МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп’ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Цимбал Денис Михайлович

Алгоритми нечіткого управління системи охорони підприємства / Algorithms of fuzzy management of enterprise security system

спеціальність: 123 - Комп’ютерна інженерія
освітньо-професійна програма - Комп’ютерна інженерія
Кваліфікаційна робота

Виконав студент
групи КІм-21
Д.М. Цимбал

Науковий керівник:
к.т.н., доцент Л.О.Дубчак

ТЕРНОПІЛЬ – 2024

АНОТАЦІЯ

Цимбал Д.М. Алгоритми нечіткого управління системи охорони підприємства. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 123 «Комп'ютерна інженерія», освітньо-професійна програма. Західноукраїнський національний університет, Тернопіль, 2024.

Робота написана обсягом 82 сторінки і містить 39 ілюстрацій, 7 таблиць, 1 додаток та 52 джерела за переліком посилань. Метою роботи є розробка алгоритму нечіткого управління системи охорони приватного підприємства підприємства.

Методи досліджень. Для розв'язання поставлених задач у кваліфікаційній роботі використано методи: аналіз технічних та програмних рішень у сфері систем ідентифікації; моделювання системи за допомогою програмного забезпечення Simulink (MATLAB), апарат нечіткої логіки для створення алгоритмів ідентифікації.

Результати дослідження: алгоритм контролю доступу до охоронюваних територій підприємства.

Розроблений алгоритм забезпечує ефективний контроль доступу до охоронюваних територій підприємства, скорочуючи ризики несанкціонованого доступу та підвищуючи безпеку об'єкта завдяки автоматизації процесу ідентифікації.

Орієнтовні напрямки розвитку досліджень: розроблення спеціалізованих систем автоматизованої ідентифікації працівників підприємства.

КЛЮЧОВІ СЛОВА: АЛГОРИТМ, ІДЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, СКУД, НЕЧІТКА ЛОГІКА.

ANNOTATION

Tsymbal D.M. Algorithms of fuzzy management of the enterprise security system - Manuscript.

Qualification work for obtaining the educational degree "Master" in specialty 123 "Computer Engineering", educational and professional program. West Ukrainian National University, Ternopil, 2024.

The work is 82 pages long and contains 39 illustrations, 7 tables, 1 applications and 52 sources for references. The purpose of the work is to develop an algorithm for fuzzy control of the security system of a private enterprise of an enterprise.

Research Methods. To solve the tasks in the qualification work used: analysis of technical and software solutions in the field of identification systems; system modeling using Simulink (MATLAB) software, a fuzzy logic device for creating identification algorithms

Research results: algorithm for controlling access to protected areas of the enterprise.

The developed algorithm ensures effective control of access to the protected areas of the enterprise, reducing the risks of unauthorized access and increasing the security of the facility thanks to the automation of the identification process.

Indicative directions of research development: development of specialized systems for automated identification of enterprise employees.

KEY WORDS: ALGORITHM, IDENTIFICATION, ACCESS CONTROL, SCUD, FUZZY LOGIC.

ЗМІСТ

ВСТУП

Актуальність роботи. Система контролю та управління доступом (СКУД) являє собою набір технічних та організаційних заходів, призначених для контролю доступу до об'єктів СКУД та моніторингу переміщення людей на охоронюваній території. На сьогодні СКУД визнані одним з найбільш ефективних засобів забезпечення комплексної безпеки на об'єктах [1].

Зважаючи на постійний розвиток СКУД і перспективу їх широкого застосування в найближчі роки, важливо пам'ятати, що СКУД полегшують процес ідентифікації, заощаджують час і підвищують ефективність роботи служб безпеки, але все ж потребують людського контролю. Залежно від рівня загроз та завдань, поставлених перед системою, потрібно правильно визначити баланс між людськими та технічними ресурсами. Встановлення СКУД дозволяє не тільки підвищити загальний рівень безпеки, але й скоротити витрати на її забезпечення, оскільки ці системи потребують менше персоналу для обслуговування та є енергоефективними.

Водночас велика кількість СКУД у світі, відсутність порівняльних аналітичних даних, нестача інформації про їхні функціональні, технічні й експлуатаційні можливості, а також недобросовісність деяких виробників значно ускладнюють вибір систем, що відповідають вимогам конкретних об'єктів [1].

Метою даного дипломного проекту є розробка алгоритму нечіткого управління системи охорони приватного підприємства підприємства. У роботі застосовано теорію нечіткої логіки, що дозволяє створювати системи для роботи в режимі реального часу.

Об'єкт дослідження - системи контролю та управління доступом (СКУД) на підприємствах, які використовують технології ідентифікації для забезпечення безпеки.

Предмет дослідження - методи і засоби ідентифікації працівників на основі нечіткої логіки, що застосовуються для підвищення ефективності роботи

програмно-апаратних СКУД.

Наукова новизна. Удосконалено алгоритм управління захисту, реалізованого у вигляді програмно-апаратної системи ідентифікації працівників підприємства, що дозволяє працювати в реальному часі та враховувати проміжні стани для підвищення точності ідентифікації.

Практична цінність. Розроблений алгоритм забезпечує ефективний контроль доступу до охоронюваних територій підприємства, скорочуючи ризики несанкціонованого доступу та підвищуючи безпеку об'єкта завдяки автоматизації процесу ідентифікації.

Методи дослідження: аналіз технічних та програмних рішень у сфері систем ідентифікації; моделювання системи за допомогою програмного забезпечення Simulink (MATLAB), апарат нечіткої логіки для створення алгоритмів ідентифікації.

Задачі, які необхідно вирішити для проведення дослідження:

1) аналіз існуючих рішень;
2) розробка алгоритмів ідентифікації працівників на основі нечіткої логіки;
3) інтеграція програмного забезпечення з апаратною частиною;
4) тестування і оптимізація системи для роботи в реальному часі.

Результати дослідження апробовані на X Всеукраїнській науково-практичній конференції «Інтелектуальні комп’ютерні системи та мережі» та науково-практичного симпозіуму «Захист інформації» (додаток А).

1 СУЧАСНІ ЗАСОБИ ПРОВЕДЕННЯ ІДЕНТИФІКАЦІЇ ПРАЦІВНИКІВ НА ПІДПРИЄМСТВІ

1.1 Аналіз сучасних технічних та програмних рішень для ідентифікації працівників на підприємствах

Основним методом криптозахисту даних від зловмисників є впровадження так званих систем ідентифікації та аутентифікації (СІА). Використання СІА передбачає, що доступ співробітника до комп'ютера або корпоративної мережі надається лише після успішного проходження процедур ідентифікації та аутентифікації.

Ідентифікація полягає у визначенні особи користувача за його унікальною або присвоєною ознакою. У процесі аутентифікації перевіряється, чи належить користувачу заявлена ним ідентифікаційна ознака [2].

До складу апаратно-програмних СІА входять ідентифікатори, пристрої введення та виведення (зчитувачі, контактні пристрої, адаптери тощо) та відповідне програмне забезпечення. Сучасні СІА поділяються на електронні, біометричні та комбіновані за типом ідентифікаційних ознак (рисунок 1.1).

В електронних системах ідентифікаційні ознаки зберігаються як цифровий код в пам'яті ідентифікатора. Такі СІА можуть використовувати різні види ідентифікаторів [2]:

-ідентифікатори iButton (information button - інформаційна «таблетка»);

-контактні смарт-картки;

-безконтактні радіочастотні ідентифікатори (RFID-системи);

-безконтактні смарт-картки;

-USB-ключі або USB-токени.

У біометричних системах ідентифікаційною ознакою виступають індивідуальні особливості людини, відомі як біометричні характеристики. Процедура ідентифікації та аутентифікації в таких системах базується на зчитуванні біометричної ознаки користувача і її порівнянні з раніше отриманим

шаблоном.

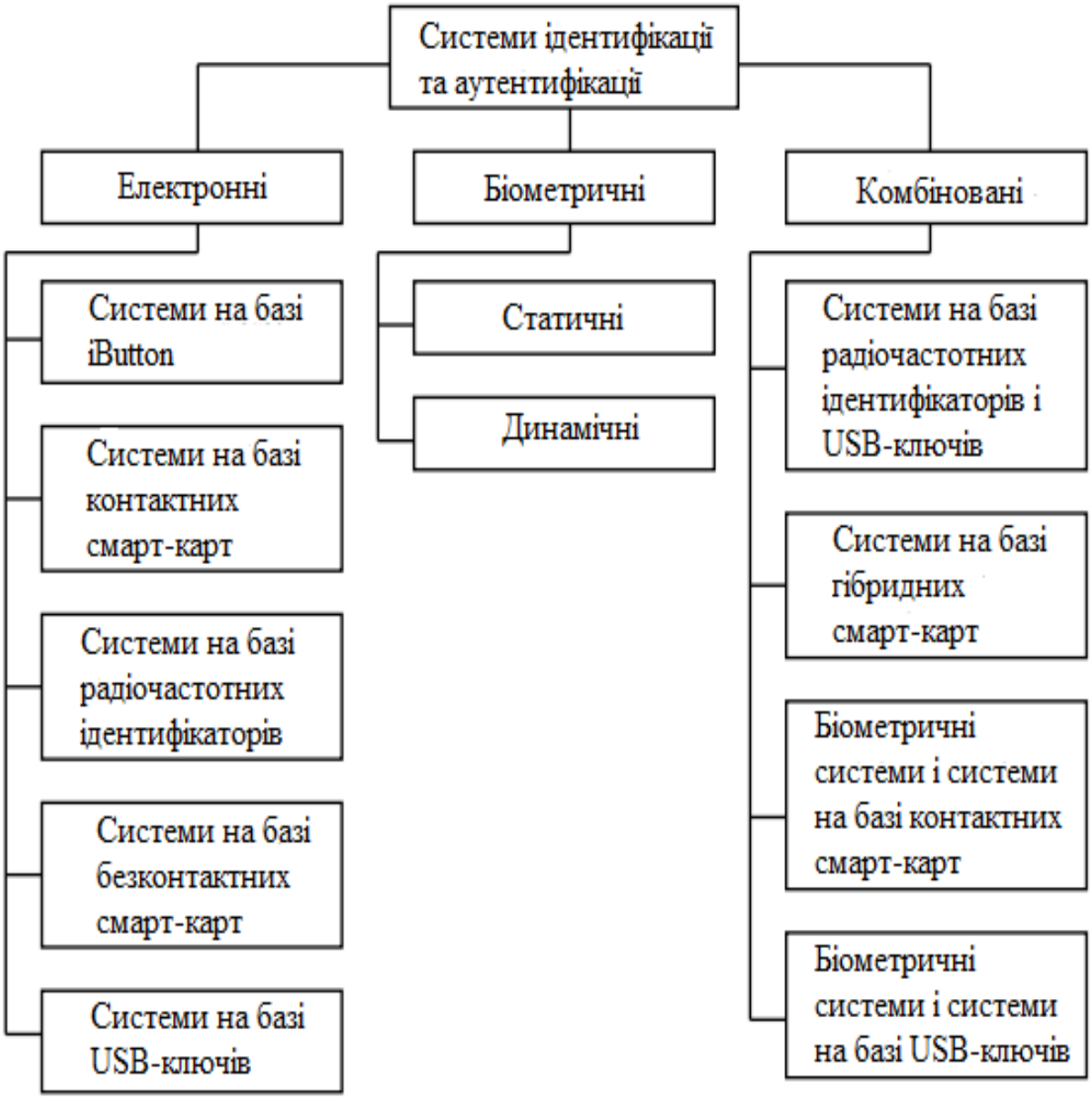

Рисунок 1.1 – Система ідентифікації та аутентифікації користувачів

Біометричні системи діляться на статичні та динамічні залежно від типу використовуваних характеристик. Статична біометрія (фізіологічна) базується на вимірюванні анатомічних особливостей, таких як відбитки пальців, форма кисті, візерунок райдужної оболонки, кровоносні судини обличчя, малюнок сітківки ока, риси обличчя тощо. Динамічна біометрія (поведінкова) використовує аналіз дій людини, зокрема голосу та динаміки підпису.

Комбіновані системи застосовують одночасно кілька ідентифікаційних ознак, що створює додаткові бар'єри для зловмисників, ускладнюючи подолання захисту [2].

Сучасні СКУД застосовують спеціалізовані технічні засоби, які дозволяють визначати рівень доступу осіб і транспортних засобів до охоронюваних зон. Вони також виконують функцію моніторингу переміщення персоналу та транспорту в межах територій організацій. Дані про проходження контрольних пунктів автоматично фіксуються у базі даних, що дозволяє їх подальший аналіз.

СКУД широко використовуються у різноманітних об’єктах, таких як офісні приміщення, бізнес-центри, промислові підприємства, торговельні майданчики та супермаркети.

Найпростішим варіантом ідентифікації є використання двох зчитувачів – окремо для входу та виходу. Під час пред'явлення картки на екрані оператора з’являються фотографія та базова інформація про власника, що дозволяє черговому підтвердити ідентичність особи та надати або обмежити доступ. У більш складних системах зазвичай застосовуються турнікети, через які можна пройти лише після сканування картки. Над турнікетами нерідко встановлюються камери відеоспостереження для додаткового контролю.

Для ідентифікації також можуть використовуватися біометричні технології, такі як сканування відбитків пальців, форми руки, райдужної оболонки ока або інші методи розпізнавання.

Біометричні технології ідентифікації набули значної популярності серед фахівців завдяки високій швидкості роботи та технічним можливостям. Їх використовують не лише у державних установах, які потребують найвищого рівня захисту, але й у комерційному секторі та повсякденному житті. Перспективи широкого впровадження біометричних систем в Україні пов’язані з розвитком бізнесу та виконанням зобов’язань, взятих країною на шляху до євроінтеграції.

Раніше основною перешкодою для масового впровадження біометричних

засобів була їх висока вартість. Однак зниження цієї характеристики робить технологію доступнішою, що дозволяє прогнозувати її поширення у різних галузях, зокрема в сфері інформаційної безпеки.

На даний момент біометрія як наука, що вивчає методи ідентифікації особи, включає кілька незалежних напрямків, кожен із яких має свої технічні досягнення. У цій статті розглянуто основні досягнення біометрії, які вже знайшли практичне застосування, а також проаналізовано їхні переваги, недоліки та перспективи розвитку.

Сканування відбитків пальців - цей метод є одним із найстаріших, проте водночас вважається одним із найперспективніших. Унікальність та незмінність відбитків пальців кожної людини підтверджена криміналістикою та практикою. Біометричні системи ідентифікації використовують два основні підходи до розпізнавання відбитків пальців: на основі точок мініатюр та методом кореляцій. Обидва способи постійно вдосконалюються, маючи свої переваги та обмеження. Їхня робота базується на аналізі фізіологічних властивостей папілярних візерунків за допомогою апаратно-програмних засобів.

Дактилоскопічна перевірка особи, яка прагне отримати доступ до охоронюваного об’єкта, виконується за допомогою телевізійної камери, що сканує папілярний візерунок пальця. Отримане зображення порівнюється з еталоном у базі даних за допомогою кореляційного методу. Випробування показали, що в таких системах можливі похибки у межах 10–20 %, зокрема через суху шкіру чи недостатньо чіткі візерунки у деяких користувачів.

Дані про відбитки зберігаються у базі аутентифікації. Для ідентифікації відбиток пальця розкладається на ключові елементи, такі як «завиток», «дуга» або «петля», а не зберігається у вигляді суцільного зображення. Це дозволяє забезпечити точність та ефективність системи. (рисунок 1.2) [5]

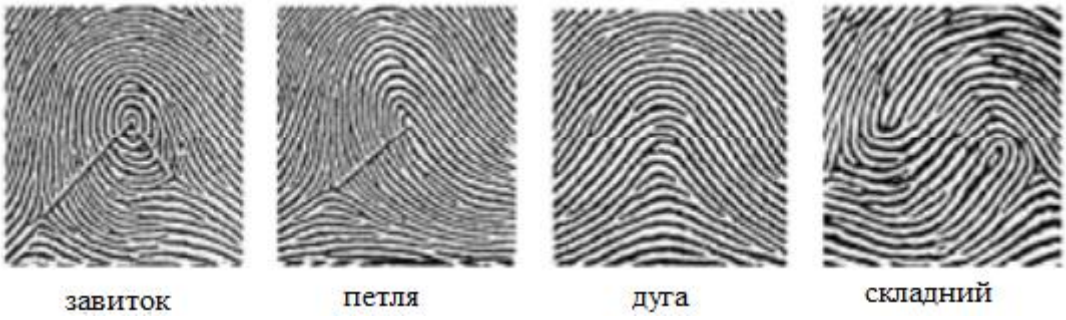

Рисунок 1.2 – Приклади основних елементів відбитка пальця

Біометричні системи, що використовують ідентифікацію за відбитком пальця, характеризуються вкрай низькими показниками відмови в доступі для зареєстрованих користувачів. При цьому вони мають невелику ймовірність помилкового допуску незареєстрованих осіб. Зазначається, що рівень відмови (КВ) зазвичай не перевищує 0,01%, а похибка помилкового доступу (КД) становить близько 0,001%. Точка, де ці два показники стають однаковими, визначається як стандартна похибка і становить приблизно 0,1%. Сучасні розробки в цій галузі зосереджені на вдосконаленні алгоритмів, здатних ефективно справлятися з "шумом" у зображеннях, що підвищує точність і швидкість роботи систем у реальному часі. Найбільше такі методи ідентифікації поширені у сфері криміналістики та безпеки.

