УДК 004.3

ЗАХИСТ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ДАНИХ В КОМП'ЮТЕРНІЙ МЕРЕЖІ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Дубчак Л.О.[1)], Пивчук В.Ю.[2)]
Тернопільський національний економічний університет,
[1)]викладач, [2)]студент

I. Постановка задачі

Захист інформації є одним з найважливіших завдань при передачі даних через комп'ютерну мережу. Для вирішення цієї задачі застосовуються симетричні та асиметричні криптоалгоритми шифрування, найпоширеніші серед яких DES, RSA та на основі еліптичних кривих [1]. Кожен з цих алгоритмів захисту має свій рівень стійкості та вимагає різних затрат пам'яті та продуктивності процесора, тому вибір криптоалгоритму необхідно здійснювати залежно від поточного стану комп'ютерної системи та рівня доступу клієнта, який здійснює запит на отримання інформації. Такий вибір найкраще здійснити за допомогою нечіткої логіки, що дозволяє будувати системи, які працюють в реальному часі.

II. Мета роботи

Метою даної роботи є вибір криптоалгоритму для передачі даних в комп'ютерній мережі на основі нечіткої логіки.

III. Нечітка система вибору криптоалгоритму

Для здійснення вибору алгоритму захисту інформації необхідно враховувати рівень доступу клієнта до інформації, а також поточний стан системи, зокрема її поточний рівень продуктивності. Нечіткий висновок найкраще здійснити на основі механізму Мамдані, описаного в [2]. Нечітка система вибору криптоалгоритму зображена на рисунку 1.

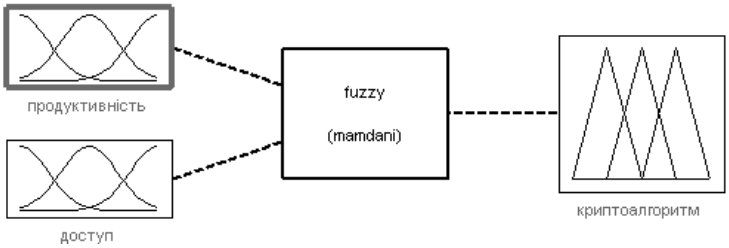
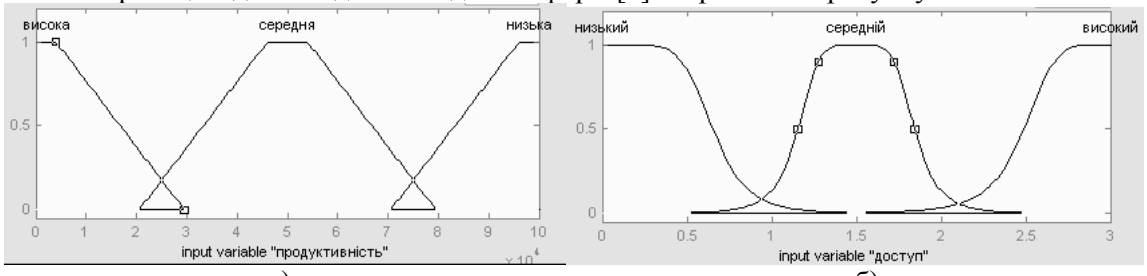


Рисунок 1 - Загальна схема нечіткої системи вибору криптоалгоритму

В якості експертної оцінки вхідних даних можна застосувати значення продуктивності, яке належить відрізку від 0 до 10^5 тактів, а значення рівня доступу – від 0 до 3. Функції належності цих вхідних змінних трапецевидних та дзвоноподібних форм [2] зображені на рисунку 2.



а) б)

Рисунок 2 – Функції належності вхідних змінних: а) продуктивності, б) доступ

Відповідно до вхідних нечітких значень рівня доступу клієнта та необхідного рівня продуктивності система видає значення, яке відповідає необхідному для застосування криптоалгоритму, а саме DES, RSA чи на основі еліптичних кривих, функції належності яких трапецевидної форми [2]. Якщо рівень доступу клієнта високий, то інформацію можна передавати без шифрування, тому виходом нечіткої системи може бути відсутність криптоалгоритму (рисунок 3).

