізації систем захисту інформації в умовах інформаційного протиборства. Таким чином, завдання побудови оптимальної комплексної системи захисту інформації може бути вирішена на основі теоретичного (системного) підходу використовує всебічний розгляд і облік основних факторів, що впливають на ефективність системи. Під дослідженням операцій розуміють застосування математичних кількісних методів для обґрунтування рішень у всіх областях цілеспрямованої людської діяльності.

При дослідженні операцій ключову роль відіграє математична модель - умовний образ деякої системи інформаційної безпеки, який з допомогою математичних методів відображає властивості об’єктів, їх взаємозв’язків і процесів, котрі виникають при їх взаємодії. При цьому важливо дотримуватись також системного підходу, який в задачах оптимізації показників систем інформаційної безпеки проявляється в тому, що система „напад-захист” розглядається у взаємодії (протидії) її складових з врахуванням їх параметрів і характеристик. Оптимізація показників ведеться в двох напрямках - відносно загальної вартості ресурсів захисту (порівняно за вартістю інформації) і відносно розподілу цих ресурсів захисту між об’єктами, котрі відрізняються вразливістю, кількістю інформації, імовірністю нападу. Вирішення цих питань, що досягається на основі математичної моделі, являє собою доволі складну задачу, обумовлену складністю встановлення функціональної залежності між показниками системи та її параметрами і характеристиками, а також відсутність усталеної методики розрахунку цих величин. Цільова функція може включати декілька показників -

таких, як частка втраченої інформації, прибуток від інвестиції в захист інформації, їх рентабельність. Пошук вирішення ускладнюється тим, що протистояння в інформаційній сфері ведеться в умовах невизначеності, коли дії суперника невідомі і можуть бути передбачені лише з певною імовірністю на основі статистичних даних або з допомогою експертної оцінки. Таким чином, оптимізація показників складних багато рубіжних систем, якими є сучасні системи захисту інформації, є водночас важливою і складною задачею вирішення якої можливе лише шляхом розробки математичних моделей на основі системного підходу та методів дослідження операцій.

Альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ) є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності. Вони уможливлюють аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використанні теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу задач з самих різних областей [3]. Теорія нечітких мір, нечіткої логіки або Fuzzy Logic – новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу – введення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі [5].

Застосування даної технології підвищує достовірність і якість рішень, що приймаються, при суттєвому зниженні вимоги до вхідних даних (їх якості,

кількості, достовірності), формалізація яких виконується настільки точно, наскільки дозволяє їх обсяг і якість. Розроблені моделі і методи вирішення задач нечіткого математичного програмування, які адекватні сучасним умовам функціонування спеціальних об'єктів інформаційної діяльносі (СОІД), дозволяють підвищити наукову обґрунтованість, ефективність рішення, що формулюється та приймається при нечіткій вхідній інформації, збільшують аналітичну базу, надають можливість формалізації різних параметрів задачі та різноманітних цільових установок [20, 21].

Жоден окремо вибраний засіб захисту інформації не може захистити від різноманіття існуючих загроз безпеці, а проста комбінація різноманітних засобів захисту призводить до зниження рівня захисту в цілому із-за можливої конфліктності розрізнених засобів захисту. Тому останнім часом gjzdbkfcm тенденція до побудови складних комплексних систем інформаційної безпеки. Ефективність КСЗІ можна охарактеризувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози. Існують якісні і кількісні методи аналізу ефективності КСЗІ. У багатьох випадках якісних оцінок не досить, щоб відповісти на питання, наскільки надійний захист інформації. Найбільш точніші кількісні методи. Проте для того, щоб "зміряти" ефективність, необхідно мати обґрунтований критерій (показник оцінки ефективності КСЗІ).

Аналізуючи існуючи методики дає змогу зробити висновок, що цілком вірно пропонується оцінювати ефективність КСЗІ, як складну систему і характеризувати декількома частковими показниками, на підставі яких формується загальний критерій [3, 22, 24].

Таким чином для вирішення задачі оцінки КСЗІ необхідно застосовувати такий підхід, який ґрунтується на використанні принципів і правил системного аналізу, експертноаналітичного методу вирішення складних систем захисту інформації [24].

РОЗДІЛ 3 ПРИКЛАД ЗАСТОСУВАННЯ НЕЧІТКОЇ ЛОГІКИ В СЕРЕДОВИЩІ РОЗРОБКИ MATLAB

3.1 Постановка задачі

Для оцінки інформаційно-комунікаційної системи були вибрані критерії захищеності від несанкціонованого доступу, несанкціонованої модифікації, контроль оброблюваної інформації та ідентифікація і контроль за діями користувачів які визначені в існуючих національних нормативних документах. Розроблена модель нечіткої ієрархічної системи оцінювання профілю захищеності, яка задає множину критеріїв оцінювання та послідовність їх використання. Запропонована ієрархічна модель дозволяє подати процес оцінювання у явному виді та реалізувати процес перевірки критеріїв із зазначенням ступеню впевненості експерта у релевантності критеріїв оцінювання. Система була реалізована у середовищі Fuzzy Logic Toolbox пакету прикладних програм Matlab. Проведені комп'ютерні експерименти показали можливість застосування розробленої моделі на практиці.

Всі критерії захищеності діляться на такі групи:

1) Конфіденційність. Це загрози які відносяться до несанкціонованого доступу до інформації.
2) Цілісність. Загрози які відносять до несанкціонованої модифікації інформації.
3) Доступність. Це загрози які контролюють можливості використання оброблюваної інформації.
4) Спостереженість. Це ідентифікація і контроль за діями користувачів.
5) Гарантія.

3.2 Програмна реалізація.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу. Створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації. Всі критерії поділяються на групи. Структура критеріїв подана на рисунку 2. Де довірча конфіденційність (КД), адміністративна конфіденційність (КА), повторне використання об’єктів (КО), аналіз прихованих каналів (КК), конфіденційність при обміні (КВ), довірча цілісність (ЦД), мінімальна адміністративна цілісність (ЦА), мінімальна цілісність при обміні (ЦВ), стійкість до відмов(ДС), реєстрація (НР), ідентифікація і автентифікація (НИ), розподіл обов’язків (НО), цілісність КЗЗ (НЦ), ідентифікація і автентифікація при обміні (НВ), автентифікація відправника (НА), автентифікація отримувача (НП).