Що стосується технологій розпізнавання обличчя, їх основною метою є ідентифікація конкретної особи серед великої кількості записів у базі даних. Якість роботи таких систем залежить від характеристик обладнання, зокрема відеокамер, які повинні мати роздільну здатність не менше 320x240 пікселів і підтримувати швидкість відеопотоку від 3 до 5 кадрів за секунду. Для забезпечення вищої якості розпізнавання потрібне збільшення швидкості відеопотоку, наприклад, до 15 кадрів за секунду або більше, що суттєво покращує результати. Камери, які відповідають цим вимогам, коштують близько 70 доларів США, а програмне забезпечення для таких систем часто доступне у відкритому доступі. Це дозволяє навіть із мінімальними фінансовими ресурсами проводити експерименти та дослідження.

Сучасні системи для сканування обличчя здійснюють обробку приблизно за 20–30 секунд, генеруючи кілька зображень. Одне якісне зображення обличчя зазвичай займає 150–300 Кб, а шаблони зображень – близько 1300 байт. Основний принцип роботи цих систем полягає у створенні "живого" шаблона в реальному часі, який порівнюється із заздалегідь збереженим зразком. Надійність результатів залежить від багатьох факторів, включаючи освітлення, дистанцію, кваліфікацію персоналу та продуктивність обладнання. При цьому якість зображення має суттєвий вплив на кінцевий результат.

У технологіях розпізнавання обличчя використовуються три ключові методи. Найпоширенішим є аналіз характерних рис обличчя, що дозволяє адаптуватися до змін міміки. Другий підхід базується на застосуванні нейронних мереж, які працюють із "особливими точками", забезпечуючи точність навіть у складних умовах. Третій метод передбачає автоматичну обробку зображення через аналіз відстаней між ключовими рисами обличчя. Хоча цей спосіб менш ефективний порівняно з іншими, він корисний для розпізнавання у поганих умовах освітлення.

Основні труднощі, які впливають на ефективність біометричних систем розпізнавання, пов’язані зі зміною освітлення, рухом обличчя, складністю виділення ключових ділянок, включаючи портретні зони, та впливом фону, що ускладнює ідентифікацію. Частково ці проблеми вирішуються автоматичним визначенням особливих точок на обличчі та вимірюванням відстаней між ними. Серед таких точок зазвичай виділяють контури очей, брів, носа, підборіддя й вух. Відстані між ними формують унікальний еталон конкретної особи, який легко адаптується до масштабування. Водночас системи цього типу не здатні розрізняти однояйцевих близнюків.

Значного прогресу у вирішенні проблем ідентифікації досягнуто завдяки використанню інфрачервоних променів. Цей метод дозволяє проводити термографію обличчя, визначаючи унікальний малюнок кровоносних судин, що постачають кров до шкіри. Такий підхід не залежить від освітлення, тому пристрої можуть працювати навіть у повній темряві. Фактори на кшталт

перегріву чи переохолодження, старіння шкіри або навіть пластичних операцій не впливають на результати, оскільки внутрішня структура судин залишається незмінною. Цей метод також дозволяє розрізняти однояйцевих близнюків, адже їхні судинні малюнки мають суттєві відмінності. У порівнянні з попередніми підходами, термографія є значно ефективнішою.

Ідентифікація за геометрією кисті руки за своїми характеристиками схожа на метод розпізнавання за відбитком пальця, однак використовується рідше. Ця технологія потребує мінімального обсягу даних для зберігання — лише 9 байт, що дає змогу накопичувати великі бази інформації та забезпечувати швидкий пошук. Одним із найрозвиненіших пристроїв цього типу є "Handkey", який сканує як зовнішню, так і внутрішню сторону долоні за допомогою вбудованої камери. Інші системи, які аналізують додаткові параметри кисті, розробляються такими компаніями, як BioMet Partners, PalmMetrics і BTG [5].

Рисунок 1.3 - Пристрій "Handkey"

Системи, які аналізують тривимірну геометрію кисті руки, є більш складними. Вони враховують об’єм пальців і кисті, нерівності долоні та розташування складок шкіри на суглобах. Для збору таких даних використовують телевізійну камеру разом з інфрачервоним підсвічуванням, яке направляється на руку під різними кутами. Світлодіоди, що послідовно вмикаються, створюють тіньові проекції, що дозволяють отримати інформацію

про об’єм і унікальні характеристики руки. Такі пристрої досить громіздкі через необхідність встановлення джерел підсвічування на відстані 10–15 см, а їхня вартість коливається в межах 600–3000 доларів. Рівень помилок першого та другого роду для цих систем не перевищує 0,2 %. Такі пристрої не вимагають особливих умов експлуатації, як-от чистота чи стабільна температура рук.

Ідентифікація за райдужною оболонкою ока здійснюється за допомогою інфрачервоного випромінювання низької інтенсивності, яке проходить через зіницю та висвітлює кровоносні судини задньої стінки ока. Ця технологія демонструє найнижчий рівень відмов у доступі. Однак для точної роботи система потребує чіткого зображення райдужної оболонки. Фізіологічні зміни організму, як-от зміна структури райдужної оболонки з віком, можуть викликати проблеми з розпізнаванням. Наприклад, у дітей райдужна оболонка змінюється настільки, що система може не впізнати особу. Крім того, навіть незначні травми ока, безсоння чи велике навантаження на зір здатні спричинити похибки в ідентифікації.

Біометричні пристрої, які аналізують сітківку ока, також використовують інфрачервоне світло для виявлення унікального малюнка кровоносних судин. Ці системи мають найменший рівень відмови серед усіх біометричних технологій і практично не допускають помилкових ідентифікацій. Однак вони вимагають чіткого зображення сітківки, а такі проблеми, як катаракта, можуть знижувати якість розпізнавання. Висока вартість пристроїв (близько 4000 доларів) і побоювання користувачів щодо можливого впливу інфрачервоного випромінювання на здоров’я знижують їхню популярність.

Технологія розпізнавання голосу базується на унікальних акустичних характеристиках голосу людини. Основною перевагою цього методу є можливість дистанційної ідентифікації, що робить його затребуваним у банках та інших установах. Для реєстрації особа вимовляє пароль, наприклад, "мій голосовий пароль", на основі чого створюється індивідуальний акустичний шаблон. У подальшому користувач повинен лише повторити цей пароль для перевірки. Процес ідентифікації відбувається швидко, зі швидкістю вимови

пароля. Однак недоліком є чутливість системи до змін голосу: навіть незначні проблеми з горлом, як-от ларингіт або хрипота, можуть унеможливити розпізнавання.

До електронних засобів ідентифікації належать пристрої, що зчитують ідентифікаційні дані, а також ідентифікатори, які зберігають інформацію про права доступу. Вони використовуються для визначення прав осіб, транспорту або майна на доступ до певних зон, що знаходяться під охороною [1].

У місцях контролю доступу, таких як двері, турнікети чи пропускні кабіни, встановлюють спеціальні зчитувачі, виконавчі пристрої та інше обладнання для забезпечення функціонування системи контролю.

Ідентифікатор є носієм унікальної кодової інформації, яка підтверджує права доступу власника. Вони можуть мати форму брелоків, ключів чи карток.

Зчитувач – це електронний пристрій, який отримує інформацію з ідентифікатора, перетворюючи її у стандартний формат для подальшого аналізу й ухвалення рішення в контролері.

Ідентифікатор iButton належить до категорії електронних контактних пристроїв і представлений різноманітним модельним рядом, що включає понад 20 моделей. Загалом, iButton – це мікросхема, розміщена у герметичному сталевому корпусі. Живлення мікросхеми забезпечує невелика літієва батарейка. Корпус пристрою за формою нагадує стандартний акумулятор (рисунок 1.4) і має діаметр 17,35 мм. Висота корпусу варіюється залежно від моделі: 5,89 мм для корпусу F5 та 3,1 мм для корпусу F3 [2].

Рисунок 1.4 – iButton ідентифікатори

Корпус ідентифікатора iButton надійно захищає пристрій від негативного впливу зовнішнього середовища, зокрема агресивних хімічних речовин, пилу, вологи, механічних ударів і електромагнітних полів. Його конструкція дозволяє легко закріпити пристрій на носії, наприклад, на брелоку чи картці.

Основними елементами чіпа є мультиплексор і пам'ять, яка складається з таких компонентів:

Постійно запам'ятовуючий пристрій (ПЗП) — зберігає 64-розрядний код, що включає унікальний 48-розрядний серійний номер, восьмирозрядний код типу ідентифікатора та восьмирозрядну контрольну суму.

Енергонезалежна оперативна пам'ять NV RAM — використовується для збереження як загальнодоступної, так і конфіденційної інформації, наприклад, криптографічних ключів чи паролів доступу.

Надоперативна пам'ять SM (scratchpad memory) — виконує роль буферної пам’яті.

Для обміну даними між ідентифікатором і зчитувачем необхідний фізичний контакт корпусу iButton зі зчитувальним пристроєм. Час, потрібний для встановлення зв’язку, становить менше 5 мс, а кількість гарантованих контактів перевищує кілька мільйонів (таблиця 1.1).

Переваги електронних ідентифікаторів iButton:

-тривалий термін служби (інформація в пам’яті зберігається щонайменше 10 років);

-високий рівень захищеності від механічних і електромагнітних впливів;

-компактність і невеликі розміри;

-доступна вартість.

Таблиця 1.1- Технічні характеристики пам’яті iButton

Тип виробу	Ємність NV RAM	Ємність SM, біт	Ємність ПЗП, байт	Примітка
DS1963S	4 Кбіт (16 сторінок по 256 біт)	256	64	8 сторінок NV RAM захищаються паролями. Реалізація SHA-1
DS1991	1152 Кбіт (4 сторінки по 256 біт)	256	64	3 блока NV RAM захищаються паролями
DS1992L	1 Кбіт (4 сторінки по 256 біт)	256	64	Незахищена NV RAM
DS1993L	4 Кбіт (16 сторінок по 256 біт)	256	64	Незахищена NV RAM
DS1994L	4 Кбіт (16 сторінок по 256 біт)	256	64	Незахищена NV RAM. Годинник реального часу
DS1995L	16 Кбіт (64 сторінки по 256 біт)	256	64	Незахищена NV RAM
DS1996L	64 Кбіт (256 сторінок по 256 біт)	256	64	Незахищена NV RAM

Недоліком є необхідність точного ручного дотику ідентифікатора до зчитувача для коректної роботи системи.

Контактні смарт-карти належать до групи електронних контактних ідентифікаторів. Їх поділяють на карти з процесором і карти з пам'яттю. Зазвичай вони виготовляються у формі пластикових карток [2].

Процесорні смарт-карти оснащені чіпом, що містить центральний процесор, оперативну пам’ять (ОЗП), постійно запам'ятовуючий пристрій (ПЗП), а також електронно стираючий програмований постійний запам’ятовуючий пристрій (ЕСППЗП або EEPROM). У багатьох моделях присутній спеціалізований співпроцесор.

Оперативна пам’ять таких карт використовується для тимчасового зберігання даних, наприклад, проміжних результатів розрахунків, виконаних

процесором. Її обсяг становить кілька кілобайт. Спеціалізований співпроцесор виконує функції підвищення захищеності системи ідентифікації, такі як:

-створення криптографічних ключів;

-виконання криптографічних алгоритмів (наприклад, ГОСТ 28147-89, DES, 3DES, RSA, SHA-1);

-проведення операцій із цифровими підписами (створення та перевірка);

-управління PIN-кодами та іншими захисними функціями.

ПЗП використовується для зберігання виконуваного коду процесора, ОЗП — як робоча пам'ять, а ЕСППЗП містить змінювані дані власника картки.

Безконтактні радіочастотні ідентифікатори, або RFID-системи (Radio Frequency Identification), відносяться до безконтактних електронних пристроїв. Вони доступні у вигляді карток, брелоків, браслетів, ключів тощо, кожен із яких має унікальний серійний номер [2].

До основних компонентів таких пристроїв належать інтегральна мікросхема для зв’язку зі зчитувачем і вбудована антена. Чіп містить пам’ять (або мікросхему з жорсткою логікою) і допоміжні модулі, такі як модулятор, блок управління, програмуючий модуль тощо. Обсяг пам’яті в таких пристроях коливається від 8 до 256 байт. У пам'яті зазвичай зберігаються унікальний номер ідентифікатора, код пристрою, а також службові дані (наприклад, біти парності чи дані для початку та завершення передачі).

Основними перевагами радіочастотних ідентифікаторів (RFID-систем) є безконтактне зчитування, висока довговічність пасивних ідентифікаторів (деякі виробники надають довічну гарантію на карти), а також точність і зручність процесу зчитування ідентифікаційних даних.

Серед недоліків RFID-систем можна виділити недостатню електромагнітну захищеність та досить високу вартість, враховуючи необхідність придбання зчитувачів.

Таблиця 1.2- Технічні характеристики безконтактних ідентифікаторів

Характеристика	Ідентифікатори Proximity	Смарт-карта	
		Стандарт ISO/IEC 14443	Стандарт ISO/IEC 15693
Частота радіоканалу	125 кГц, 13.56 МГц	13.56 МГц	13.56 МГц
Дистанція читання	До 1 м	До 10 м	До 1 м
Вбудовані типи чіпів	Мікросхема пам'яті, мікросхема з жорсткою логікою	Мікросхема пам'яті, мікросхема з жорсткою логікою, процесор	Мікросхема пам'яті, мікросхема з жорсткою логікою
Функція пам'яті	Тільки читання	Читання/запис	Читання/запис
Ємність пам'яті	8-256 байт	64 байт – 64 Кб	256 байт – 2 Кб
Алгоритми шифрування і аутентифікації	По опціях	Технологія MIFARE, DES, 3DES, AES, RSA, ECC	DES, 3DES
Механізм антиколізії		Є	Є

Ідентифікатори на основі USB-ключів відносяться до електронних контактних пристроїв. Вони не потребують дорогих зчитувачів, оскільки підключаються безпосередньо до USB-порту або через з'єднувальний кабель.

USB-ключі можуть включати такі компоненти: процесор для управління та обробки даних; криптографічний процесор для виконання алгоритмів криптографічних перетворень, таких як ГОСТ 28147-89, DES, 3-DES, RSA, DSA, MD5, SHA-1 та інші; USB-контролер для забезпечення зв'язку з USB-портом комп'ютера; оперативну пам'ять (ОЗП) для зберігання змінних даних; ЕСППЗП для збереження ключів шифрування, паролів, сертифікатів та інших важливих даних; постійну пам'ять (ПЗП) для збереження команд і констант.

Таблиця 1.3- детальні характеристики USB-ключів

Виріб	Ємність пам'яті	Розрядність серійного номера	Алгоритм шифрування
iKey 20xx	8/32	64	DES, 3DES, RC2, RC4, MDS, RSA-1024/2048
eToken R2	16/32/64	32	DESX (ключ 120 біт), MDS
eToken PRO	16/32	32	RSA/1024, DES, 3DES, SHA-1
ePass1000	8/32	64	MD5, MD5-HMAC
ePass2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1
ruToken	8/16/32/64/128	32	ГОСТ 28147-89, RSA, DES, 3DES, RC2, RC4, MD4, SHA-1

Основні переваги ідентифікаторів на основі USB-ключів полягають у тому, що вони не потребують спеціального апаратного зчитувача, мають компактні розміри і зручні для зберігання, а також легко підключаються до USB-порту. Однак, до мінусів можна віднести відносно високу вартість і слабкий рівень механічної захищеності брелка.

Останнім часом популярність здобувають комбіновані системи ідентифікації, які використовують двофакторну аутентифікацію для забезпечення безпечного доступу до інформаційних ресурсів компаній. Впровадження таких систем в корпоративну інформаційну безпеку дозволяє використовувати кілька ідентифікаційних факторів одночасно. Сьогодні існують різні типи комбінованих систем ідентифікації та аутентифікації, зокрема:

-Системи на основі радіочастотних ідентифікаторів та USB-ключів;

-Системи на базі гібридних смарт-карт;

-Біоелектронні системи.

Деякі з цих систем також здатні контролювати фізичний доступ до будівель і приміщень. Інтеграція USB-ключів і радіочастотних ідентифікаторів

передбачає встановлення антени і мікросхеми з безконтактним інтерфейсом у корпус брелка. Це дозволяє використовувати один ідентифікатор для управління доступом до комп'ютера та до приміщення. Співробітник може використовувати цей ідентифікатор для доступу до службових приміщень як безконтактну карту, а для доступу до захищених комп'ютерних даних — як USB-ключ. Витягнувши ідентифікатор із USB-порту, він автоматично заблокує роботу комп'ютера, що додає зручності та безпеки.

Прикладом такого ідентифікатора є RFiKey, який є USB-ключем iKey з вбудованою мікросхемою Proximity. Цей пристрій підтримує інтерфейси USB 1.1/2.0 та сумісний із зчитувачами HID Corporation. Основні характеристики RFiKey включають підтримку криптографічних алгоритмів, таких як MD5, RSA, DES, 3-DES, а також наявність апаратного датчика випадкових чисел і підтримку кількох стандартів, таких як PKCS #11, MS Crypto API, PC/SC.

Гібридні смарт-карти поєднують різні чіпи, один з яких підтримує контактний інтерфейс, а інший — безконтактний (Proximity, ISO14443/15693). Такі карти вирішують дві важливі задачі: захист доступу до комп'ютерів і приміщень компанії. Окрім того, на картці може бути поміщена фотографія співробітника, що забезпечує візуальну ідентифікацію. Впровадження гібридних карт, подібно до комбінації USB-ключів і RFID, підкреслює ефективність принципу «два в одному», а додавання фотографії перетворює їх у «три в одному».