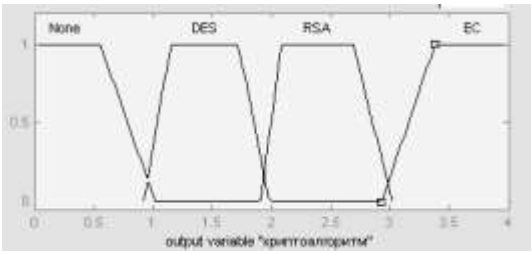


Рисунок 3 – Функції належності виходу «криптоалгоритм»

База правил нечіткого висновку даної системи вибору криптоалгоритму містить 15 правил типу «if - then» (рисунок 4).

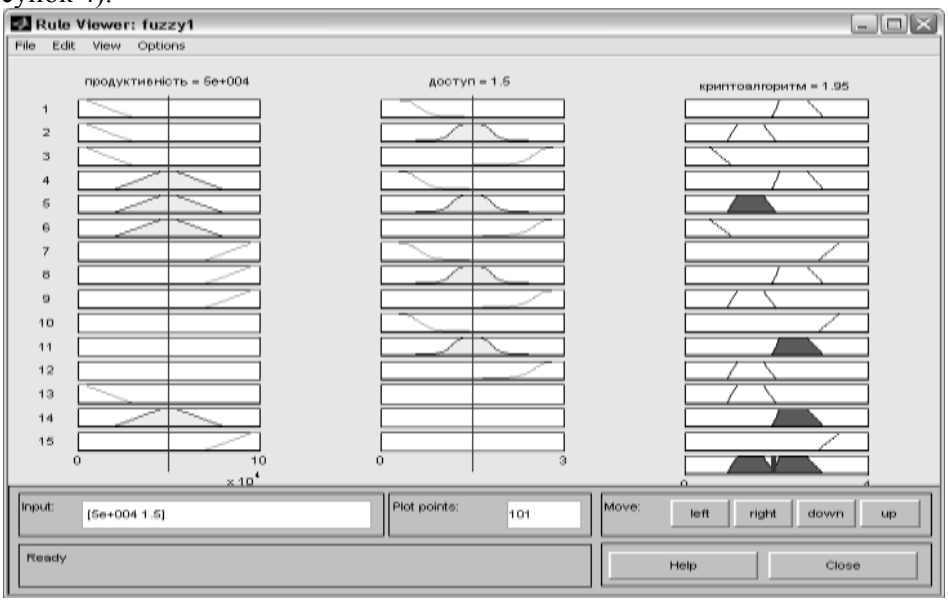


Рисунок 4 – База правил нечіткої системи вибору криптоалгоритму

На рисунку 5 зображено поверхню значень розробленої нечіткої системи, що підтверджує правильність її роботи.

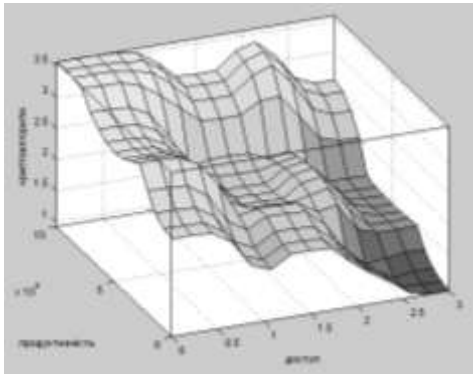


Рисунок 5 – Поверхня значень виходу нечіткої системи вибору криптоалгоритму

Висновок

В даній роботі здійснено моделювання та дослідження нечіткої системи вибору криптоалгоритму з метою захисту інформації при передачі даних в комп'ютерній мережі. Дана система працює в реальному часі і може застосовуватись в комп'ютерних системах, що здійснюють передачі таємної інформації.

Список використаних джерел

1. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації: Навчальний посібник. – К.: Вища шк., 2000.
2. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику / С.Д.Штовба [Електронний ресурс] - Режим доступу: http://matlab.exponenta.ru/fuzzylogic/book1/