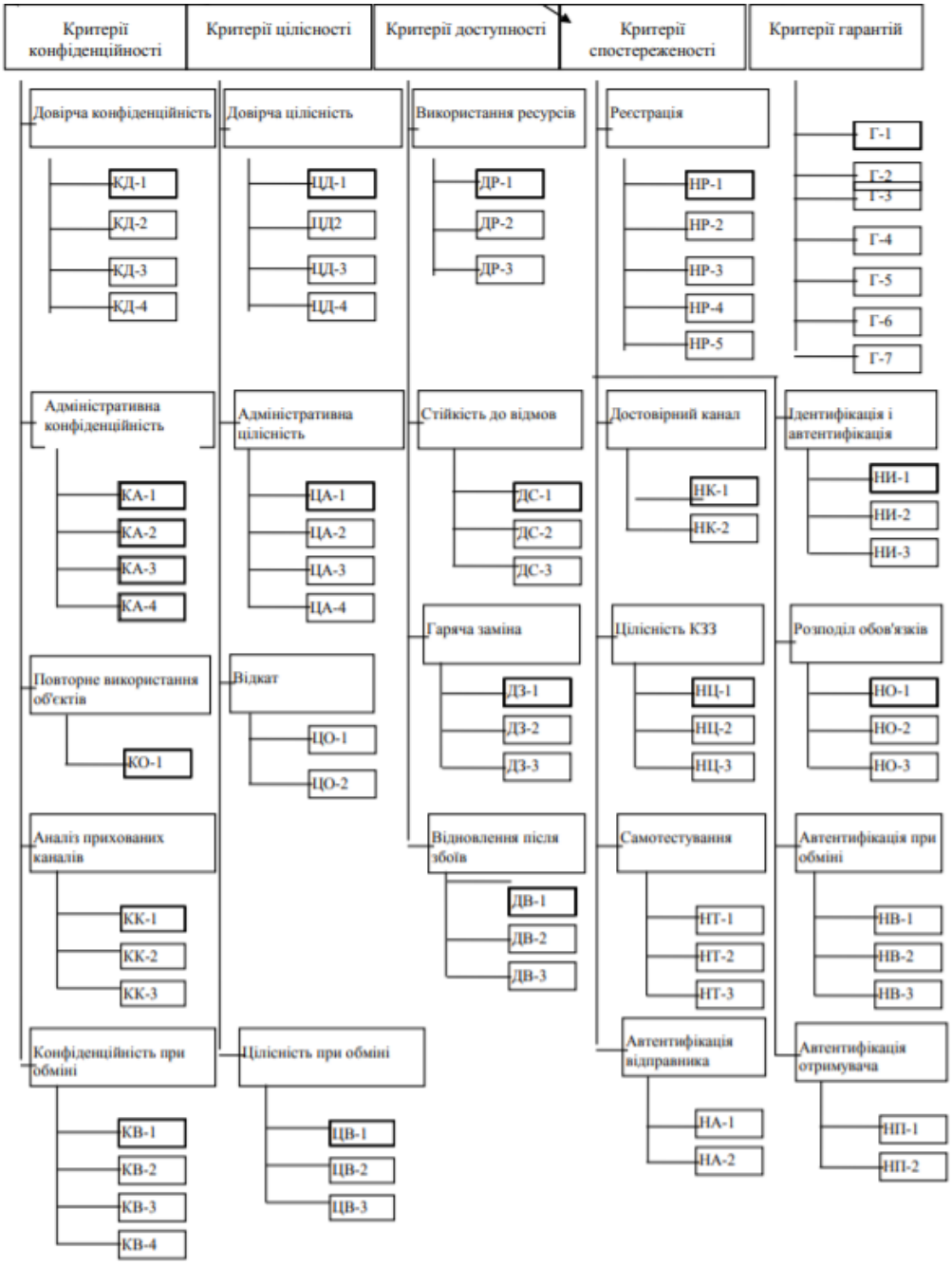

Рисунок 2. - Структура критеріїв

Оцінка конфідеційності в інформаційно-комунікаційної системі.

Створимо систему для визначення критерію конфіденційності.

Першим кроком створимо 4 вхідні та 1 вихідну змінну в системі. Задамо наші змінні:

- KD-1 – Мінімальна конфіденційність;

- KD-2 – Базова конфіденційність;
- KD-3 – Повна конфіденційність;
- KD-4 – Абсолютна конфіденційність;
- 6.1 – показник конфіденційності.

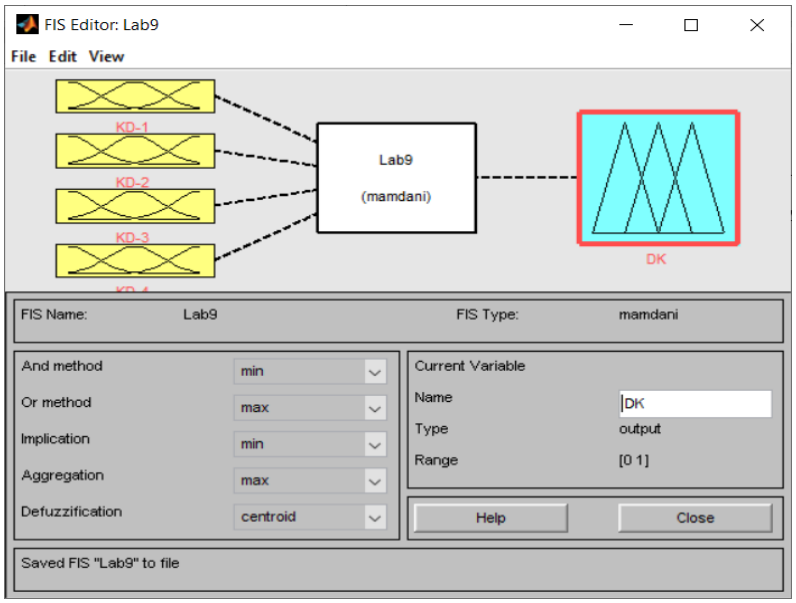

Рисунок 3. - Вхідні та вихідні змінні

Тепер відредагуємо кожну змінну. Для всіх змінних встановимо трикутну функцію приналежності з числом 3 та встановимо такі параметри [-0.4 0 0.4], [0.1 0.5 0.9] і [0.6 1 1.4]. Також змінимо назви для створених функцій на NV – не відповідає, CHV – частково відповідає та VV – відповідає.

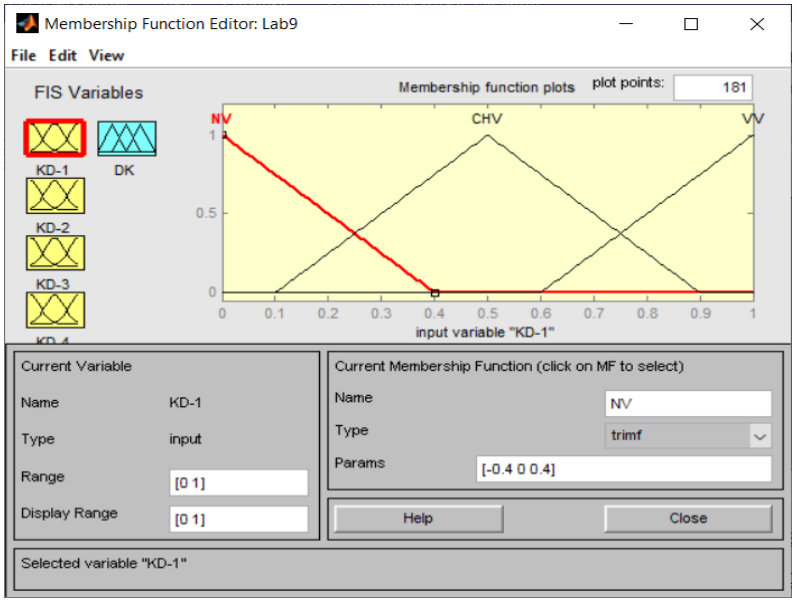

Рисунок 4. - Значень вхідних змінних

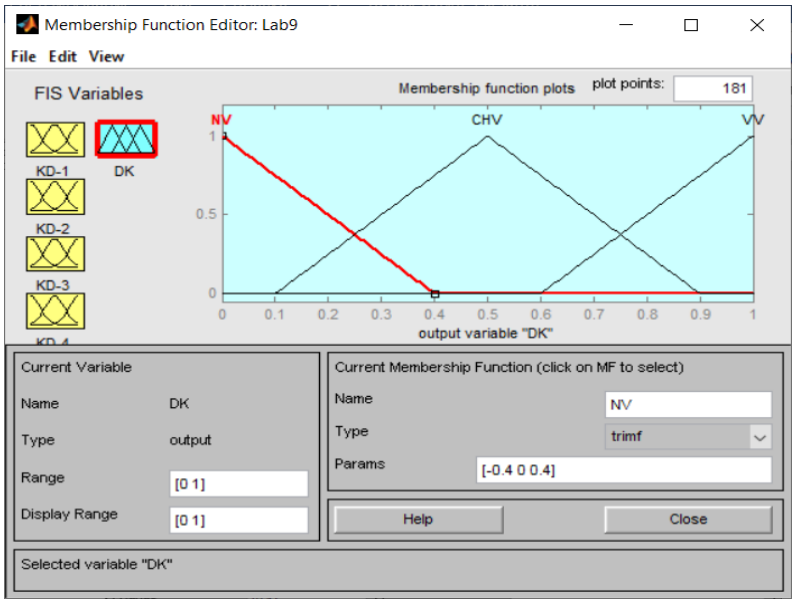

Рисунок 5. - Значень вихідних змінних

Створимо вирішальні правила для нашої системи.

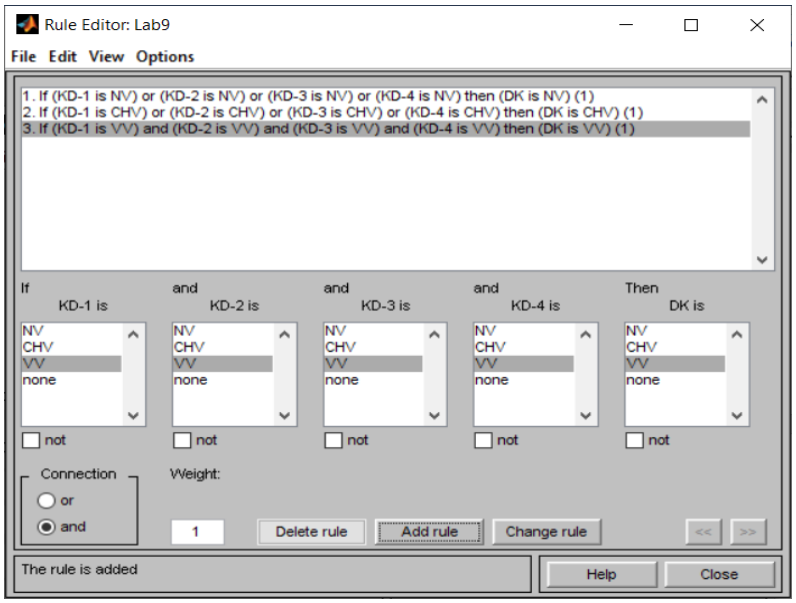

Рисунок 6. - Система продукційних правил

Після виконаних пунктів перевіримо нашу систему в дії встановивши такі значення змінних KD-1 – 0.7, KD-2 – 0.75, KD-3 – 0.9, KD-4 – 0.8. Як результат часткова довірча конфіденційність – 0.549.