Інтеграція безконтактних смарт-карт з електронними системами здебільшого застосовується в системах контролю фізичного доступу до приміщень. Як приклад такої інтеграції можна навести пристрої Precise 100 MC від компанії Precise Biometrics AB. Для отримання доступу до комп'ютерних ресурсів користувач повинен вставити смарт-карту у зчитувач та одночасно прикласти палець до сканера. Шаблони відбитків пальців зберігаються в зашифрованому вигляді в захищеній пам'яті картки. Якщо відбиток на сканері збігається з шаблоном, доступ до комп'ютера надається. Пристрій Precise 100 MC є USB-пристроєм, сумісним з операційною системою Windows. Зчитувач

підтримує всі типи мікропроцесорних карток, що відповідають стандарту ISO 7816-3 (протоколи T=0, T=1). Дактилоскопічний зчитувач представляє собою ємнісний сканер, який здатний обробляти до 4 відбитків пальців на секунду.

1.2 Вибір методу ідентифікації на підприємстві

Біометричне розпізнавання за обличчям є технологією, що дозволяє ідентифікувати людей на основі аналізу їхнього обличчя. Система здійснює вимірювання ключових характеристик, таких як відстань між очима, довжина носа та форма щелепи, і на основі цих даних створюється унікальний шаблон. Порівнюючи нове зображення з наявними шаблонами, система оцінює рівень схожості та визначає, чи є особа в базі даних. Для ідентифікації використовуються зображення з камер спостереження або фотографії з баз даних, наприклад, з водійських посвідчень. Проте, старі або зернисті зображення можуть суттєво знижувати точність.

В реальних умовах зазвичай система працює з двовимірними зображеннями обличчя, що спрощує алгоритми та зменшує обчислювальні витрати, але при цьому зберігається складність через необхідність враховувати фактори освітлення, вираз обличчя, макіяж чи окуляри. Обсяг бази даних зазвичай не перевищує 10 000 зображень.

Існують чотири основні методи розпізнавання обличчя:

1. Метод "Eigenfaces" – використовує двовимірні зображення обличчя для створення шаблонів, на основі яких система порівнює зображення та визначає ідентичність.

2. Метод аналізу "відмінних рис" – дозволяє враховувати зміни у виразі обличчя, використовуючи локальні характеристики (наприклад, кути рота, лінії очей), що дозволяє ідентифікувати людину навіть при зміні виразу.

3. Метод нейронних мереж – порівнює унікальні параметри обличчя з

шаблонами в базі даних, враховуючи найбільшу кількість характеристик, що підвищує точність у складних умовах.

4. Метод автоматичної обробки зображення обличчя – використовує базові геометричні точки, такі як очі, ніс і кути рота, що дозволяє швидко ідентифікувати особу, навіть при низькій якості зображення.

Робота системи розпізнавання осіб залежить від кількох факторів, зокрема якості зображення, актуальності фотографії в базі даних та обсягу цієї бази. Висока якість відеокамер і стабільний відеопотік значно покращують точність ідентифікації. В ідеальних умовах, для досягнення високої точності, система потребує камери з роздільною здатністю не менше 320x240 пікселів і швидкістю зйомки від 3 до 5 кадрів на секунду.

Системи контролю доступу, що використовують безконтактні пластикові proximity картки (зображення 1.5), знаходять широке застосування в різних організаціях та установах. Ці картки дозволяють отримати доступ до захищених приміщень, фактично виконуючи роль електронних ключів. Вони належать до пасивних ідентифікаторів, оскільки не мають власного джерела енергії, що гарантує тривалий термін служби карток.

Рисунок 1.5 - Proximity картка

Кожна карта доступу має унікальний код та серійний номер. Вона складається з двох пластикових пластин, між якими розміщені антена та мікросхема. Пластини герметично з'єднуються на заводі. Мікросхема включає передавач, приймач та процесор, на якому зберігається ідентифікаційний код карти, записаний під час виробництва. Процес зчитування та ідентифікації коду здійснюється за допомогою безконтактної технології радіочастотної ідентифікації. Зчитувач випромінює радіосигнал на частоті 125 кГц, і коли карта потрапляє в зону дії цього сигналу, вона починає передавати відповідь через вбудовану антену. Сигнал приймається зчитувачем, демодулюється і з нього виділяється код доступу, який надсилається на контролер системи. Після ідентифікації система дозволяє доступ або видає помилку. Дистанція, на якій картка спрацьовує, може варіюватися від 7 до 60 см.

З точки зору співвідношення ціни та якості, proximity картки є більш вигідними порівняно з традиційними металевими ключами, особливо на підприємствах з високою плинністю кадрів. Окрім того, безконтактні картки дозволяють значно швидше здійснювати доступ до приміщень, ніж звичайні ключі. Якщо на картці є ідентифікаційні дані співробітника (фото, ім'я, прізвище, посада), вона може виконувати функцію перепустки в разі відсутності зчитуючих пристроїв чи їх несправності.

При виборі моделі зчитувача важливо враховувати не тільки ціну, але й відстань, на якій картка може передавати свій ідентифікаційний код, а також тип інтерфейсу для передачі даних на контролер доступу. Також варто звернути увагу на здатність працювати з вуличними і внутрішніми зчитувачами, а також з пристроями для доступу до комп'ютерних мереж.

Proximity карти мають різні формати, серед яких найпоширенішими є:

-Em-Marine – це один з найпопулярніших форматів безконтактних карт, завдяки низькій вартості;

-HID – формат, розроблений компанією HID Corp. Він є більш захищеним, але також дорожчим;

-Mifare – картки цього формату використовуються в системах оплати

послуг, таких як метрополітени або курорти, і дозволяють зберігати додаткову інформацію.

Наприклад, безконтактна картка Em-Marine містить мікросхему з фіксованим або перепрограмовуваним кодом, котушку індуктивності та конденсатор, що утворюють резонансний контур. Стандарт Em-Marine, розроблений компанією EM Microelectronic, відзначається простотою, доступною ціною та високою надійністю. Ці картки забезпечують довгий термін служби та високу точність при передачі ідентифікаційного коду. Вони працюють за технологією RFID (радіочастотної ідентифікації), і передача даних від картки до зчитувача відбувається безконтактно через радіочастотний сигнал.

Програмована карта ST-PC020EM виробництва Smartec використовує proximity технологію і призначена для ідентифікації персоналу в системах контролю доступу. Вона має пам’ять на 64 біти, що дозволяє зберігати ідентифікаційний код, який може передаватися необмежену кількість разів. Карта працює на частоті 125 кГц і має зчитувану відстань до 10 см, при цьому її товщина всього 0.8 мм.

Рисунок 1.6 – Карта програмована ST-PC020EM

Ідентифікаційна карта ST-PC020EM належить до пасивних пристроїв стандарту Em Marine, оскільки не має власного джерела живлення. Її принцип роботи ґрунтується на proximity технології, за якою зчитувач карт безперервно

випромінює сигнал на частоті 125 кГц. Коли карта потрапляє в радіус дії цього сигналу, вона отримує енергію і генерує радіосигнал з унікальним ідентифікаційним кодом. Ця технологія реалізована через вбудований мініатюрний чіп, що складається з передавача, приймача, процесора та антени. Ідентифікаційний код зберігається в пам'яті процесора, і цей код програмується під час виготовлення.

У порівнянні з іншими RFID-ідентифікаторами, такими як Proximity, Mifare або iClass, карти стандарту Em Marine є найбільш доступними за ціною при збереженні аналогічних функціональних можливостей. Карта ST-PC020EM має високу механічну міцність, стійка до вигинів та ударів, не боїться вологи та забруднень. Виготовлена з міцного PVC пластику, вона має необмежений термін служби. Це дозволяє використовувати картку в різних кліматичних умовах, витримуючи температури від -25°C до +85°C та відносну вологість до 90%.

Як і інші пластикові ідентифікатори, карта ST-PC020EM виготовляється шляхом термопресування двох пластикових пластин, між якими вмонтовано смарт-чіп Em-Marine і антена. Поверхні картки дозволяють наносити будь-яке зображення — написи, фотографії, логотипи та інше — за допомогою різних методів друку, таких як сублімація, офсетний або шовкотрафаретний друк.

Процесор картки Smartec використовує технологію CMOS (метал-оксид-провідник) і має 64 біти пам'яті. Він також захищений від впливу статичної електрики та електромагнітних полів. Під час передачі даних на зчитувач карта ST-PC020EM використовує три види модуляції: Manchester Code, Biphase Code і PSK Code, що відрізняються кількістю імпульсів на один біт.

Таблиця 1.4 - Характеристики карти ST-PC020EM

Параметри	Значення
Робоча частота	100 -150 кГц
Чіп	H-4100
Тип пам’яті	Тільки для читання
Об’єм пам’яті	64 бит
Відстань зчитування	0,1 м
Максимальна кількість відтворень	Не обмежується
Розмір картки	85,4 x 54,0 x 0,8 мм
Матеріал	Полівінілхлорид
Вологість	90%
Діапазон робочих температур	-25°C … +85°C
Температура зберігання	-40°C...+70°C

1.3 Аналіз технічного завдання та постановка задачі

У даній роботі планується розробка програмно-апаратної системи ідентифікації працівників підприємства, що базується на використанні нечіткої логіки. Метою цієї системи є спрощення процесу доступу працівників до території підприємства, забезпечуючи водночас ефективний контроль і захист від несанкціонованого доступу до охоронюваних об'єктів.

Система буде реалізована із застосуванням нечіткої логіки, оскільки вона знаходить все більше застосування в різних сферах технологій. Нечітка логіка дозволяє працювати з множиною значень, що є більш гнучким варіантом порівняно з класичною булевою алгеброю, де результатом може бути лише два значення (істина або хиба). Такий підхід дає можливість точніше моделювати реальні ситуації, де можуть бути проміжні стани.

Проектування цієї системи здійснюватиметься з використанням програмного забезпечення Simulink, яке входить до складу MATLAB. MATLAB є потужним інструментом для математичних розрахунків і моделювання, зокрема для роботи з матрицями, вирішення рівнянь, побудови графіків, а також для обробки та аналізу даних. Це середовище дозволяє виконувати чисельний аналіз, оптимізацію, обробку статистичних даних, а також вирішувати диференціальні рівняння і працювати з великими обсягами даних.

Simulink, як частина MATLAB, пропонує інтерактивне середовище для створення та моделювання динамічних систем. Це дозволяє будувати складні моделі за допомогою графічних блок-діаграм, імітувати роботу систем, а також інтегрувати алгоритми, написані на різних мовах програмування, з іншими системами. Ключовими перевагами є розширювані бібліотеки блоків, підтримка різних типів моделей і можливість імітації нелінійних та складних систем.

Процес розробки системи можна поділити на кілька етапів. Спочатку проводиться аналіз системи, на якому визначаються її основні властивості та функції. Наступним кроком є постановка задачі, що включає опис мети та завдань, які має вирішити система. На третьому етапі вибирається метод проектування, і для цієї системи обрано використання нечіткої логіки. Четвертий етап передбачає вибір інструменту для автоматизованого проектування, і для цієї мети вибрано Simulink в складі MATLAB. Останнім етапом є тестування системи, під час якого перевіряється відповідність результатів, отриманих у ході тестування, з очікуваними результатами, зазначеними на етапі постановки задачі.

Рисунок 1.7 – Запропоноване дерево рішень

1.4 Висновки до розділу 1

У першому розділі розглянуто сучасні апаратно-програмні засоби для ідентифікації працівників на підприємствах. Основна увага приділена системам ідентифікації та аутентифікації (CIA), які забезпечують захист доступу до

корпоративних мереж і охоронюваних зон. Було проаналізовано переваги та недоліки різних типів ідентифікаційних технологій, включаючи електронні, біометричні та комбіновані системи.

Визначено ключові характеристики біометричних систем, таких як сканування відбитків пальців, розпізнавання обличчя, геометрія кисті руки та ідентифікація за райдужною оболонкою ока. Біометричні методи ідентифікації показали високу точність і ефективність, особливо у сфері інформаційної безпеки. Окрему увагу приділено перспективам впровадження біометричних систем в Україні, зокрема їх економічній доступності та адаптації до потреб бізнесу.

Також розглянуто електронні засоби ідентифікації, зокрема системи на основі RFID-технологій, контактних і безконтактних смарт-карток, USB-ключів та комбінованих пристроїв. Було підкреслено переваги таких систем, як зручність використання, довговічність і висока швидкість обробки, а також зазначено можливі недоліки, такі як вартість обладнання або залежність від зовнішніх умов.

Проаналізовані рішення показали, що комбіновані системи, які використовують кілька ідентифікаційних ознак, забезпечують найвищий рівень захисту. Такі системи є перспективним напрямком розвитку технологій ідентифікації завдяки їхній універсальності та здатності адаптуватися до різних умов експлуатації.

Розділ завершується постановкою завдання розробки програмно-апаратної системи ідентифікації на основі нечіткої логіки. Використання цього підходу дозволить підвищити гнучкість і точність системи, що є важливим фактором для ефективного функціонування в умовах реальних сценаріїв.

2 МОДЕЛЬ СИСТЕМИ ІДЕНТИФІКАЦІЇ

2.1 Структурна схема моделі

Термін "нечітка логіка" вперше з’явився в кінці 60-х років XX століття і спочатку позначав будь-яку логічну систему, в якій існувало більше двох істинних значень. Сьогодні цей термін має два основних значення.

У вузькому розумінні нечітка логіка є розширенням багатозначної логіки. Однак її операції значно відрізняються як за формою, так і за змістом від операцій, властивих багатозначним логічним системам. Нечітка логіка в цьому сенсі є спеціалізованою багатозначною логікою, спрямованою на створення формальних основ для градуйованого підходу до нечіткості. Цей підхід, характерний для людського мислення, застосовується для визначення, чи має об’єкт певну властивість у повному обсязі або лише частково через її нечіткість. Наприклад, вислови "практично біла пляма" або "дуже потужний мотор" містять шкалу інтенсивності властивостей.

У більш широкому значенні нечітка логіка є розширенням нечіткої логіки у вузькому сенсі та має на меті створення математичної моделі природних людських міркувань, де важливу роль відіграє природна мова. В цьому контексті нечітка логіка збігається з теорією нечітких множин, що описує класи з нечіткими, розмитими межами.

Нечітка логіка в цілому є результатом застосування градуйованого підходу до формальних логічних схем. Важливо зазначити, що це не є наслідком безмежних узагальнень. Завдяки такому підходу нечітка логіка дає змогу розв'язувати проблеми, які були б неможливими для класичної логіки. Прикладом є класичні парадокси, такі як парадокс купи і парадокс лисої людини.

Парадокс купи стверджує, що одне зерно пшениці не утворює купи, і так само для двох, трьох і більше зерен. Відповідно, "купа" взагалі не існує. Парадокс лисої людини говорить, що людина без волосся або з одним волоском є лисою, і це справедливо для будь-якої кількості волосків, що призводить до висновку, що

всі люди – лисі. Ці парадокси виникають, коли властивості "бути купою" чи "бути лисим" трактуються як точні, без врахування нечіткості. Класична логіка не здатна розв'язати ці проблеми.

Пропоноване рішення, яке використовує нечітку логіку, ґрунтується на припущенні, що імплікація $F(x) \Rightarrow F(x+1)F(x)$, де $F(x)$ означає, наприклад, твердження "x зерен не утворюють купу", є істинною лише з певним ступенем впевненості, близьким до 1, наприклад, $1-\varepsilon$, де $\varepsilon>0$. За такого підходу парадокси, подібні до "парадоксу купи" або "парадоксу лисої людини", усуваються.

Нечіткі логічні операції базуються на основах класичної булевої логіки, де два твердження A і B можуть бути істинними або хибними, тобто приймати значення "1" або "0". Для цих двох тверджень існує 16 можливих логічних операцій, з яких лише п'ять мають змістовну інтерпретацію: кон’юнкція, диз’юнкція, виключне АБО, імплікація і еквівалентність. Таблиці істинності для цих операцій подані в таблиці 2.1 [15].

Таблиця 2.1 – Таблиці істинності в булевій логіці

A	B	$A \wedge B$	$A \vee B$	$A \oplus B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Нечітка логіка є особливим типом багатозначної логіки, де значення істинності визначаються за допомогою лінгвістичних змінних або термінів, які відображають рівні достовірності. Основою для розробки операцій нечіткої логіки є булеві логічні операції, які узагальнюються відповідно до специфіки цієї системи [15].

Переваги нечітких систем у порівнянні з іншими методами полягають у наступному:

– здатність працювати з неточними або нечіткими вхідними даними, наприклад, величинами, які змінюються з часом, що є важливим для розв'язання динамічних задач;

– можливість формалізації нечітких критеріїв для оцінки і порівняння, що забезпечує гнучкість в аналізі;

– здатність проводити якісну оцінку як вхідних даних, так і отриманих результатів, враховуючи не лише значення, але й ступінь їх імовірності та розподіл;

– ефективне моделювання складних динамічних систем із можливістю порівняльного аналізу: нечіткі методи дозволяють описувати поведінку систем без потреби у точному визначенні змінних або побудові складних математичних моделей, економлячи час та забезпечуючи прогнозування результатів [16].

Хоча математичні основи нечіткої логіки активно розвиваються, процес її вдосконалення триває. Це зумовлено складністю моделювання природної мови, яке є ключовим елементом у створенні рішень на основі нечіткої логіки, що розширює її можливості для різних застосувань.

Формалізація нечіткої множини ґрунтується на узагальненні концепції належності. У класичній теорії множин існує кілька способів визначення множин, одним з яких є характеристична функція.

Нехай U – універсальна множина, x – елемент U, а R – деяка властивість.

Звичайна (чітка) підмножина A універсальної множини U, елементи якої задовольняють властивість R, визначається як множина впорядкованих пар $\mathrm{A} = \{\mu_A(x)/x\}$, де $\mu_A(x)$ – характеристична функція, що приймає значення 1, якщо x задовольняє властивість R, і 0 – в іншому випадку [14].

Розглянемо множину , що містить всі числа від 0 до 10. Визначимо підмножину множини , яка містить всі дійсні числа від 5 до 8. Далі розглянемо функцію належності множини , яка надає значення 1 або 0 кожному елементу множини , в залежності від того, чи належить цей елемент підмножині . Результати представлені на рисунку 2.1.

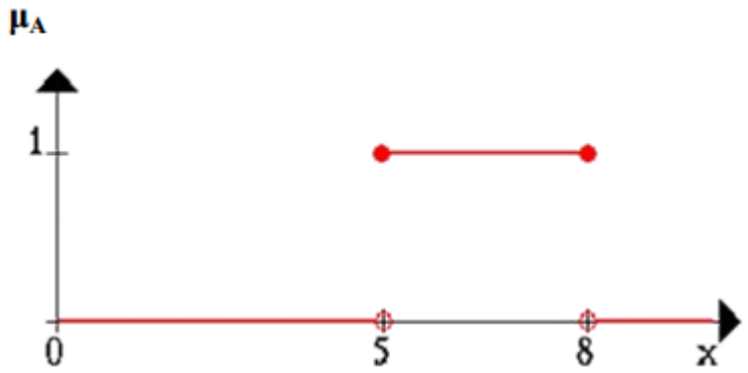

Рисунок 2.1 – Функція належності множини А

Елементи, які відповідають значенню 1, можна розглядати як такі, що належать множині А, а елементи, що відповідають значенню 0, як ті, що їй не належать. Цей підхід застосовується в багатьох сферах, однак є випадки, коли він виявляється занадто обмеженим. Нечітка підмножина відрізняється від звичайної тим, що для елементів з універсальної множини немає однозначної відповіді на питання про належність до певної властивості . Тому нечітка підмножина множини визначається як множина впорядкованих пар , де є характеристичною функцією належності, значення якої належать певному впорядкованому інтервалу , зазвичай . Ця функція вказує на рівень належності елемента підмножині . Множина називається множиною належностей. Якщо , тоді нечітка підмножина може трактуватися як чітка множина. Таким чином, нечіткі множини є природним узагальненням чітких, коли характеристична функція може приймати будь-які значення на відрізку , а не лише 0 або 1.

Розглянемо множину молодих людей. Формально це можна записати як *B={множина молодих людей}*. Оскільки вік починається з 0, нижня межа цієї множини дорівнює нулю. Верхню межу встановити складніше. Припустимо, верхня межа дорівнює 20 років, і множина стає обмеженим інтервалом . Однак постає питання: чому особа, яка в день свого 20-річчя є молодою, на наступний день вже не вважається молодою? Це викликає структурну проблему, і, змінюючи верхню межу, можна задати те ж питання з іншого боку.

Більш природним підходом є ослаблення чіткої границі між молодими та немолодими людьми. Для цього можна ввести більш гнучкі формулювання,

наприклад: "Так, він досить молодий", або "Ні, він вже не дуже молодий", замість чітких тверджень на кшталт "Так, він молодий" або "Ні, він не молодий".

Формально це можна представити як розширення концепції характеристичної функції. У попередньому прикладі всі елементи були кодовані лише значеннями 0 або 1. Для узагальнення цієї концепції можна ввести значення між 0 і 1, а в теоретичному випадку навіть необмежену кількість таких значень. Тепер інтерпретація значень у характеристичній функції стає складнішою: значення 1 вказує на те, що елемент належить множині *B*, значення 0 — що він не належить. Інші значення відображають ступінь належності елемента до множини *B* .

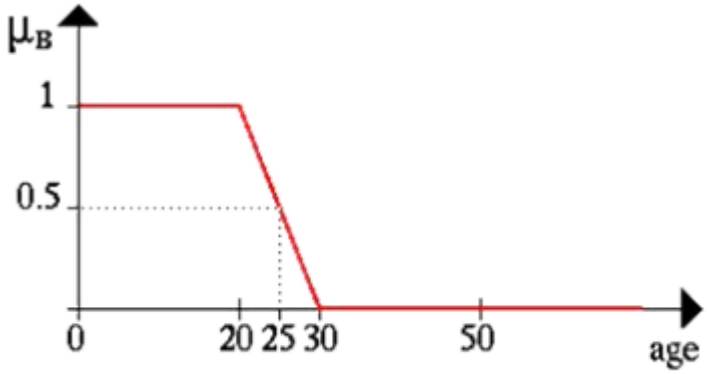

Рисунок 2.2 – Функція належності молодих людей

Розглянемо ще один приклад нечіткої множини. Формалізуємо поняття "гарячий чай". Для цього в якості *U* (області міркувань) використаємо шкалу температури в градусах Цельсія, яка змінюється в межах від 0 до 100 градусів. Нечітка множина для поняття "гарячий чай" буде визначена таким чином:

A = {0/0; 0/10; 0/20; 0,15/30; 0,30/40; 0,60/50; 0,80/60; 0,90/70; 1/80; 1/90; 1/100}.

Наприклад, чай з температурою 60°C належить множині "Гарячий" зі ступенем належності 0,80. Для однієї людини чай при такій температурі може бути достатньо гарячим, тоді як для іншої — лише помірно гарячим. Це ілюструє нечіткість визначення множини "гарячий чай", оскільки різні люди можуть по-

різному сприймати одну й ту ж температуру.

Множину *A* можна також представити у вигляді:

$$A = 0+0+0{,}15+0{,}30+0{,}60+0{,}80+0{,}90+1+1+1.$$

Функція належності не є ймовірністю, оскільки відсутня функція розподілу та немає повторних експериментів. Наприклад, при прогнозуванні погоди, коли потрібно вибрати одну з двох взаємовиключних подій — дощ чи відсутність дощу — і присвоїти їм певні ранги, то сума цих рангів не обов'язково дорівнюватиме 1. Однак, якщо рівність дійсно має місце, то нечітка множина вважається нормованою. Значення функції належності зазвичай визначаються за допомогою апріорних знань або опитувань експертів.

Функції належності можуть будуватися двома основними способами. Один із них — це прямий метод, у якому експерт або задає значення для кожного x з універсальної множини U, або формулює функцію належності аналітично, використовуючи математичні вирази. Цей підхід часто застосовується для оцінки таких параметрів, як швидкість, час, відстань, тиск чи температура, а також у випадках, коли важливо визначити граничні значення.

Прямі методи також можуть включати групові підходи. Наприклад, групі експертів демонструють певний образ, і кожен учасник відповідає на питання: "Ця людина лиса?" або "Ця людина не лиса?". Частка позитивних відповідей у загальній кількості експертів буде використовуватися для визначення значення μ"лисий" для даного образу.

У практиці часто спостерігається суб’єктивна тенденція, коли експерти схиляються до оцінок, розташованих на крайніх точках оціночної шкали. Тому прямі методи, які передбачають безпосереднє визначення значень функцій належності, зазвичай застосовуються лише тоді, коли ймовірність таких помилок є незначною або малоймовірною.

Непрямі методи визначення значень функцій належності використовуються в тих випадках, коли відсутні елементарні вимірювальні

характеристики для визначення нечіткої множини. Наприклад, поняття "краса", яке є значно складнішим і важче формалізованим, на відміну від таких понять, як "довжина" чи "висота". У таких ситуаціях зазвичай застосовуються рангові методи, при яких об'єкти порівнюються попарно, і встановлюються переваги одного об'єкта перед іншим.

У рамках непрямих методів значення функції належності вибираються таким чином, щоб задовольняти вже визначені умови. Експертні дані є лише вихідними для подальшої обробки. Можливі додаткові умови, що накладаються як на вид отримуваної інформації, так і на саму процедуру обробки. До таких умов може належати, наприклад, вимога, щоб функція належності відображала близькість до певного еталону або щоб результат обробки задовольняв умови інтервальної шкали.

Непрямі методи більш трудомісткі, ніж прямі, але їхня перевага полягає в стійкості до спотворень в оцінках. Як і прямі методи, непрямі можуть застосовуватись як для одного експерта, так і для групи експертів.

Базою для нечіткого логічного висновку є набір правил, що містять нечіткі висловлювання типу "Якщо щось", а також функції належності для відповідних лінгвістичних термінів. При цьому мають бути виконані такі умови:

1) для кожного лінгвістичного терміна вихідної змінної повинно бути хоча б одне правило;

2) для будь-якого терміна вхідної змінної має існувати хоча б одне правило, де цей термін виступає як передумова (ліва частина правила).

Загалом, процес нечіткого логічного висновку включає чотири етапи: фазифікація (введення нечіткості), нечіткий висновок, композиція та дефазифікація (переведення до чіткості) (рисунок 2.3)[17]

Алгоритми нечіткого висновку здебільшого відрізняються типом застосовуваних правил, логічних операцій та специфікою методу дефазифікації. Різні моделі нечіткого висновку, зокрема моделі Мамдані, Сугено, Ларсена та Цукамото, були розроблені для вирішення різноманітних задач у нечітких системах.

Рисунок 2.3 – Загальна схема нечіткого висновку системи

Зупинимося детальніше на механізмі нечіткого висновку Мамдані (Mamdani), оскільки це один із найпоширеніших методів в нечітких системах. Він використовує мінімаксну композицію нечітких множин і охоплює наступну послідовність операцій [18]:

1. Процес фазифікації: визначаються ступені істинності, що відповідають значенням функцій належності для лівих частин кожного правила (передумов). Для бази правил з *m* правил ступені істинності позначаються як:

$$A_{ik}(x_k), \text{ де } i=1\ldots..m,\ k=1\ldots..n; \tag{2.1}$$

2) Нечіткий висновок починається з визначення рівнів "відсікання" для лівих частин кожного правила:

$$\text{alfa}_i = \min(Aik(xk)) \tag{2.2}$$

Далі знаходяться “усічені” функції належності виходу:

$$B_i^*(y) = \min(\text{alfa}i, Bi(y)); \tag{2.3}$$

3) Композиція, або об'єднання усічених функцій, здійснюється за допомогою максимального об'єднання нечітких множин.

$$MF(y) = (B_i^*(y)), \tag{2.4}$$

де *MF* (*y*) - функція приналежності підсумкового нечіткої множини;

4) Дефазифікація, або процес повернення до чіткої форми, включає різні методи. Одним із таких є метод середнього центру, також відомий як центроїдний метод:

$$MF(y) = \max\left(B_i^*(y)\right), \tag{2.5}$$

Геометричне значення цього підходу полягає в знаходженні центру ваги для кривої MF (y). На рисунку 2.4 демонструється графічно процес нечіткого висновку за методом Мамдані для двох вхідних змінних і двох нечітких правил R1 та R2 [18].

Основним недоліком нечіткого висновку, побудованого на класичному механізмі Мамдані, є необхідність обробляти всю базу правил для будь-яких вхідних даних, що включає три етапи: визначення значень функцій належності для вхідних змінних, мінімаксну композицію та дефазифікацію. Такий підхід уповільнює роботу системи та потребує значних ресурсів пам'яті [16].

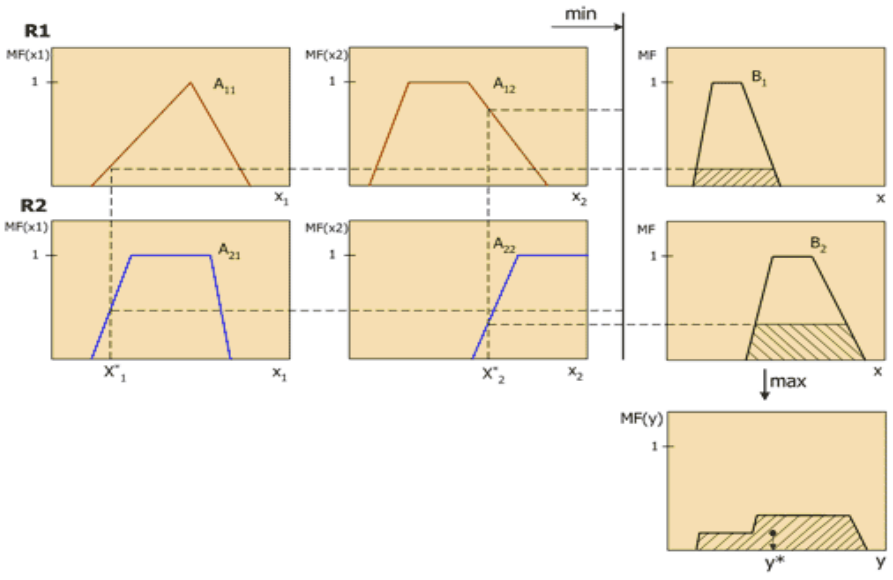

Рисунок 2.4 – Схема структурна нечіткого висновку Мамдані

Процес обробки нечітких даних за методом Мамдані полягає в розподілі етапів обробки вхідної нечіткої інформації на два основні етапи: навчання та

експлуатацію. Під час етапу навчання визначаються області функцій належності для вихідних значень кожного з правил. На етапі експлуатації спочатку здійснюється порівняння вхідних даних із значеннями функцій належності виходу, які зберігаються в пам'яті згідно з визначеними базою правил областями. Потім відсікаються значення функцій належності виходу, що перевищують вхідні дані. Після цього вибираються мінімальні значення відсічених функцій належності, з яких будується відповідна фігура. Завершальним етапом обробки є знаходження центру ваги цієї фігури, що утворюється в результаті додавання відсічених функцій належності. Схему алгоритму реалізації цього методу можна побачити на рисунку 2.5 [16].

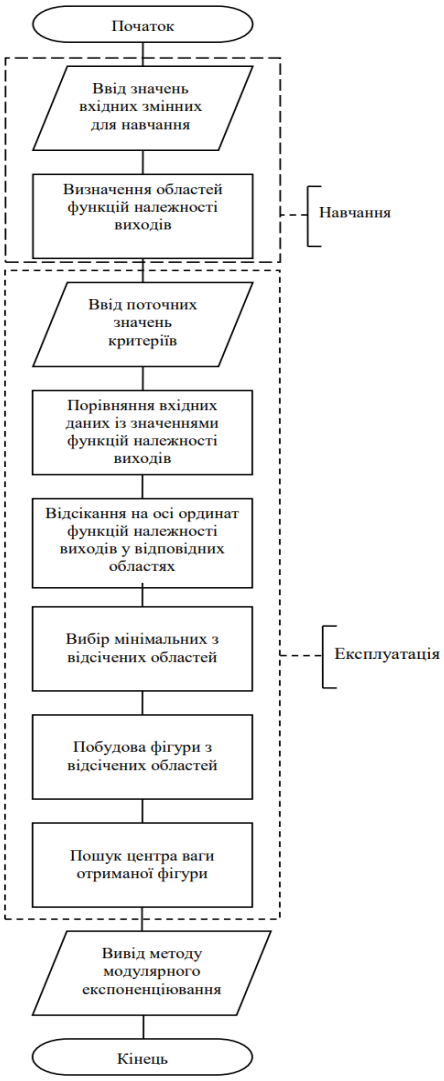

Рисунок 2.5 – Алгоритм обробки нечітких даних на основі методу Мамдані

Запропонований метод обробки нечітких даних, що базується на механізмі Мамдані, сприяє підвищенню ефективності систем, які вирішують інженерні задачі, завдяки розподілу процесу реалізації на етапи навчання та експлуатації.

Пропонована система ідентифікації працівників включає підсистему ідентифікації клієнта, командну підсистему та блок обробки інформації (рисунок 2.6)

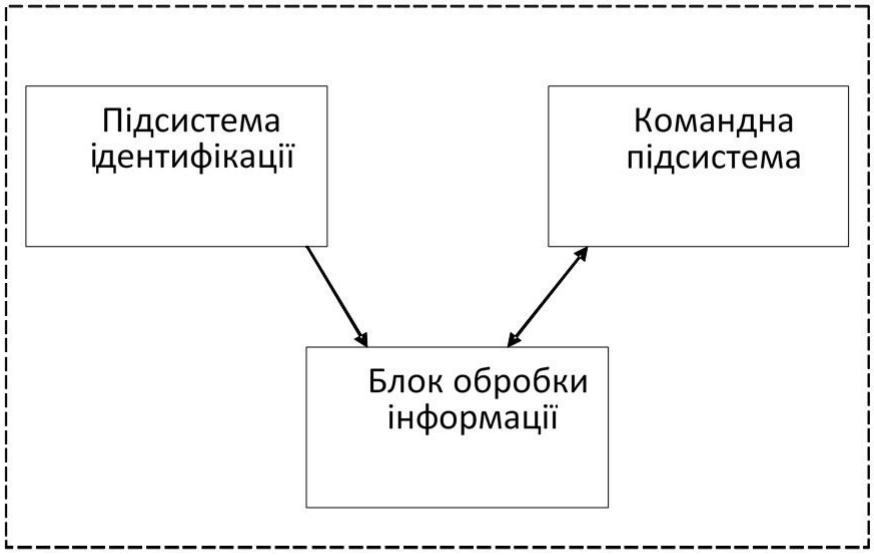

Рисунок 2.6 – Структурна схема процесу ідентифікації користувачів

Система ідентифікації передає до блоку обробки інформації дані про конкретного співробітника. Якщо користувач є новим для системи або має низький рівень довіри, система встановлює максимальний рівень стійкості, який дорівнює 1. У випадку, коли рівень довіри до співробітника високий, параметр стійкості може бути наближеним до 0, що позитивно впливає на продуктивність системи, зменшуючи час обробки.