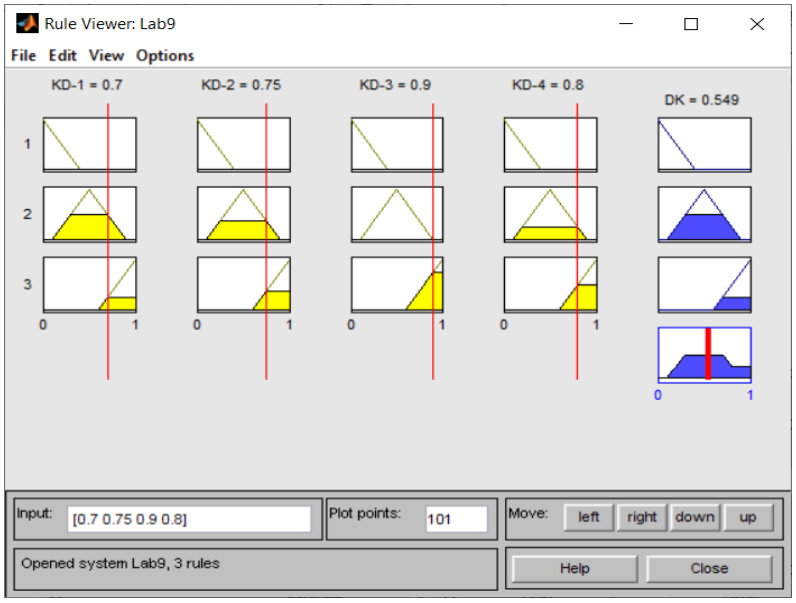

Рисунок 7. – Перевірка роботи системи

Висновок: нечітка експертна система, для оцінки критеріїв конфідеційності побудована та працює за встановленими правилами.

Оцінка цілісності в інформаційно-комунікаційної системі.

Розглянемо методику побудови нечіткої експертної системи, для оцінки критеріїв цілісності. Що має три рівні:

ЦД-1. Мінімальна цілісність;

ЦД-2. Базова цілісність ;

ЦД-3. Повна цілісність ;

ЦД-4. Абсолютна цілісність;

Так, відповідно, позначу функції входів.

Загальний вигляд нечіткої експертної системи. Зображення входів та виходів. Де E - інтегральний показник.

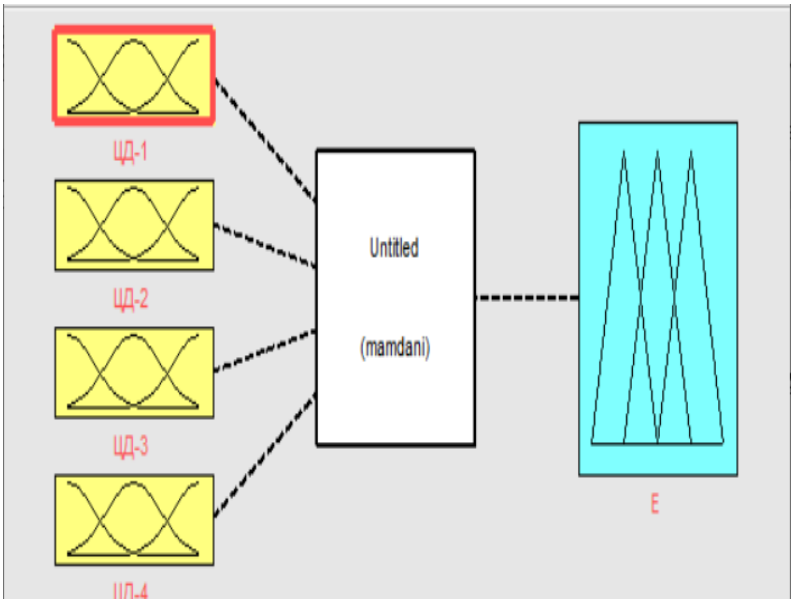

Рисунок 8. – вхідні та вихідні змінні

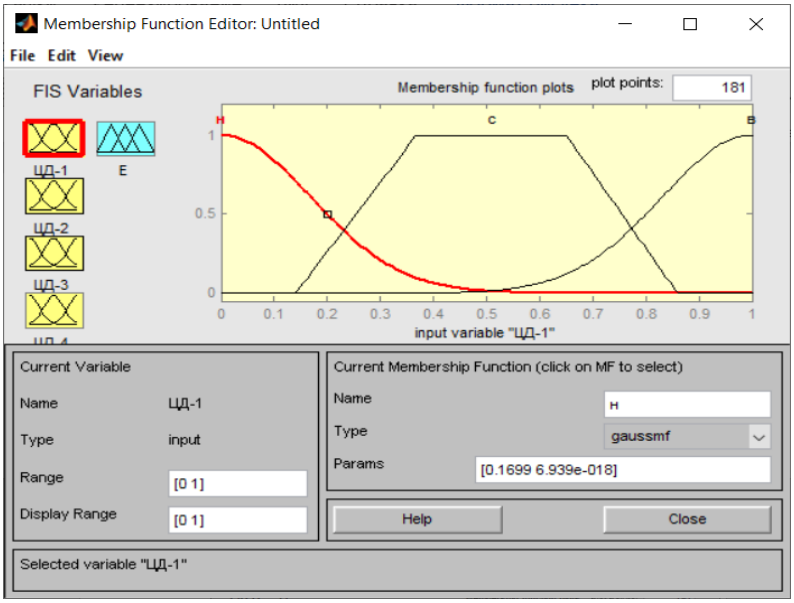

Рисунок 9. – Значення вхідних змінних

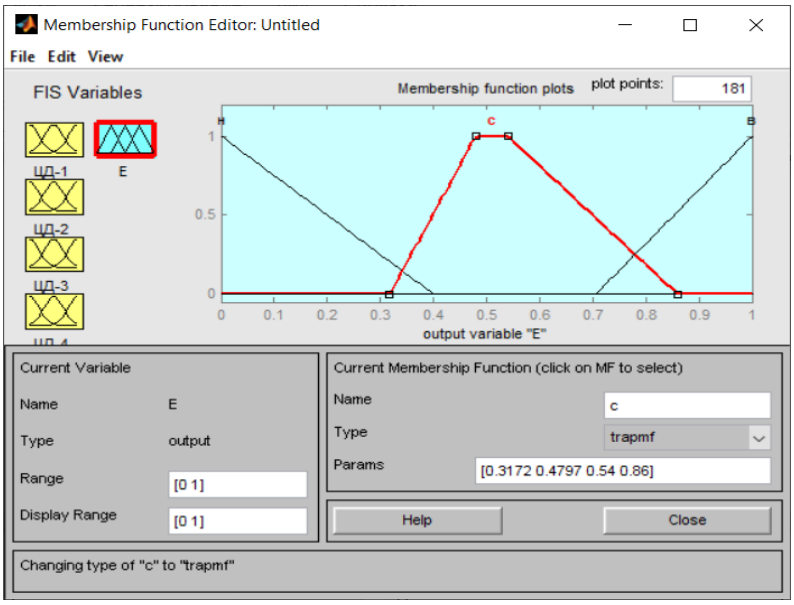

Рисунок 10. – Значення вихідних змінних

Створення правил.

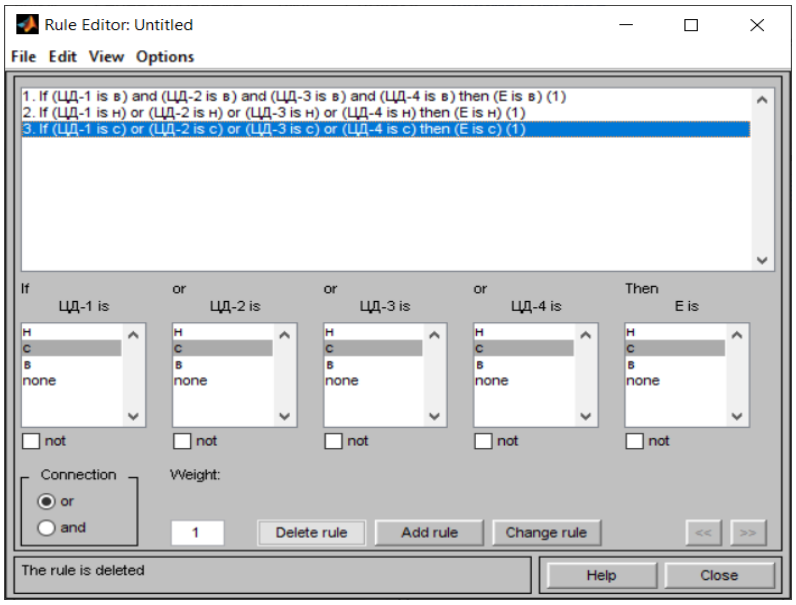

Рисунок 11. – Система продукційних правил

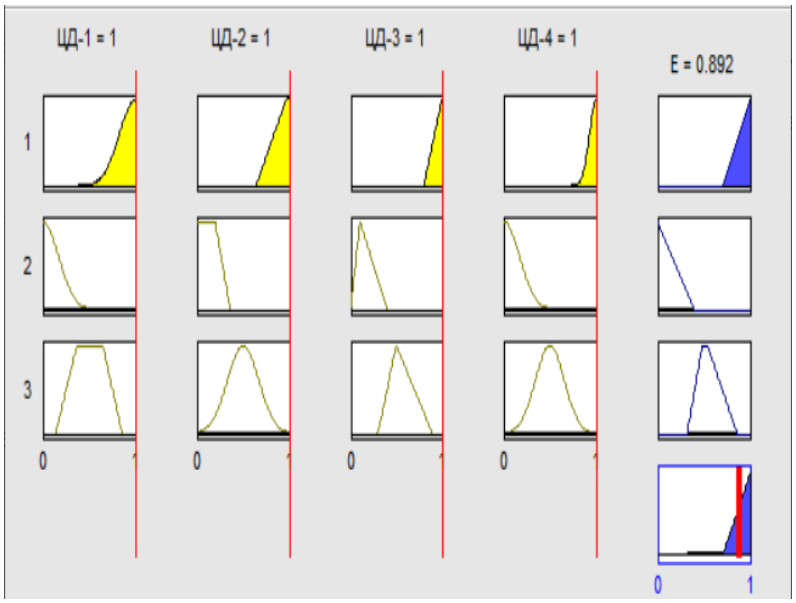

Рисунок 12. – Перевірка роботи системи

Всі критерії високі, отже цілісність забезпечується на високому рівні.

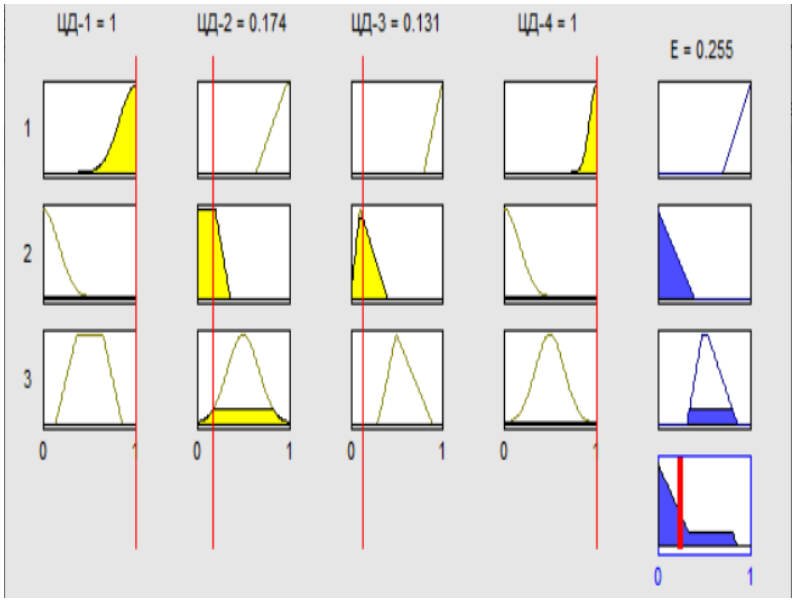

Рисунок 13. – Перевірка роботи системи

Один з критеріїв середній, отже цілісність забезпечується на середньому рівні.

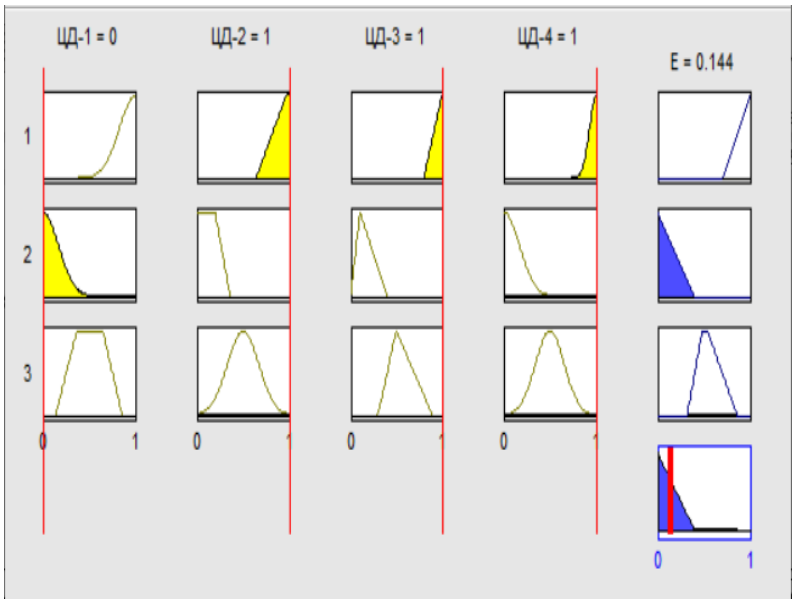

Рисунок 14. – Перевірка роботи системи

Один з критеріїв низький, отже цілісність забезпечується на низькому рівні.

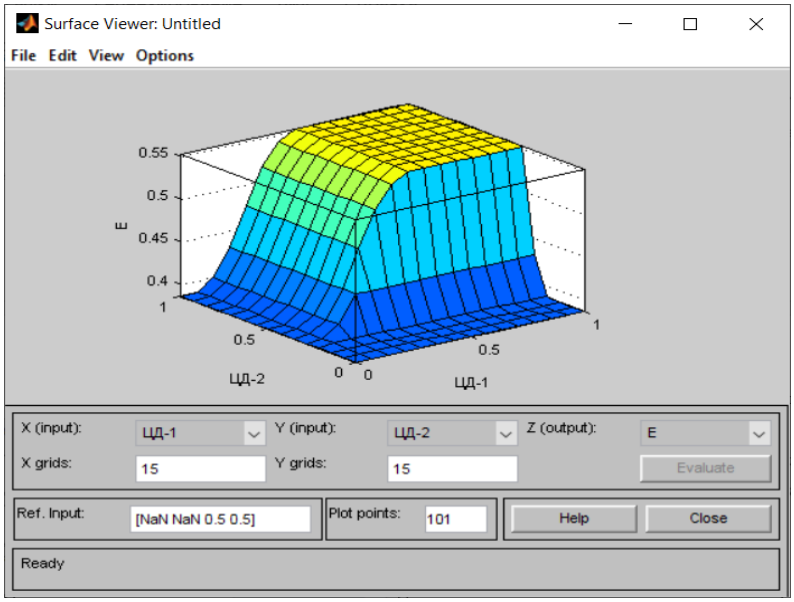

Рисунок 15. - Відображення результуючої поверхні

Висновок: нечітка експертна система, для оцінки критеріїв цілісності побудована та працює за встановленими правилами

Оцінка доступності в інформаційно-комунікаційної системі.

Розглянемо методику побудови нечіткої експертної системи, для оцінки критеріїв доступності. Що має три рівні:

Першим кроком створимо 3 вхідні та 1 вихідну змінну в системі. Задамо наші змінні:

- DR-1 – Квоти;
- DR-2 – Недопущення захоплення ресурсів;
- DR-3 – Пріоритетність використання ресурсів;
- D – показник доступності.