Блок обробки інформації проводить аналіз отриманих даних і передає результат командній підсистемі, яка приймає рішення щодо доступу співробітника до підприємства. В середовищі Matlab розроблена модель системи ідентифікації представлена на рисунку 2.7.

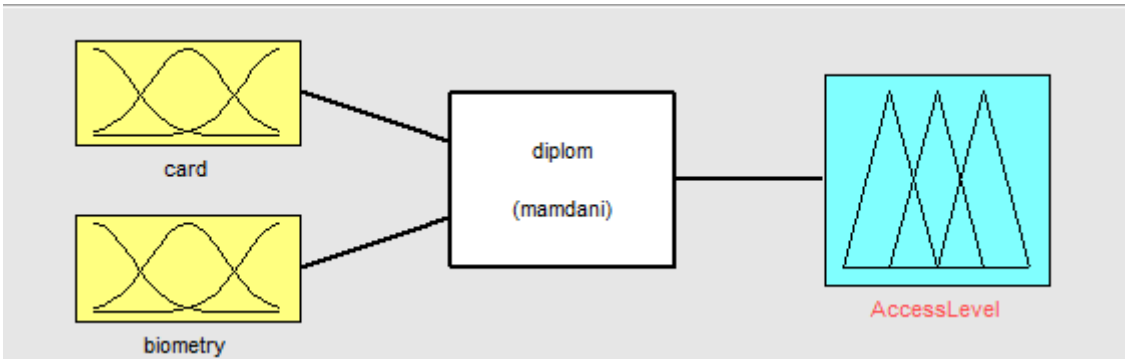

Рисунок 2.7 – Структурна схема розроблювального засобу ідентифікації працівника

Card та biometry — це вхідні параметри, які відповідають за зчитування даних з картки та біометричну ідентифікацію обличчя відповідно.

AccessLevel — це вихідний параметр, який має два можливі стани: "надавати доступ" або "не надавати доступ".

2.2 Реалізація проекту засобами MATLAB

Fuzzy Logic Toolbox — це розширення для MATLAB, що забезпечує набір інструментів для створення систем на основі нечіткої логіки. Він дозволяє розробляти експертні системи, здійснювати кластеризацію за допомогою нечітких алгоритмів, а також проектувати нечіткі нейронні мережі.

Пакет включає зручний графічний інтерфейс, який дає змогу покроково створювати нечіткі системи, і набір функцій для роботи в командному рядку, що дозволяє програмувати та автоматизувати процеси. Крім того, Fuzzy Logic Toolbox пропонує спеціальні блоки для інтеграції систем нечіткої логіки у середовищі Simulink. Всі алгоритми пакета реалізовані мовою MATLAB з відкритим вихідним кодом, що дозволяє користувачам модифікувати існуючий код, створювати власні функції та налаштовувати алгоритми під специфічні завдання [19].

Ключовим компонентом пакета є структура FIS (Fuzzy Inference System) — система нечіткого висновку. Ця структура містить всю необхідну інформацію для перетворення вхідних даних у вихідні значення на основі принципів нечіткої логіки. Основні етапи роботи FIS представлені у вигляді схеми (рисунок 2.8) [20].

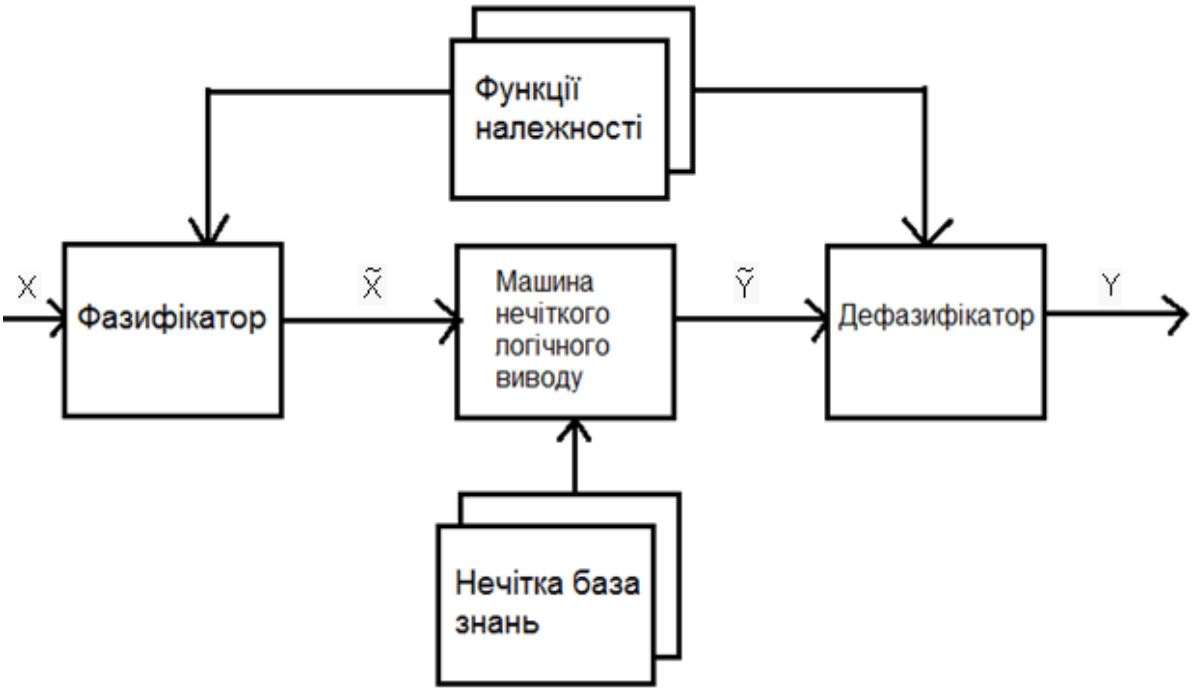

Рисунок 2.8 – Загальна схема нечіткого висновку

X – вхідне чітке значення;

$\tilde{X}$ - нечіткі множини, відповідні X;

$\tilde{Y}$ - результат логічного висновку у вигляді вектора нечітких множин;

Y – вихідне значення.

Основні переваги використання Fuzzy Logic Toolbox включають наявність графічного інтерфейсу для зручного покрокового проектування нечітких систем, а також функції для створення експертних систем на основі нечіткої логіки. Пакет підтримує використання логічних операцій І, АБО та НЕ в налаштовуваних правилах, а також дозволяє працювати з типовими моделями експертних систем нечіткої логіки, такими як Mamdani і Sugeno. Крім того, він містить функції для нейроадаптивної та нечіткої кластеризації з навчанням, інтеграції нечітких систем у Simulink-моделі та генерації С-коду для створення

незалежних додатків, що реалізують нечіткі системи логіки.

Завдяки Fuzzy Logic Toolbox у середовищі MATLAB 7.9.0 (R2009b) можна створювати нечіткі системи ідентифікації, які базуються на значеннях картки працівника та біометричних даних, таких як дані обличчя. Комбінація цих вхідних даних дозволяє точніше визначити рівень доступу до підприємства — або повний доступ, або відмову в доступі.

Значення функцій $_{\text{належності}}$ можуть бути задані різними типами функцій, такими як трапецевидні, дзвоноподібні або трикутні. У подальшій роботі будуть використовуватися дзвоноподібна та трикутна функції належності.

Синтаксис:

$$y = \text{gbell}_{\text{mf}}(x,\text{params}) \qquad (2.5)$$

Функція gbell_{mf} задає функцію належності у вигляді симетричної кривої у формі дзвону. Ця функція задається формулою

$$\mu(x) = \frac{1}{1+\left|\frac{x-c}{a}\right|^{2b}}, \qquad (2.6)$$

Параметри функції належності мають геометричну інтерпретацію наступним чином:

a — коефіцієнт, що визначає концентрацію функції належності;

b — коефіцієнт, який визначає крутизну функції належності;

c — координата, що відповідає максимуму функції належності.

Функція gbell використовується для побудови «гладких симетричних» функцій належності. Вона має два вхідних параметри:

1. x — вектор, для обчислення степені належності;

2. params — вектор параметрів функції належності, який задається в порядку [abc].

Функція gbellmf повертає результат у вигляді вектора y, який містить степені належності для кожної координати з вектора x.

Приклад:

```
x = 0: 0.1: 10;
y1 = gbellmf (x, [3 1 5]);
y2 = gbellmf (x, [3 2 5]);
y3 = gbellmf (x, [3 3 5]);
plot (x, [y1; y2; y3])
title (' gbellmf, a=3, b=1,…,3, c=5')
legend('b=1', 'b=2', 'b=3')
```

На рисунку 2.9 показано побудову графіку дзвоноподібних функцій належності з різними коефіцієнтами крутизни [21].

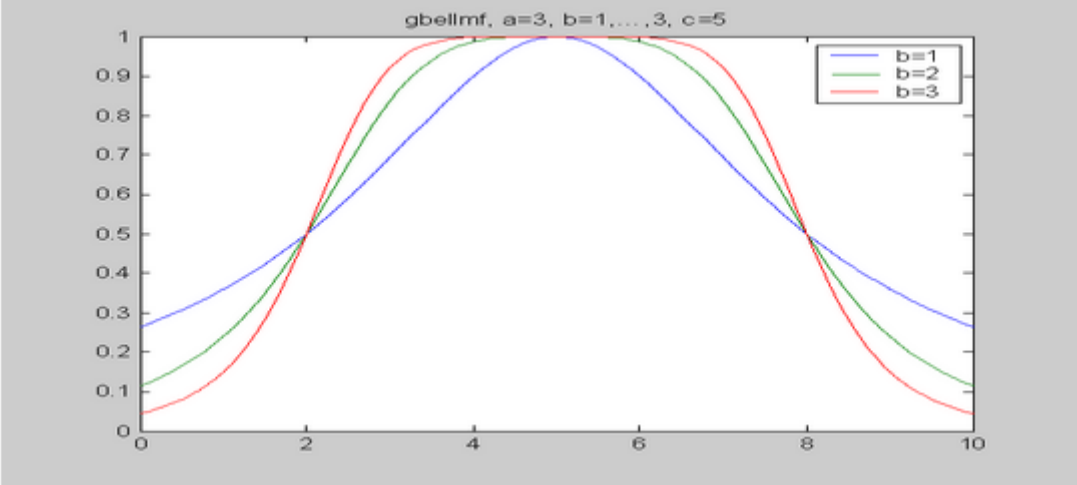

Рисунок 2.9 – Графіки дзвоноподібних функцій належності з різними коефіцієнтами крутизни

Трикутна функція належності [22].

Синтаксис:

$$y = \text{trimf}\ (x, \text{params}) \qquad (2.7)$$

Функція trimf визначає функцію належності у вигляді трикутника, що є

однією з найбільш простих і широко використовуваних форм належності.

Трикутна функція належності містить наступні параметри:

[a, c] — інтервал змінної;

b — значення змінної, яке є найбільш ймовірним.

Функція trimf має два вхідних параметри:

1. x — вектор, для координат якого потрібно обчислити степінь належності;
2. params — вектор параметрів функції належності, який вказується у порядку [abc]. Параметри повинні задовольняти умову $a \leq b \leq c$

Функція trimf повертає результат у вигляді вектора y, що містить степені належності для координат з вектора x.

Приклад:

```
x = 0: 0.1: 10;
y1 = trimf (x, [0 0 10]);
y2 = trimf (x, [0 3 10]);
y3 = trimf (x, [0 7 10]);
plot (x, [y1; y2; y3])
title (' trimf, a=0, b=0…7, c=10')
legend (‘b=0’, ‘b=3’, ‘b=7’)
```

Значення функцій належності для вхідних змінних, таких як card та biometry, задаються за допомогою дзвоноподібної функції, яка визначається чотирма параметрами (a, b, c, d), що представляють абсциси вершин дзвону. Для вихідної змінної output1 функція належності має трикутну форму, яка залежить від трьох параметрів (a, b, c), що визначають абсциси вершин трикутника. Моделювання нечіткого висновку проводиться за принципом Мамдані, як описано раніше. Функції належності для змінних card та biometry зображені на рисунках 2.10 і 2.11 відповідно, і поділені на три інтервали.

Для задання даних картки застосовуються змінні $small \in [0, 95]$, $middle \in [50, 210]$ та $high \in [175, 256]$.

Для задання даних біометрії обличчя пропонуються змінні $small \in [0,30]$, $middle \in [15,85]$ та $high \in [70,100]$, що відповідають малому, середньому та високому рівню.

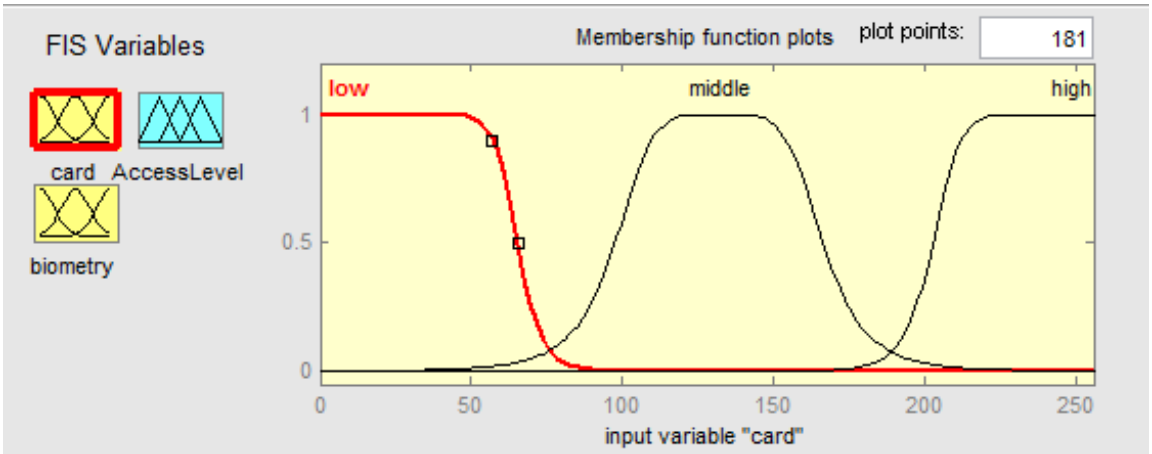

Рисунок 2.10 - Функції належності змінної *card*

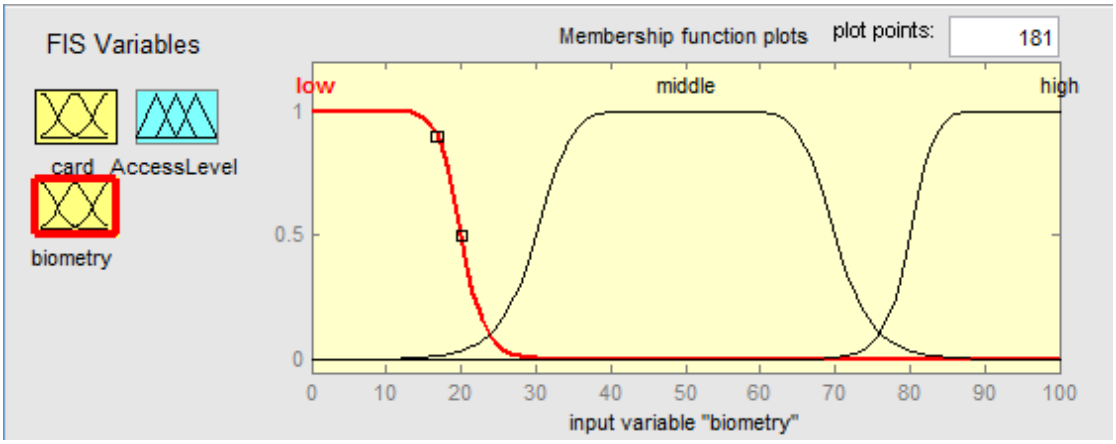

Рисунок 2.11 - Функції належності змінної *biometry*

Функції належності для вихідної змінної output1 представлені на рисунку 2.12. Вони позначені однаковими інтервалами на осі ординат, що дозволяє точно визначити центр ваги, який відображає нечіткий висновок системи.