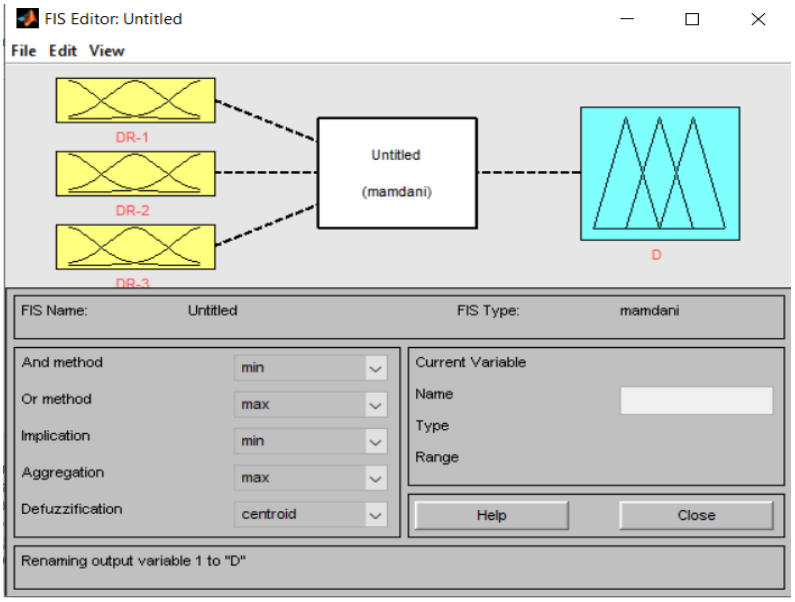

Рисунок 16. – Вхідні та вихідні змінні

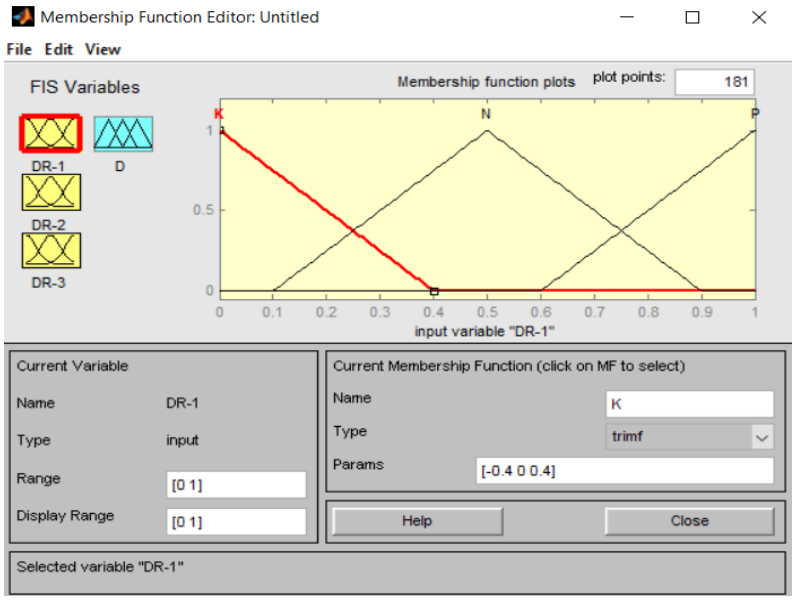

Рисунок 17. – Значення вхідних змінних

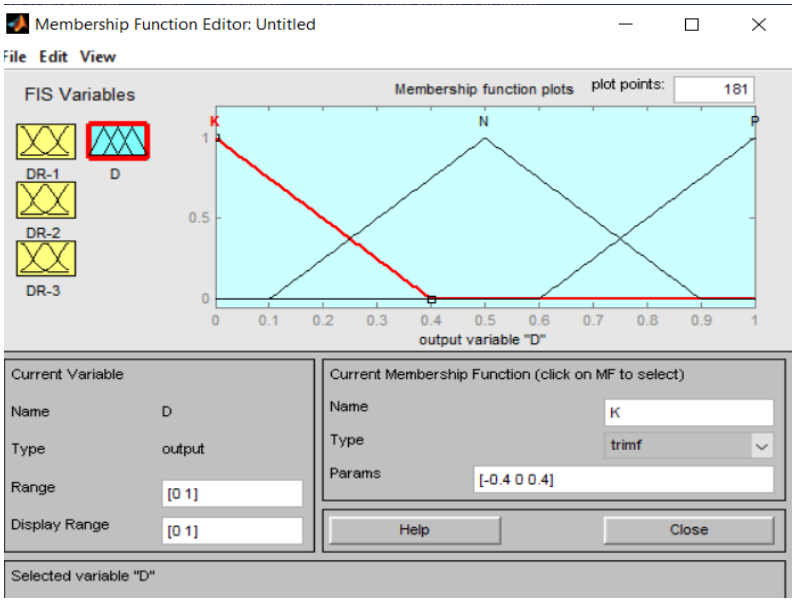

Рисунок 18. – Значення вихідних змінних

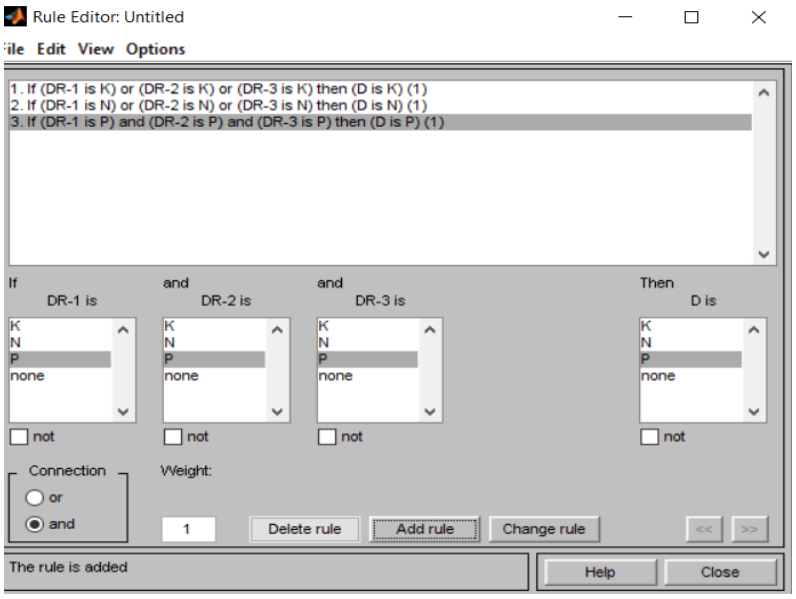

Рисунок 19. - Система продукційних правил

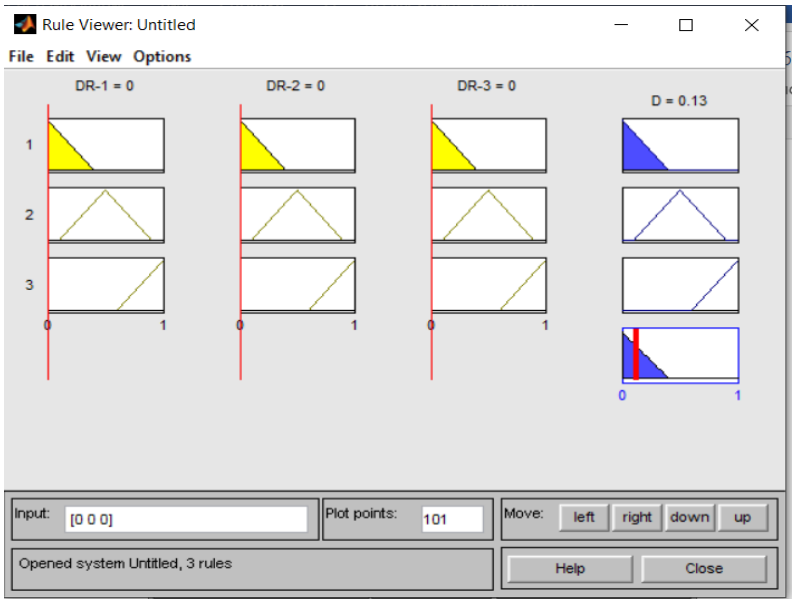

Рисунок 20. – Перевірка роботи системи

Всі критерії низькі, отже це квота.

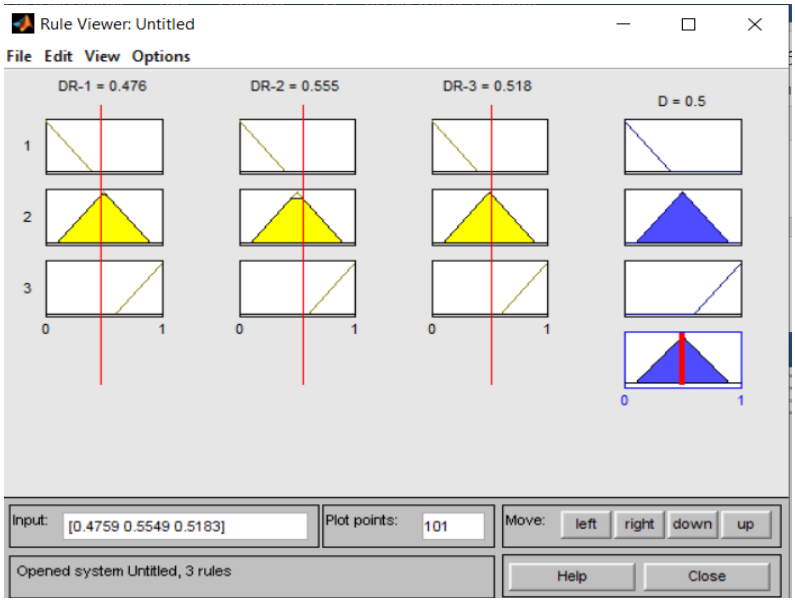

Рисунок 21. – Перевірка роботи системи

Всі критерії середні, отже це недопущення захоплення ресурсів.

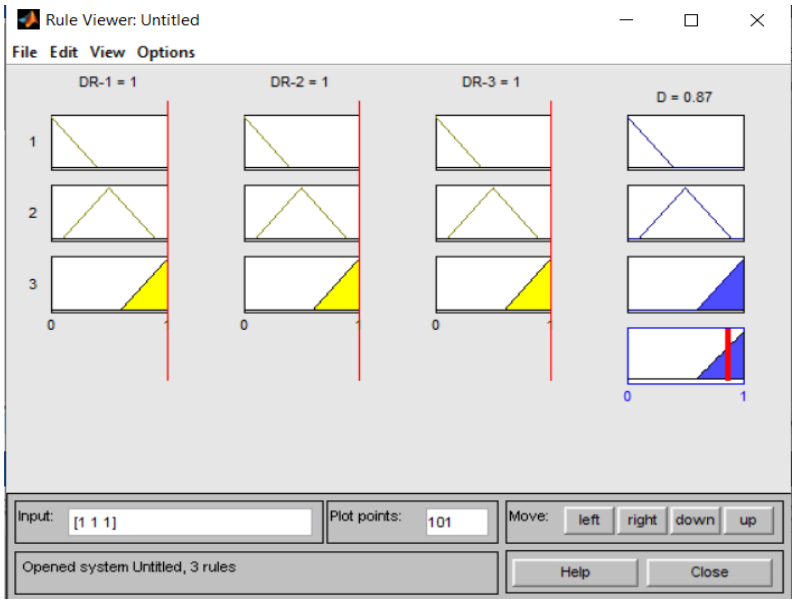

Рисунок 22. – Перевірка роботи системи

Всі критерії високі, отже це пріоритетність використання ресурсів.

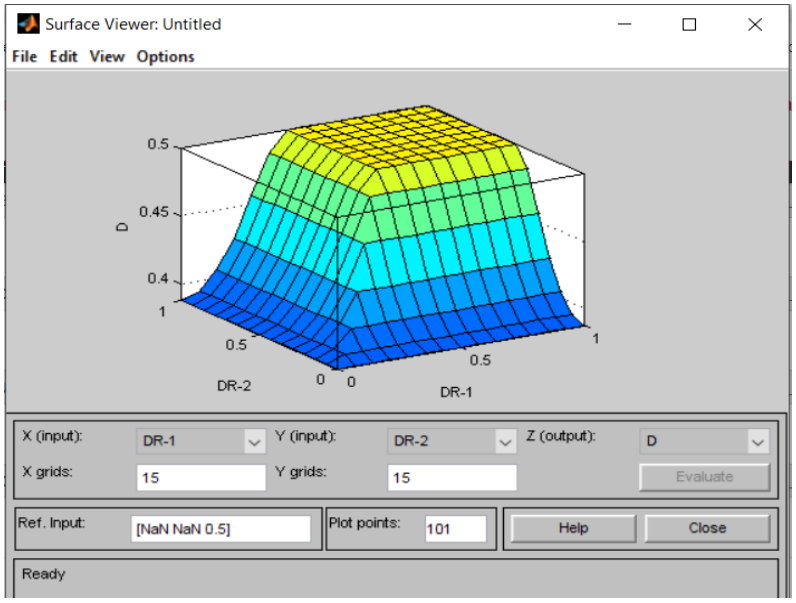

Рисунок 23. - Відображення результуючої поверхні

Висновок: нечітка експертна система, для оцінки критеріїв цілісності побудована та працює за встановленими правилами

Оцінка критерія спостереженості в інформаційно-комунікаційної системі.

Розглянемо методику побудови нечіткої експертної системи, для оцінки критерія спостереженості. Що має три рівні:

Першим кроком створимо 3 вхідні та 1 вихідну змінну в системі. Задамо наші змінні:

- NI-1 – зовнішня ідентифікація і автентифікація;
- NI-2 – Одиночна ідентифікація і автентифікація;
- NI-3 – Множинна ідентифікація і автентифікація;
- N – показник критерія спостереженості.