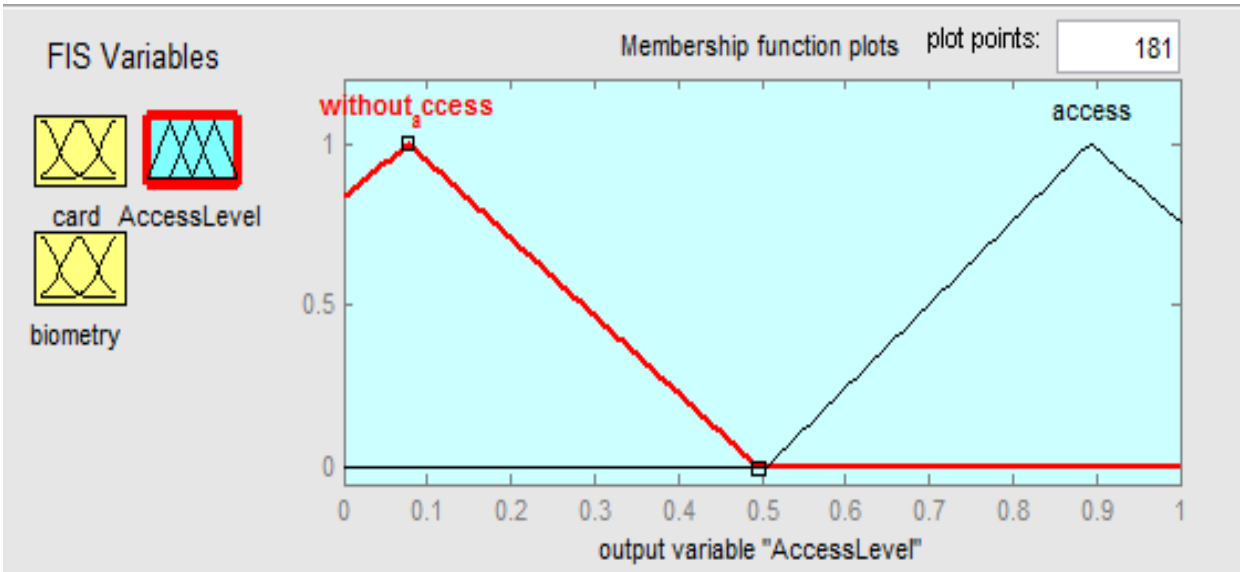

Рисунок 2.12 - Функції належності змінної *AccessLevel*

without_access це позначення означає відмову в доступі, а "access" — підтвердження доступу. База знань для створення цієї нечіткої моделі складається з правил типу «якщо - то», де кожна вхідна змінна має три нечітких стани, а також стан none, що позначає, коли значення вхідної змінної не задано системою. Оскільки випадок, коли всі вхідні змінні не мають значень, є практично неможливим, загальна кількість правил нечіткого висновку для цієї системи буде визначатися відповідно до конкретних умов.

2.3 Функційна симуляція проекту

Нечіткий висновок цієї моделі базується на 15 описаних вище правилах з поточними значеннями змінних «card», «biometry» та «accesslevel», представлений на рисунку 2.13.

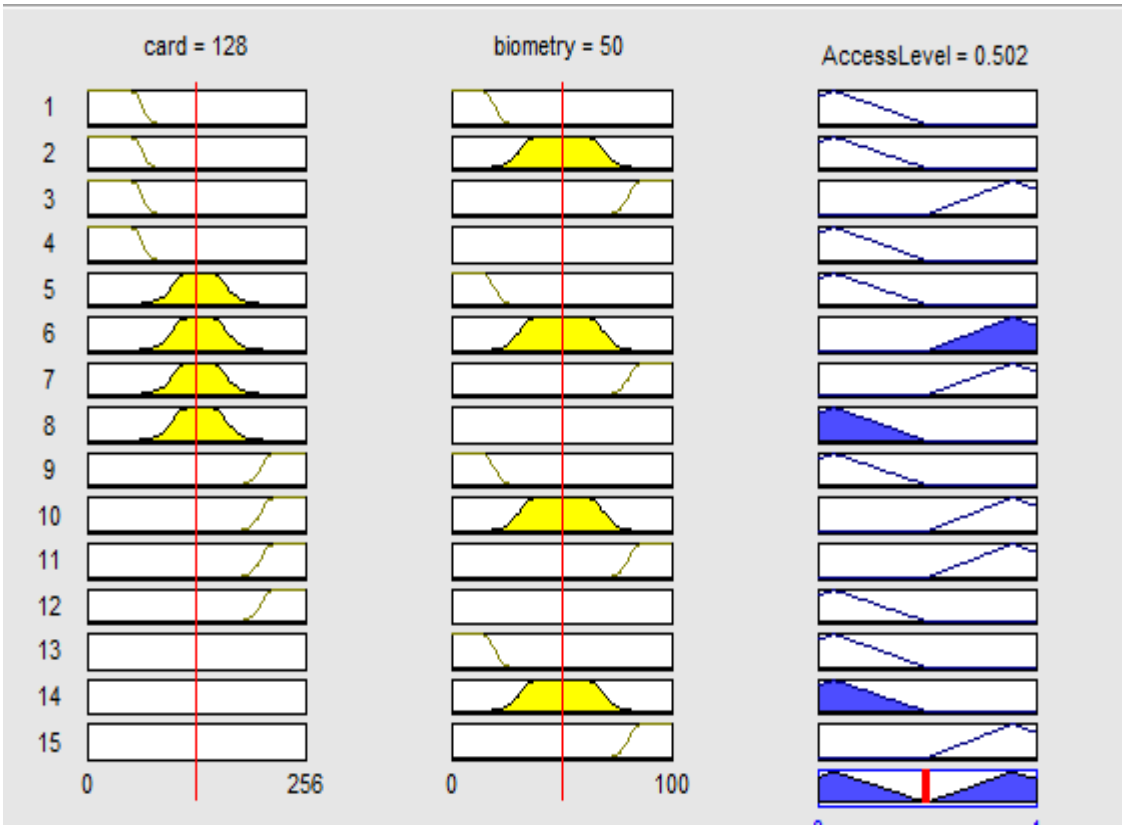

Рисунок 2.13 – Нечіткий висновок моделі

Змінюючи значення на входах системи від менших до більших і назад, можна перевірити коректність роботи розробленого пристрою (див. таблиця 2.2).

Таблиця 2.2 – Правильність роботи правил

Card	Biometry	AccessLevel
29,4	21,4	0,174
66,9	35	0,21
97,5	26,8	0,401
126	39,5	0,502
222	76,8	0,291
175	64,1	0,344
85,7	92,3	0,688

Поверхня значень нечіткої системи, побудованої на основі механізму

Мамдані, показана на рисунку 2.14, що підтверджує коректність конструкції бази правил нечіткого висновку.

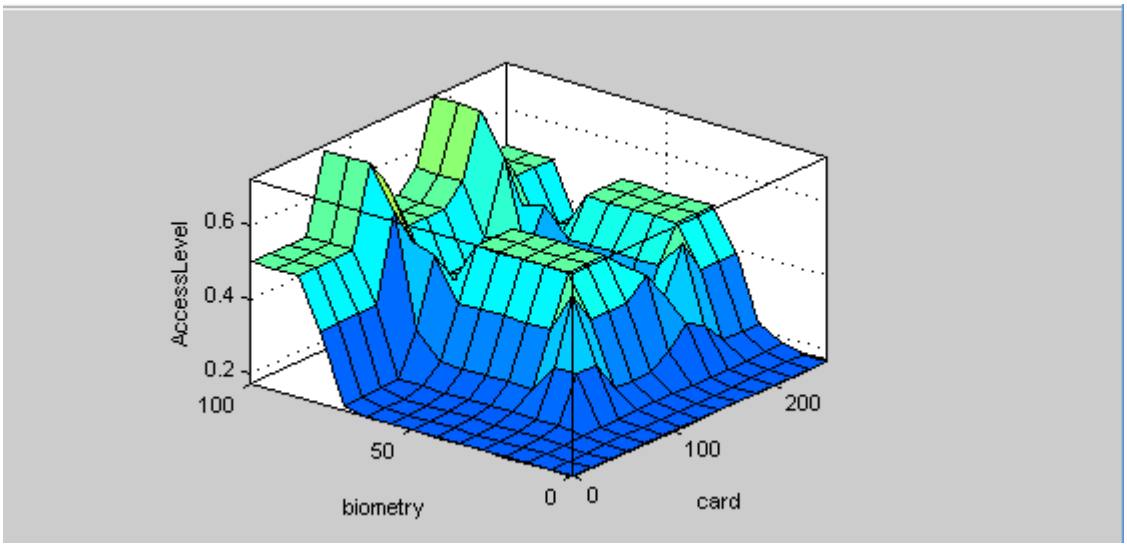

Рисунок 2.14 - Поверхня значень виходу нечіткої системи на основі механізму Мамдані

Головним недоліком нечіткого висновку, реалізованого за класичним механізмом Мамдані, є необхідність обробляти всю базу правил для будь-яких вхідних даних, що вимагає проходження через три етапи. Однак його основною перевагою є легкість розширення нечіткої системи через нові вхідні параметри та здатність працювати в режимі реального часу.

2.4 Висновки до розділу 2

У другому розділі описано розробку моделі системи ідентифікації працівників на основі нечіткої логіки, що забезпечує ефективну ідентифікацію за допомогою комбінації даних з картки працівника та біометричних параметрів, таких як обличчя. Було досліджено теоретичні основи нечіткої логіки, яка дозволяє працювати з неточними даними, надаючи системам ідентифікації

гнучкість і точність.

Запропонована модель включає використання нечіткої логіки Мамдані для прийняття рішень, пов’язаних з доступом до підприємства. Реалізація системи здійснюється в середовищі MATLAB із застосуванням інструменту Fuzzy Logic Toolbox. Використання цього програмного середовища забезпечує простоту проектування, моделювання та симуляції нечітких систем.

Розроблено функції належності для змінних, пов'язаних із карткою та біометрією. Вхідні параметри моделюються за допомогою дзвоноподібної та трикутної функцій належності.

Визначено базу правил нечіткого висновку, що складається з 15 правил, побудованих на комбінації вхідних змінних і вихідного рівня доступу.

Продемонстровано коректність роботи системи за допомогою симуляцій у MATLAB і графічного аналізу поверхонь значень вихідної змінної.

Використання нечіткої логіки забезпечує зменшення часу обробки даних та адаптивність системи до змін вхідних параметрів. Розроблена модель може бути основою для створення практичних систем ідентифікації, що відповідають сучасним вимогам безпеки та швидкодії.

3 РЕАЛІЗАЦІЯ ПРОЕКТУ НАДАННЯ ДОСТУПУ НА ПІДПРИЄМСТВІ

3.1 Модель розробленого нечіткого контролера засобами Simulink

Розробка системи надання доступу на підприємстві буде здійснюватися за допомогою програмного пакету Matlab, детально описаного в п. 1.3. Для реалізації буде використовуватися версія Matlab. Основні характеристики цієї версії програми включають такі особливості:

-вона підтримує роботу лише в середовищі Windows, хоча існує аналогічна версія для UNIX-систем (Linux, Solaris, Mac);

-наявність математичних та обчислювальних функцій;

-можливості для розробки алгоритмів;

-інструменти для візуалізації даних;

-підтримка зовнішніх інтерфейсів;

-використання MEX-файлів;

-доступність наборів інструментів.

.Matlab 7.9.0 містить велику кількість функцій для побудови графіків, включаючи тривимірні, а також інструменти для візуального аналізу даних та створення анімацій.

Вбудоване середовище розробки Matlab дозволяє створювати графічні інтерфейси користувача з різноманітними елементами управління, такими як кнопки, поля для введення та інші. Завдяки компоненту MATLAB Compiler, ці інтерфейси можуть бути перетворені в автономні додатки, для запуску яких на інших комп'ютерах необхідно мати встановлену бібліотеку MATLAB Component Runtime.

Для розробки моделі системи ідентифікації працівників підприємства використовується інструмент Simulink, що входить до складу Matlab. Він дозволяє виконувати симуляцію динамічних характеристик системи та переглядати результати вже під час проведення симуляції. Для забезпечення необхідної швидкості та точності симуляції, Simulink надає ODE-рішення з

фіксованим і змінним кроком, а також графічний відладчик та підпрограму для оцінки часу виконання окремих функцій моделі.

Для запуску Simulink у робочій області Matlab потрібно ввести команду simulink і натискати Enter. Після цього відкриється вікно бібліотеки Simulink (Simulink Library Browser)

Simulink Library Browser містить колекцію блоків, які найбільше використовуються для моделювання різних систем. До цієї бібліотеки входять:

-блоки для безперервної та дискретної динаміки, такі як Integrator (Інтегратор) і Unit Delay (Затримка);

-алгоритмічні блоки, наприклад, Sum, Product, Lookup Table;

-структурні блоки, такі як Mux, Switch, Bus Selector.

Для створення моделі необхідно спершу ініціювати новий проект (New Model), після чого відкрити робочу область та додати потрібні елементи. Для даної системи будуть використані наступні блоки (рисунок 3.1):

а) генератор випадкових чисел (Random Number);

б) осцилограф (Scope);

в) мультиплексор (Mux);

г) нечіткий регулятор (Fuzzy Logic Controller).

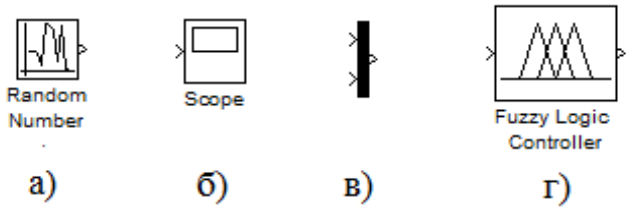

Рисунок 3.1 – Об’єкти для побудови моделі надання доступу

Оскільки система буде працювати на основі даних картки та біометричних відбитків, модель включатиме такі елементи:

-два генератори випадкових чисел, з іменами card і biometry;

-три осцилографи: два для вхідних сигналів (card1 і biometry1) та один для вихідного сигналу (access);

-мультиплексор для об'єднання двох вхідних сигналів;

-нечіткий регулятор (Fuzzy Logic Controller).

Fuzzy Logic Controller — це регулятор, побудований на основі нечіткої логіки. Для його реалізації необхідно:

1. визначити вхідні лінгвістичні змінні, наприклад, "час відвідування підприємства" і "частота відвідувань", які використовуватимуться для оцінки відвідуваності;

2. встановити лінгвістичну змінну, яку потрібно отримати — в даному випадку це "відвідуваність";

3. розробити правила для перетворення вхідних змінних в результуючу змінну.

Ця система має кілька практичних застосувань:

-може використовуватися окремо для виконання функцій лінійного перетворення в автоматизованому управлінні;

-застосовується для вирішення задач алгоритмічної обробки даних, таких як фільтрація;

-використовується в системах з нечіткою послідовністю перевірки статистичних гіпотез;

Модель нечіткого висновку, що базується на класичному механізмі Мамдані, представлена на рисунку 3.2.

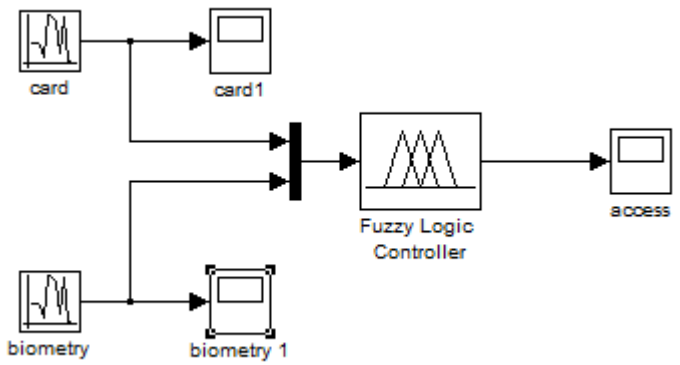

Рисунок 3.2 – Модель розробленого засобу

Вхідними даними для нечіткого контролера (Fuzzy Logic Controller), що працює на основі механізму Мамдані, є значення картки (card) та біометричних даних (biometry), а вихідним результатом є рівень доступу, який вказано в таблиці 2.2.

Щоб виконати симуляцію, необхідно спочатку вказати шлях до нашої системи в Fuzzy Logic Controller. Для цього потрібно двічі клацнути мишкою на параметрах Fuzzy Logic Controller, що відкриє вікно для введення шляху до системи (рисунок 3.3).

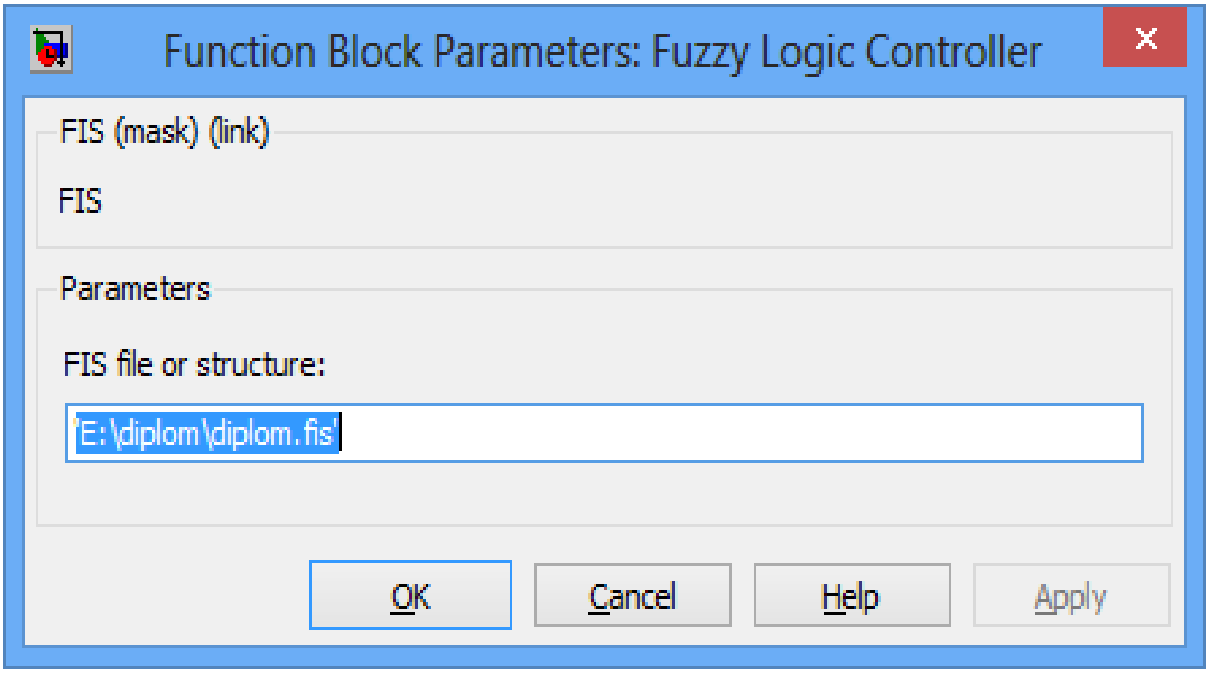

Рисунок 3.3 – Задання параметри нечіткого контролера

Після виконання зазначених дій, можна переглянути значення, які показує осцилограф. Для цього необхідно клацнути правою кнопкою миші на осцилографі картки і вибрати опцію "Look Under Mask". Така ж операція виконується для осцилографа, що відповідає за біометричні дані. Після завершення симуляції значення, що зчитуються з осцилографів, відображені на рисунках 3.4 та 3.5 відповідно.

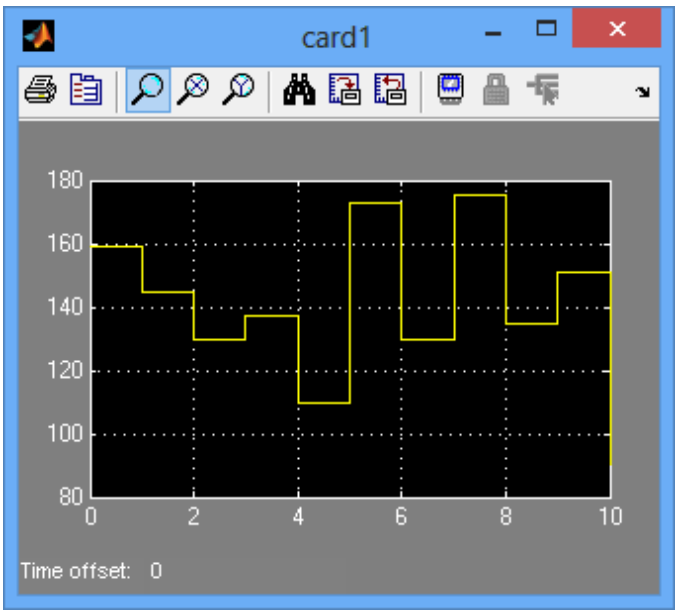

Рисунок 3.4 – Осцилограф картки

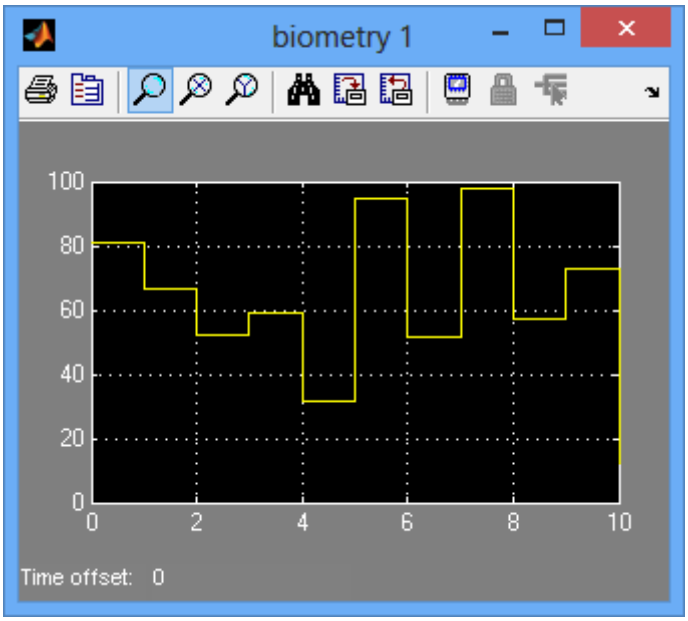

Рисунок 3.5 – Осцилограф біометрії

Як показано на рисунках 3.4 та 3.5, значення як картки, так і біометрії не перевищують попередньо заданих меж (256 і 100 відповідно). Рисунок 3.6 демонструє фрагмент схеми нечіткого контролера для ідентифікації працівників на підприємстві.

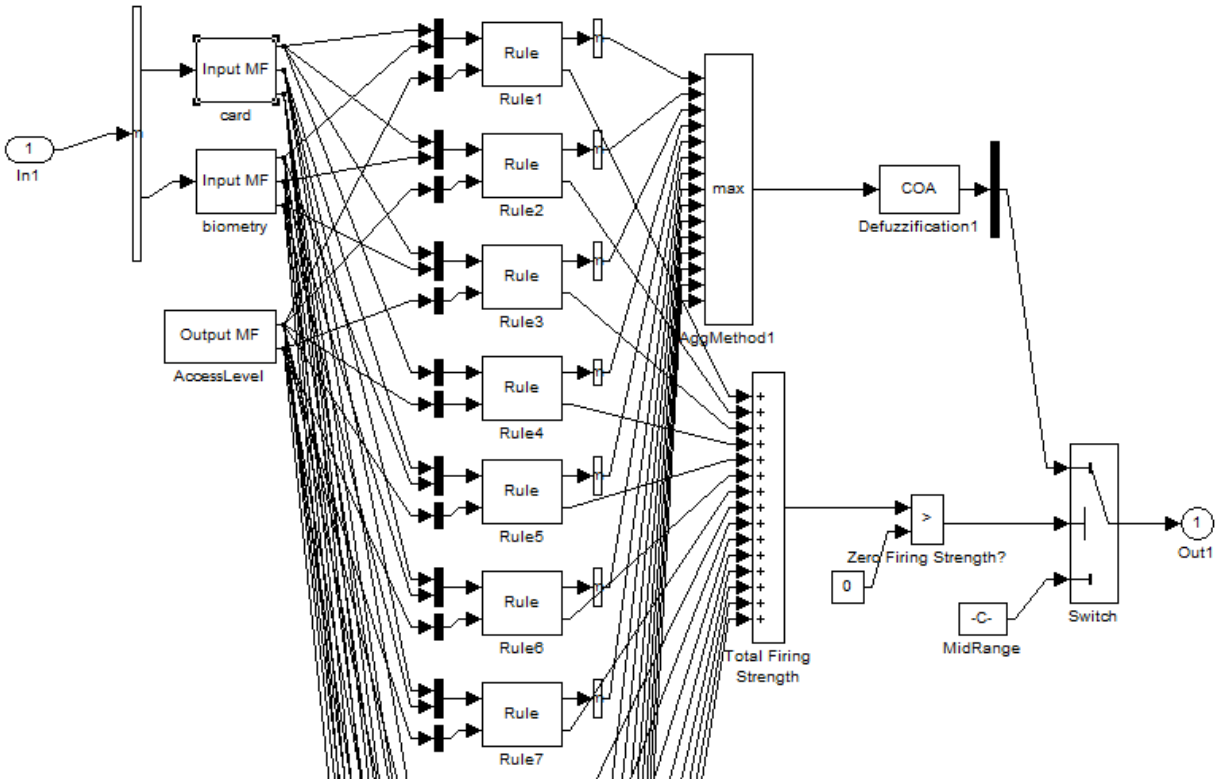

Рисунок 3.6 – Схема розробленого нечіткого контролера

Розроблена схема нечіткого контролера включає три блоки, що описують функції належності для вхідних змінних (блоки Input MF), блок для опису функцій належності вихідної змінної (Output MF), виходи яких передаються на вхід до 15 правил (блоки Rule 1 … 15).

3.2 Симуляція та верифікація нечіткого контролера

Схема обчислення функцій належності для вхідних та вихідної змінних, розроблена в середовищі Simulink, представлена на рисунках 3.7 та 3.8 відповідно.

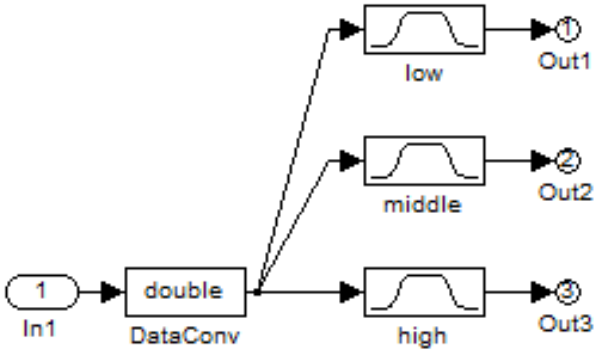

Рисунок 3.7 - Схема обчислення функцій належності вхідних зміних

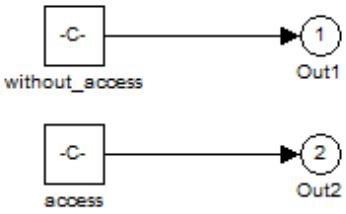

Рисунок 3.8 - Схема обчислення функцій належності вихідної змінної

Формування кінцевої фігури для обчислення центру ваги та обробки нечітких змінних здійснюється за механізмом Мамдані, описаним у п. 2.1, схема якого представлена на рисунку 2.4. Для обробки правил з бази знань Simulink враховує рейтинг, що відображається через константу Weight. Схема обробки нечітких значень показана на рисунку 3.9.

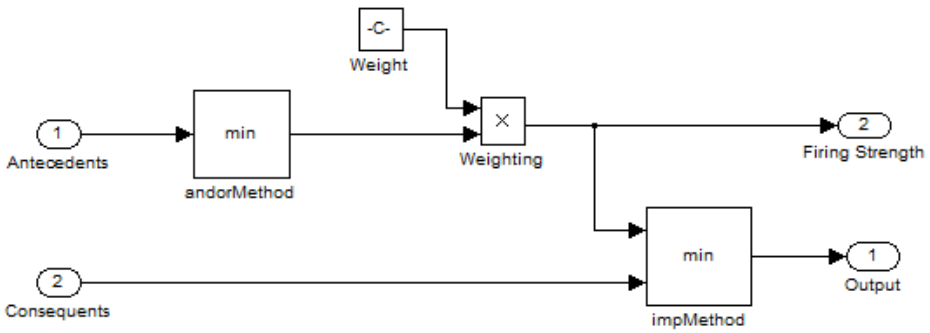

Рисунок 3.9 - Схема роботи бази правил

Вхідні змінні картки та біометрії є компонентами правила, що відповідають першому входу, а другий вхід визначає рівень доступу, який буде надано залежно від умов. Блок min виконує обробку даних, застосовуючи мінімальний закон. Виходи цієї схеми включають значення функції належності для рівня доступу (вихід 1) та послідовність, що визначає інтервал для цього виходу (вихід 2). Для обчислення центру ваги кінцевої фігури, яка формується після поєднання виходів усіх 15 правил, тобто виконання висновку за механізмом Мамдані, нечіткий контролер проводить дефазифікацію. Схема дефазифікації показана на рисунку 3.10.

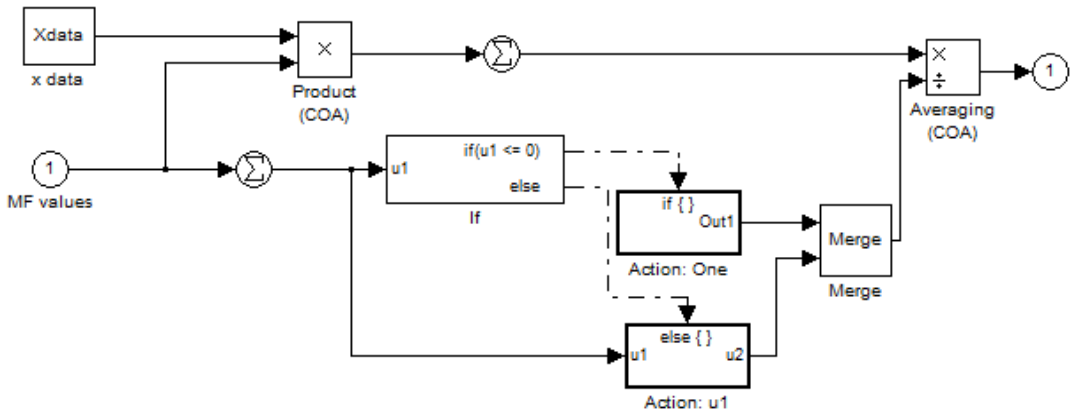

Рисунок 3.10 - Схема стуктурна здійснення нечіткого висновку

Дефазифікація виконується за наступною формулою:

$$r_{cv} = \frac{\sum_{j=1}^{m} r_j \mu(r_j)}{\sum_{j=1}^{m} \mu(r_j)} \tag{3.1}$$

де m - кількість прямокутників, на які поділено кінцеву фігуру,

r_j - значення абсциси,

$\mu(r_j)$ - значення ординати j-ї фігури.

Як результат роботи моделі з вхідними даними картки та біометрії (детальніше див. рисунки 3.6, 3.7), отримується значення центру ваги, що зображене на рисунку 3.11.

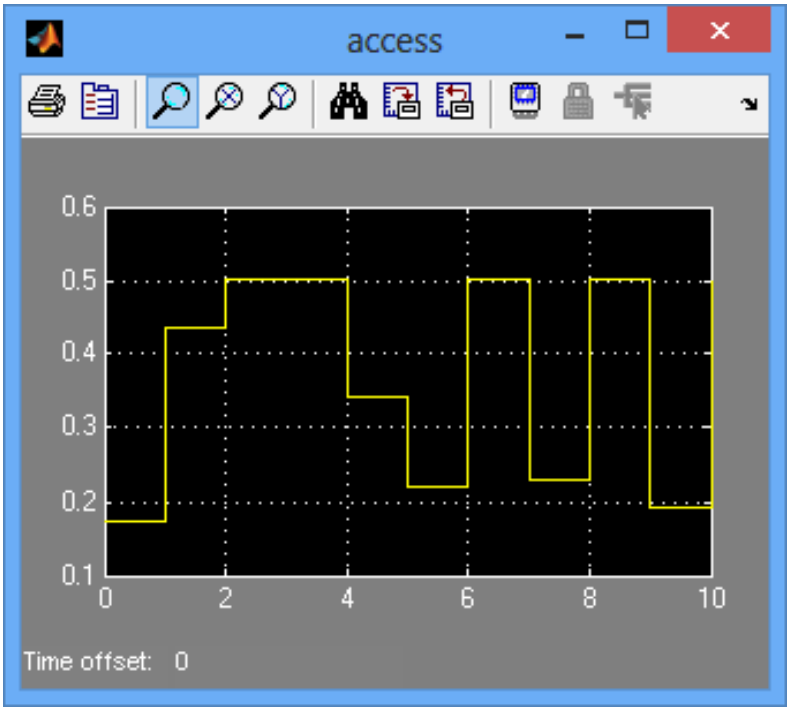

Рисунок 3.113 – Результати роботи розробленої нечіткої моделі

Тестові значення вхідних та вихідних змінних для нечіткої системи ідентифікації працівників підприємства наведені в таблиці 3.1.

Таблиця 3.1 – Тестові значення змінних нечіткої системи ідентифікації працівників підприємства.

№п/п	Card	Biometry	AccessLevel
1	160	81	0,17
2	147	69	0,45
1	2	3	4
3	131	57	0,51
4	140	61	0,52
5	110	32	0,33
6	177	97	0,22
7	129	51	0,5
8	178	99	0,25

Після аналізу таблиці 3.1 можна зробити висновок, що середнє відхилення результатів роботи системи від значень нечіткого контролера, що функціонує за механізмом Мамдані, становить не більше ніж 0,1. Ці результати підтверджують коректність функціонування та ефективність системи.

3.3 Стійкість розробленої нечіткої системи

Заходи захисту для системи ідентифікації працівників підприємства мають бути:

-відповідними до існуючих загроз;

-розробленими з урахуванням потенційних наслідків їх застосування;

-спрямованими на забезпечення ефективності захисту протягом визначеного періоду.

Нечітку систему ідентифікації співробітників можна реалізувати з використанням програмованих логічних матриць (ПЛМ) або програмованих логічних інтегральних схем (ПЛІС). Такий підхід гарантує захист даних, забезпечуючи конфіденційність, цілісність і приватність інформації, до якої надається доступ. Контролери, що застосовуються в цих системах, зазвичай випускаються у вигляді готових апаратних рішень.

Одним із основних недоліків програмного захисту порівняно з апаратним є його низька стійкість до зламу, а також знижена ефективність під час роботи з великими обсягами даних, що може призводити до збоїв у системі. Сучасні апаратні контролери, зокрема ті, що базуються на ПЛІС, мають суттєві переваги, включаючи високу продуктивність, надійність і стійкість до зовнішніх атак.

Програмовані логічні інтегральні схеми (ПЛІС) є елементами електроніки, що поєднують властивості репрограмованих пристроїв і дискретної логіки. Вони складаються з логічних блоків, з'єднаних вентильними схемами та матрицями переходів. ПЛІС мають низку переваг перед мікроконтролерами, зокрема

відсутність затримок при виконанні команд, що є важливим при використанні на критичних об'єктах.