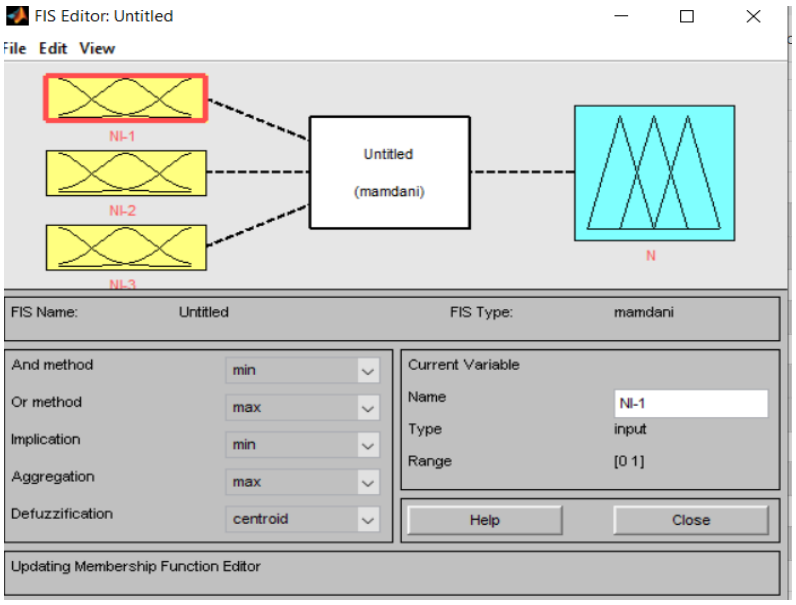

Рисунок 24. – Вхідні та вихідні змінні

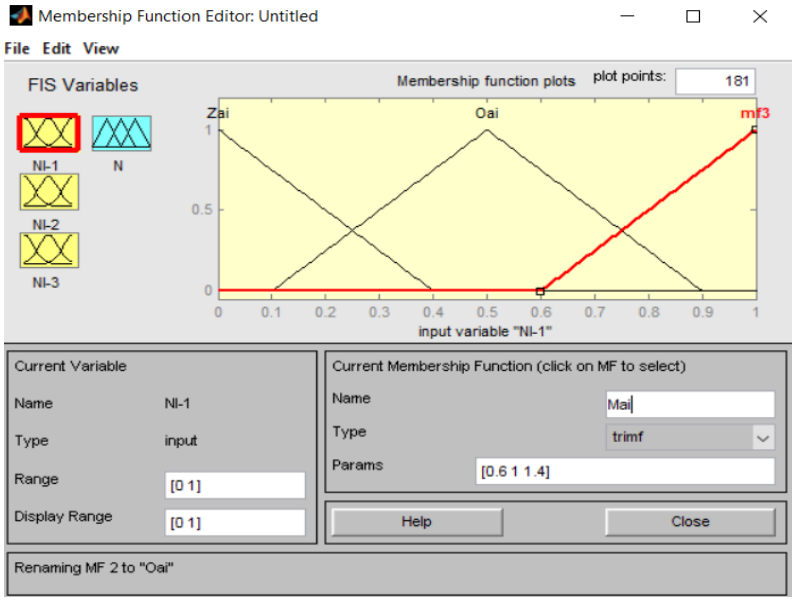

Рисунок 25. – Значення вхідних змінних

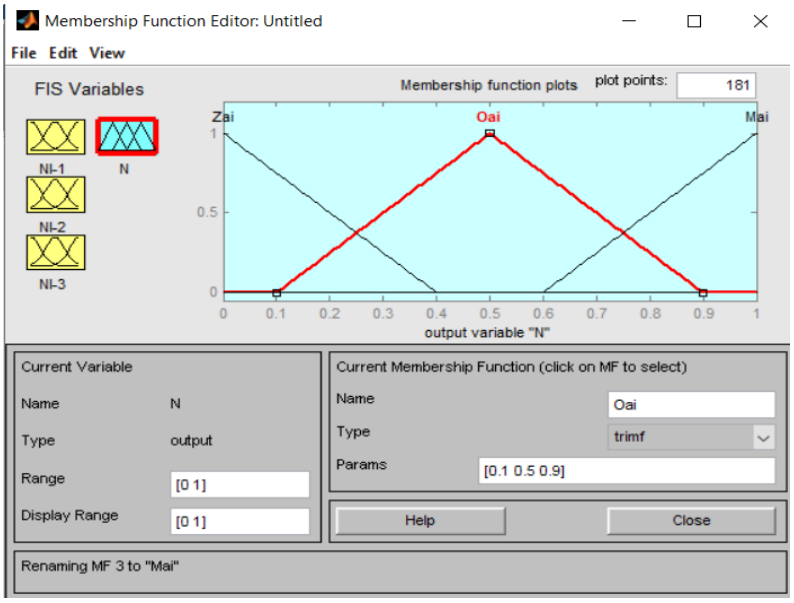

Рисунок 26. – Значення вихідних змінних

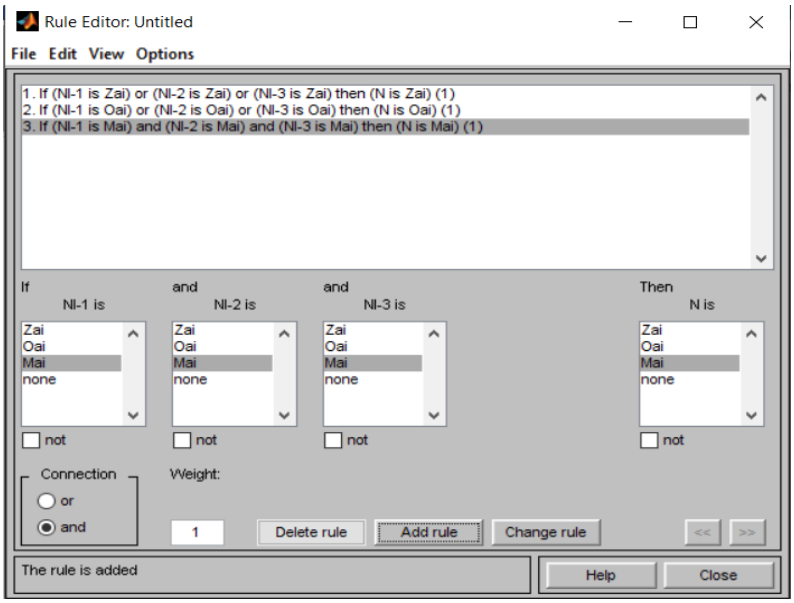

Рисунок 27. – Система продукційних правил

Рисунок 28. – Перевірка роботи системи

Всі критеріїв низький, отже зовнішня ідентифікація і автентифікація.

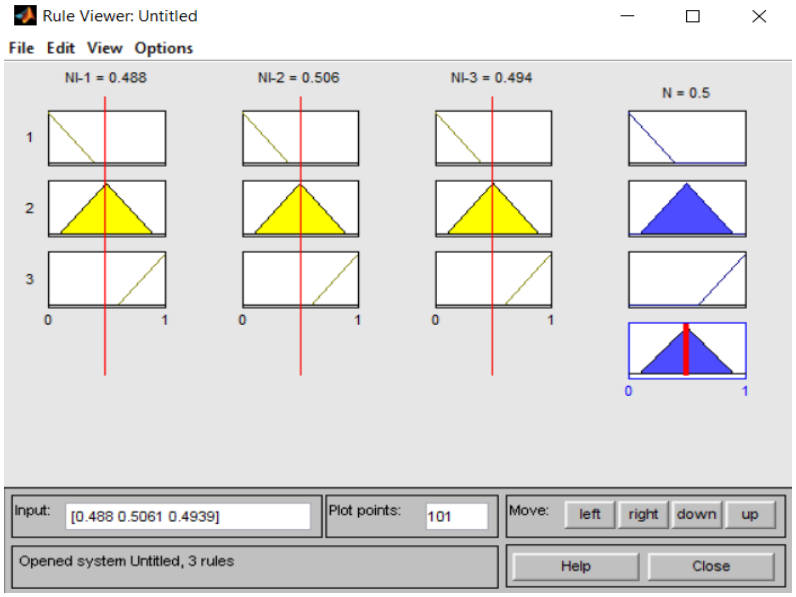

Рисунок 29. – Перевірка роботи системи

Всі з критеріїв середні, отже одиночна ідентифікація і автентифікація.

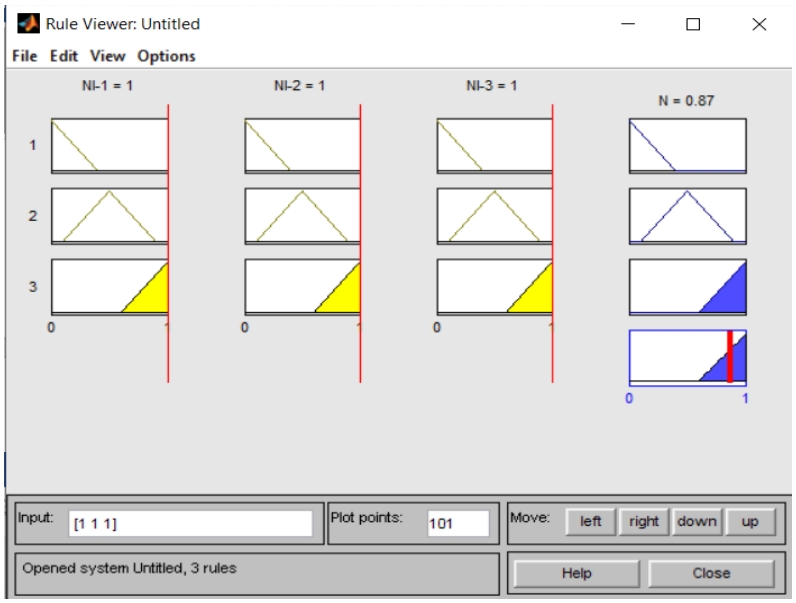

Рисунок 30. – Перевірка роботи системи

Всі критерії високі, отже множинна ідентифікація і автентифікація

Висновок: нечітка експертна система, для оцінки критеріїв цілісності побудована та працює за встановленими правилами.

Розроблена система нечіткого логічного виведення для оцінки інтегрального показника відповідності допоможе удосконалити нечітку модель шляхом введення ієрархічної структури критеріїв оцінювання, що дозволить подати процес у явному виді та реалізувати процес перевірки критеріїв із зазначенням ступеню впевненості експерта у релевантності критеріїв оцінювання. Нечіткі множини сформовані за результатом перевірки критеріїв відповідності визначеним для них рівням захищеності на верхніх рівнях ієрархії є вхідними даними для критеріїв нижніх рівнів.

ВИСНОВОК

У дипломній роботі було розкрито сутність оцінювання ризиків інформаційної безпеки, в результаті реалізації яких, телекомунікаційні підприємства можуть понести, як фінансовий, так і іміджевий збиток. Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування, які завжди пов’язана з певним ризиком.

Проблеми ризиків інформаційної безпеки і знаходження шляхів зниження шкоди постають з кожним роком все гостріше. Однак не всі власники і користувачі інформаційних ресурсів можуть самостійно забезпечити надійний захист інформації та гарантоване покриття можливих втрат від ризиків.

В даній роботі було виконано математичний опис завдання оцінювання захищеності інформаційно комунікаційних систем. Була розроблена модель нечіткого логічного виведення.

Та був проведений аналіз нормативних документів технічного захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень : навчальний посібник. – Запоріжжя: ЗНТУ, 2008. – 341 с.
2. Нечеткие множества и теория возможностей. Последние достижения / Под ред. Р.Р. Ягера. – М.: Радио и связь, 1986. – 408 с
3. Орловский С.А. Проблемы принятия решений при нечеткой исходной информации. – М.: Радио и связь, 1981. – 286 с.
4. Рідкокаша А.А., Голдер К.К. Основи систем штучного інтелекту. Навчальний посібник. Черкаси, "ВІДЛУННЯ – ПЛЮС", 2002. – 240 с
5. При Прикладные нечеткие системы / Асаи К., Ватада Д., Иваи С. и др./Под ред. Т. Тэрано, К. Асаи, М. Сугено. – М.: Мир, 1993. – 368 с.
6. Мелихов А.Н., Берштейн Л.С., Коровин С.Я. Ситуационные советующие системы с нечеткой логикой. – М.: Наука, 1990. – 272 с.
7. Несенюк А.П. Неопределенные величины в задачах управления с неполной информацией // Автоматика. – 1979. – № 2. – С.55 – 64.
8. Кандель А., Байатт У.Дж. Нечеткие множества, нечеткая алгебра, нечеткая статистика // Труды американского общества инженеров – радиоэлектроников. – 1978. – Т. 66. – №12. – С.37 – 61
9. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.:Мир, 1976. – 165 с
10. Малышев Н.Г., Бернштейн Л.С., Боженюк А.В. Нечеткие модели для экспертных систем в САПР. — М.: Энергоиздат, 1991. — 136 с
11. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 05.07.1994 р. № 80/94-ВР – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text – 26.08.2020.

12. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text – 26.08.2020.

13. Методика оцінки кібернетичної захищеності ін-формаційно-телекомунікаційного вузла зв’язку / В.В Куцаєв [та ін.] // Збірник наукових праць ВІТІ. — 2018. — Т. 2. — С. 67—76.

14. Салієва О. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання [Електронний ресурс] / О. Салієва, Ю. Яремчук. — Режим доступу: https://doi.org/10.18372/2225-5036.26.14669.

15. Бурячок В.Л. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах [Текст] / В.Л Бурячок // Сучасний захист інформації. – Київ, 2015. – № 3. – С. 4–12.

16. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення [Текст]/ Р.В Киричок // Наукові записки Українського науково-дослідного інституту зв’язку. – Київ, 2016. – № 3(43). – С. 48–61.

17. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] : Постанова Національного банку України від 28.09.2017 р. № 95. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17#n12 – 26.08.2020.

18. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації [Електронний ресурс] : Наказ від 16.05.2007 р. № 93 – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0820-07#Text – 26.08.2020.

19. Ротштейн О. Моделювання та оптимізація надійності багатовимірних алгоритмічних процесів [Текст] / О.П Ротштейн, С.Д Штовба, О.М Козачко. – Вінниця : УНІВЕРСУМ-Вінниця, 2007. – 212 с.

20. Левченко Е.Г. Показники багатоступінчатих систем захисту інформації / Е.Г. Левченко, Р.Б. Прус, А.О. Рабчун // Вісник Інженерної академії України. – 2009. – №1. - С. 61-65.

21. Бочарников В.П. Fuzzy - технология: Математические основы. Практика моделирования в экономике / В.П. Бочарников. - СПб.: “Наука” РАН, 2001. - 328 с.

22. Бочарников В.П. Fuzzy - технология: Основы моделирования и решения експертно-аналитических задач / В.П. Бочарников, С.В. Свєшников. - К.: Эльга, Ника-Центр, 2003, - 296 с.

23. Алексеев А.В. Интерпретация и определение функций принадлежности нечетких множеств / А.В. Алексеев // Методы и системы принятия решений. - Рига: Риж. политехн. ин-т, 1979. - С. 42 - 50.

24. Толюпа С.В., Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних / С.В. Толюпа, О.М. Іванова, І.О. Демченко // Науковотехнічний журнал “Сучасний захист інформації”. – 2013. - №1. – С. 25-30.

ДОДАТОК А

Лістинг коду :

```
[System]
Name='Untitled_1'
Type='mamdani'
Version=2.0
NumInputs=3
NumOutputs=1
NumRules=3
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
[Input1]
Name='NI-1'
Range=[0 1]
NumMFs=3
MF1='Zai':'trimf',[-0.4 0 0.4]
MF2='Oai':'trimf',[0.1 0.5 0.9]
MF3='Mai':'trimf',[0.6 1 1.4]
[Input2]
Name='NI-2'
Range=[0 1]
NumMFs=3
MF1='Zai':'trimf',[-0.4 0 0.4]
MF2='Oai':'trimf',[0.1 0.5 0.9]
MF3='Mai':'trimf',[0.6 1 1.4]
[Input3]
Name='NI-3'
Range=[0 1]
NumMFs=3
MF1='Zai':'trimf',[-0.4 0 0.4]
MF2='Oai':'trimf',[0.1 0.5 0.9]
MF3='Mai':'trimf',[0.6 1 1.4]
[Output1]
Name='N'
Range=[0 1]
NumMFs=3
```

MF1='Zai':'trimf',[-0.4 0 0.4]
MF2='Oai':'trimf',[0.1 0.5 0.9]
MF3='Mai':'trimf',[0.6 1 1.4]
[Rules]
1 1 1, 1 (1) : 2
2 2 2, 2 (1) : 2
3 3 3, 3 (1) : 1

[System]
Name='Untitled_2'
Type='mamdani'
Version=2.0
NumInputs=3
NumOutputs=1
NumRules=3
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
[Input1]
Name='DR-1'
Range=[0 1]
NumMFs=3
MF1='K':'trimf',[-0.4 0 0.4]
MF2='N':'trimf',[0.1 0.5 0.9]
MF3='P':'trimf',[0.6 1 1.4]
[Input2]
Name='DR-2'
Range=[0 1]
NumMFs=3
MF1='K':'trimf',[-0.4 0 0.4]
MF2='N':'trimf',[0.1 0.5 0.9]
MF3='P':'trimf',[0.6 1 1.4]
[Input3]
Name='DR-3'
Range=[0 1]
NumMFs=3
MF1='K':'trimf',[-0.4 0 0.4]
MF2='N':'trimf',[0.1 0.5 0.9]

MF3='P':'trimf',[0.6 1 1.4]
[Output1]
Name='D'
Range=[0 1]
NumMFs=3
MF1='K':'trimf',[-0.4 0 0.4]
MF2='N':'trimf',[0.1 0.5 0.9]
MF3='P':'trimf',[0.6 1 1.4]
[Rules]
1 1 1, 1 (1) : 2
2 2 2, 2 (1) : 2
3 3 3, 3 (1) : 1

[System]
Name='Untitled_3'
Type='mamdani'
Version=2.0
NumInputs=4
NumOutputs=1
NumRules=3
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
[Input1]
Name='KD-1'
Range=[0 1]
NumMFs=3
MF1='NV':'trimf',[-0.4 0 0.4]
MF2='CHV':'trimf',[0.1 0.5 0.9]
MF3='VV':'trimf',[0.6 1 1.4]
[Input2]
Name='KD-2'
Range=[0 1]
NumMFs=3
MF1='NV':'trimf',[-0.4 0 0.4]
MF2='CHV':'trimf',[0.1 0.5 0.9]
MF3='VV':'trimf',[0.6 1 1.4]
[Input3]
Name='KD-3'

Range=[0 1]
NumMFs=3
MF1='NV':'trimf',[-0.4 0 0.4]
MF2='CHV':'trimf',[0.1 0.5 0.9]
MF3='VV':'trimf',[0.6 1 1.4]
[Input4]
Name='KD-4'
Range=[0 1]
NumMFs=3
MF1='NV':'trimf',[-0.4 0 0.4]
MF2='CHV':'trimf',[0.1 0.5 0.9]
MF3='VV':'trimf',[0.6 1 1.4]
[Output1]
Name='6.1'
Range=[0 1]
NumMFs=3
MF1='NV':'trimf',[-0.4 0 0.4]
MF2='CHV':'trimf',[0.1 0.5 0.9]
MF3='VV':'trimf',[0.6 1 1.4]
[Rules]
1 1 1 1, 1 (1) : 2
2 2 2 2, 2 (1) : 2
3 3 3 3, 3 (1) : 1

[System]
Name='Untitled_4'
Type='mamdani'
Version=2.0
NumInputs=4
NumOutputs=1
NumRules=3
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
[Input1]
Name='CD-1'
Range=[0 1]

NumMFs=3
MF1='N':'trimf',[-0.4 0 0.4]
MF2='S':'trimf',[0.1 0.5 0.9]
MF3='V':'trimf',[0.6 1 1.4]
[Input2]
Name='CD-2'
Range=[0 1]
NumMFs=3
MF1='N':'trimf',[-0.4 0 0.4]
MF2='S':'trimf',[0.1 0.5 0.9]
MF3='V':'trimf',[0.6 1 1.4]
[Input3]
Name='CD-3'
Range=[0 1]
NumMFs=3
MF1='N':'trimf',[-0.4 0 0.4]
MF2='S':'trimf',[0.1 0.5 0.9]
MF3='V':'trimf',[0.6 1 1.4]
[Input4]
Name='CD-4'
Range=[0 1]
NumMFs=3
MF1='N':'trimf',[-0.4 0 0.4]
MF2='S':'trimf',[0.1 0.5 0.9]
MF3='V':'trimf',[0.6 1 1.4]
[Output1]
Name='E'
Range=[0 1]
NumMFs=3
MF1='N':'trimf',[-0.4 0 0.4]
MF2='S':'trimf',[0.1 0.5 0.9]
MF3='V':'trimf',[0.6 1 1.4]
[Rules]
1 1 1 1, 1 (1) : 2
2 2 2 2, 2 (1) : 2
3 3 3 3, 3 (1) : 1