ПЛІС надають можливість багаторазового програмування, що дозволяє користувачу налаштовувати систему відповідно до своїх потреб, не вносячи змін у друковані плати. Це значно підвищує надійність і спрощує процес проектування. Вони також дозволяють скоротити розміри апаратного забезпечення порівняно з великими інтегральними схемами.

Апаратні засоби захисту мають ряд переваг порівняно з програмними, зокрема:

-фізичний захист від несанкціонованого доступу;

-стійкість до атак "на відмову";

-неможливість віддаленого внесення змін у систему;

-автономність роботи.

Однак для належної роботи апаратних засобів необхідно забезпечити безперервне живлення, підтримку оптимальних умов навколишнього середовища та захист від фізичних пошкоджень і електромагнітних впливів.

Оскільки система ідентифікації є програмно-апаратною, важливим є також захист програмного забезпечення. Це буде здійснюватися через ідентифікацію користувачів, які при вході в систему вводять свої персональні дані, такі як ім’я користувача та пароль. У разі успішного введення користувач отримує доступ до певних об'єктів, а при спробі доступу до несанкціонованих об'єктів система видає повідомлення «У доступі відмовлено».

Для адміністрування доступу в мережі комп'ютерів можна використовувати інструменти, що містяться у додатку "Управління комп’ютером", доступ до якого здійснюється через Панель управління — Адміністрування — Управління комп’ютером.

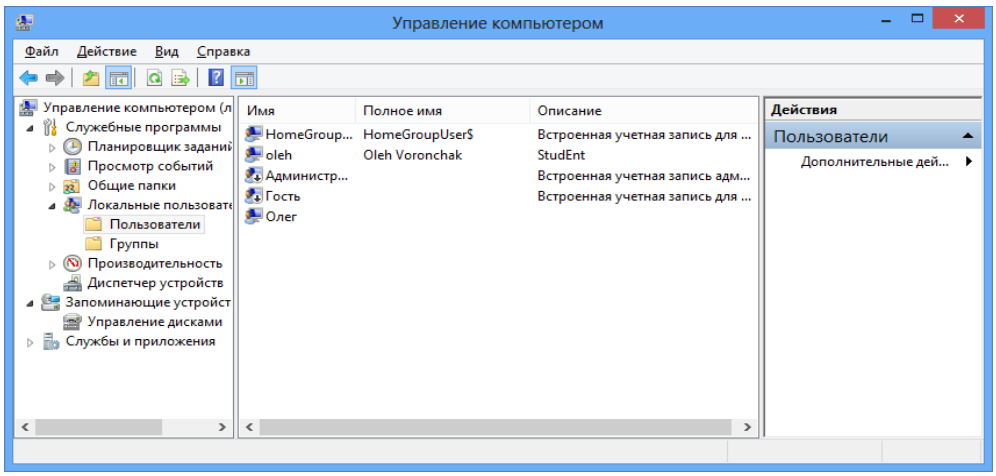

Рисунок 3.14 – Вікно додатку “Управління комп’ютером”

Основне вікно додатку містить всі ключові елементи, необхідні для управління системою. Процес входу користувача до системи здійснюється в кілька етапів:

1. перевірка наявності користувача з відповідними параметрами;
2. ідентифікація пароля;
3. перевірка прав доступу користувача до ресурсів системи.

В додатку "Управління комп’ютером" можна виконувати різні операції з користувачами, які зареєстровані в системі. Однією з основних можливостей є створення нового користувача. Для цього потрібно у меню "Користувачі" обрати пункт "Новий користувач", після чого відкриється вікно для введення даних нового користувача (рисунок 3.15).

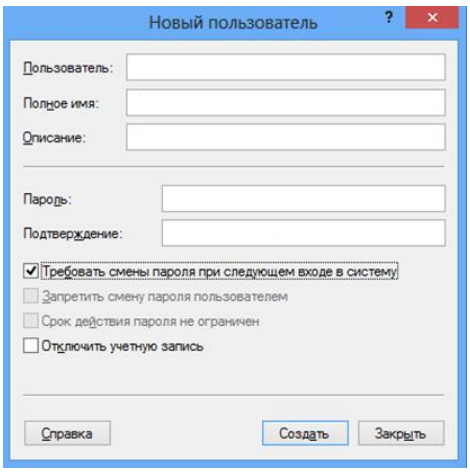

Рисунок 3.15 – Вікно створення нового користувача

При створенні нового користувача необхідно ввести основну інформацію (ім'я, короткий опис). Після цього система запропонує встановити пароль, який потрібно ввести двічі для підтвердження правильності.

Якщо при створенні користувача активувати опцію "Вимагати зміну пароля при наступному вході", то під час першого входу користувач спочатку введе поточний пароль, після чого зможе змінити його на новий і лише після цього отримає доступ до системи.

Так само, як і при створенні користувача, можна здійснити його видалення. Для цього в меню користувача потрібно вибрати пункт "Видалити" (рисунок 3.16).

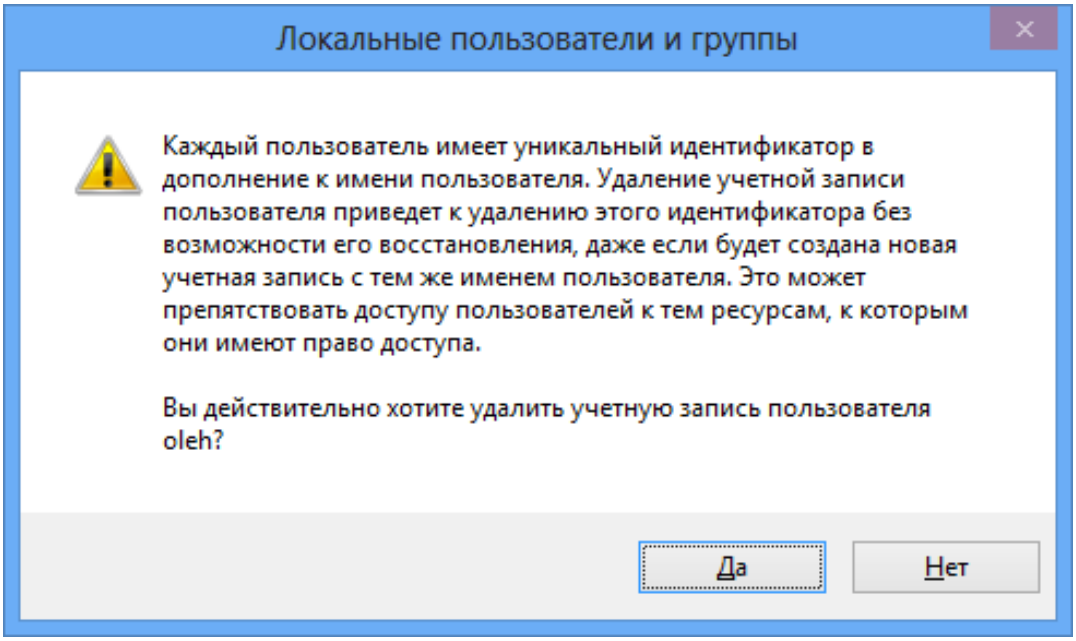

Рисунок 3.16 – Видалення користувача oleh

Існує важливий параметр, який визначає статус користувача як адміністратора. Суть полягає в тому, що навіть якщо користувач не має доступу до певних об’єктів програмного забезпечення, наявність параметра "адміністраторський доступ" надає йому повний контроль. Це означає, що незалежно від налаштувань груп доступу до конкретних об’єктів, активувавши цей параметр, користувач отримає без обмежень доступ до всіх частин

програмного забезпечення (рисунок 3.17).

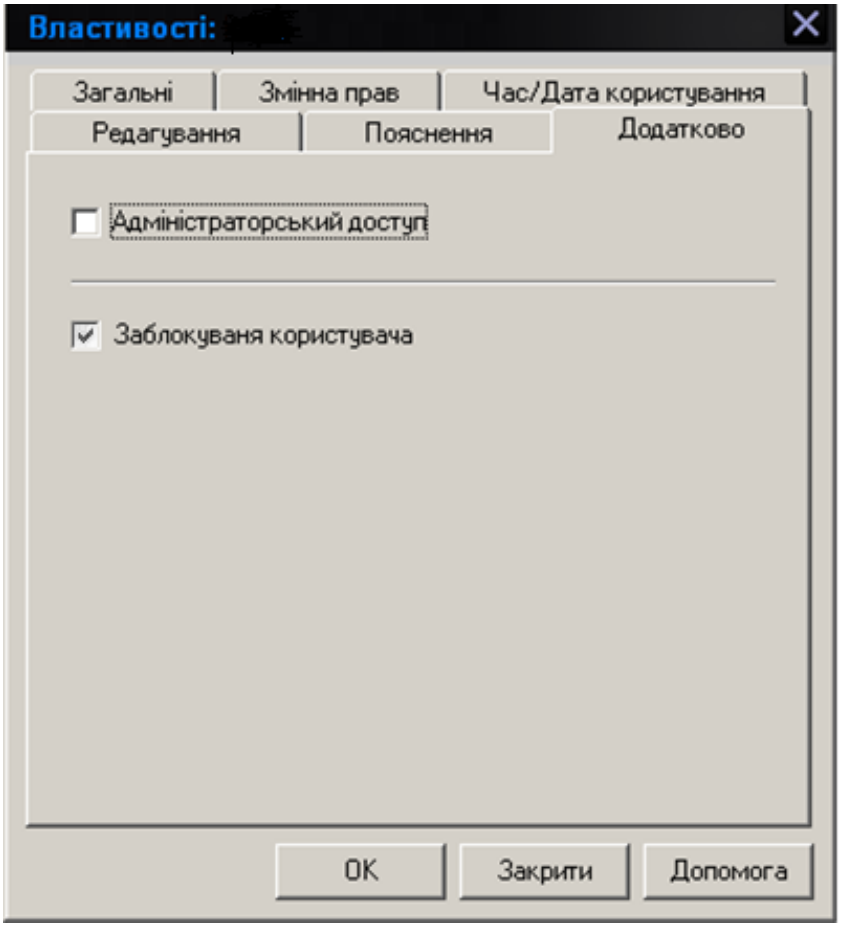

Рисунок 3.17 – Надання адміністраторського доступу/блокування користувача

У цьому ж вікні є можливість заблокувати користувача, для чого слід поставити відмітку в полі "Заблокувати користувача". Користувач залишатиметься заблокованим до того часу, поки адміністратор не зніме блокування. Перевага цього підходу в тому, що немає потреби видаляти користувача та створювати його заново. Така операція корисна, коли потрібно тимчасово позбавити користувача доступу до системи.

Крім того, для кожного користувача можна встановити обмеження на час перебування в системі. Для цього потрібно відкрити меню "Властивості" і задати необхідні параметри часу (рисунок 3.18).

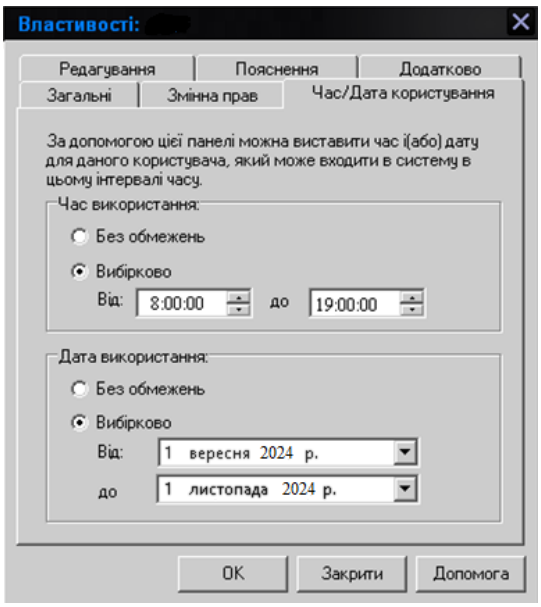

Рисунок 3.18 – Параметри користувача (час роботи)

Якщо потрібно обмежити доступ до системи на тривалий період, можна встановити обмеження за датою.

Захист програмного забезпечення, що використовує систему прав доступу для користувачів, є надійним засобом для запобігання несанкціонованому доступу. Така система може бути застосована в будь-яких комп'ютерних системах.

3.4 Висновки до розділу 3

Використання середовища Matlab та його компонента Simulink дозволило створити дієву модель системи доступу. Нечіткий контролер на основі механізму Мамдані забезпечує коректну обробку вхідних даних (картки та біометрії) і визначення рівня доступу з мінімальним відхиленням (до 0,1).

Результати симуляцій підтвердили точність функціонування розробленої системи, забезпечуючи надійну ідентифікацію працівників на основі заданих параметрів. Це свідчить про відповідність моделі поставленим вимогам.

Система є програмно-апаратною, що дозволяє поєднати переваги обох підходів. Використання програмованих логічних інтегральних схем (ПЛІС) забезпечує підвищену надійність, стійкість до збоїв і захист від атак.

Реалізація заходів із захисту даних і управління доступом (паролі, права користувачів, обмеження за часом) додає додатковий рівень безпеки для системи. Важливим є поєднання фізичних і програмних методів захисту.

Розроблена система може бути ефективно впроваджена в автоматизовані системи управління доступом, забезпечуючи високу точність і стійкість до зовнішніх впливів.

Таким чином, система ідентифікації співробітників, реалізована на базі нечіткого контролера, відповідає сучасним вимогам до безпеки і продуктивності, забезпечуючи ефективність роботи на підприємстві.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було здійснено наступне:

1. Проведено огляд сучасних систем ідентифікації, що показав чітку тенденцію до використання біометричних методів, оскільки цей тип розпізнавання є зручним і надійним для порівняння біометричного ключа (ознаки) з конкретним користувачем.

2. Розроблено алгоритм ідентифікації працівників підприємства на основі нечіткої логіки, на основі якого створена структурна схема пристрою, реалізація якого виконана з використанням Matlab та проведена його функціональна симуляція.

3. Здійснено впровадження розробленого проекту за допомогою Simulink була побудована модель нечіткого контролера та перевірено його коректність роботи, що дозволяє застосовувати розроблений контролер в реальних системах охорони підприємств. Отримані в ході функціональної симуляції результати співпали з тими, що були отримані при перевірці нечіткого контролера за допомогою Simulink. На підставі цього можна зробити висновок, що розроблений апаратно-програмний засіб спроектований правильно та працює коректно.

Запропонований алгоритм нечіткого управління системи охорони підприємства може бути реалізований у вигляді програмного чи апаратного засобу, залежно від потреб та можливостей користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про запровадження 12-ти бальної шкали оцінювання навчальних досягнень учнів у системі загальної середньої освіти // Початкова школа. – 2000. – № 4. – С. 31-33.

2. Закон України «Про освіту» (статті 12, 32, 33). URL :www.golos.com.ua/article/294010

3. Закон України «Про повну загальну середню освіту» (статті 10, 11, 14, 17, 35). URL : osvita.ua/legislation/law/2232

4. Критерії оцінювання навчальних досягнень учнів (вихованців) у системі загальної середньої освіти // Інф. зб. та коментарі Міністерства освіти і науки України. 2011. № 4 – 5 – 6. С. 84 – 93.

5. Модельні навчальні програми з української мови. І цикл (1 –2 класи). URL : mon.gov.ua/osvita/zagalna-seredna-osvita

6. Нова українська школа: Концептуальні засади реформування середньої школи. URL : mon.gov.ua/новини %202016/12/05/Koncepziya.pdf

7. Про затвердження орієнтовних вимог оцінювання навчальних досягнень учнів із базових дисциплін у системі загальної середньої освіти // Інф. зб. та коментарі Міністерства освіти і науки України. 2013. № 22 – 23 – 24. С. 3 – 82.

8. Соловей М. І., Кудіна В. В., Спіцин Є. С. Професійно-педагогічнапідготовка майбутнього вчителя в кредитно-модульній системі організації навчання: Навч. посіб. Вид. 3-є, доповн. Київ : Ленвіт, 2013. С. 50 – 65.

9. Зайченко І. В. Педагогіка: підручник. Вид. 3-є, переробл. і доповн. Київ: Вид. Ліра, 2016. С. 268 – 281.

10. Kevin McMahan Distance Educators’ Desk Guide [Електронний ресурс]. – Режим доступу: http://www.bizresourses.com/learning/de_deskguide.html)

11. Гронлунд Норман, Е. Оцінювання студентської успішності [Текст] : практичний посібник / Е. Норман Гронлунд – К. : Навчально-методичний центр "Консорціум із удосконалення менеджмент-освіти в Україні", 2005. – 312 с.

12. Дем'яненко, О.О. Про методи оцінювання навчальних досягнень школярів з літератури і тести навчального призначення [Текст] / О.О. Дем'яненко // Зарубіжна література. – 2008. – №9. – С. 12-14.

13. Дем'яненко, О.О. Тестові завдання та їх використання на уроках [Текст] / О.О. Дем'яненко // Всесвітня література. – 2002. – №10. – С.54-55.

14. Дичківська, І.М. Інноваційні педагогічні технології [Текст] : навчальний посібник / І.М.Дичківська. – К. : Академвидав, 2004. – 218 с.

15. Загвоздкін, В.К. Портфель індивідуальних навчальних досягнень – щось більше, ніж просто альтернативний спосіб оцінки [Текст] / В.К.Загвоздкін // Шкільні технології. – 2004. – №3. – С. 32-36.

16. Конструювання тестів. Курс лекцій [Текст] : навч. посібник / Л.О.Кухар, В.П.Сергієнко. – Луцьк, 2010. – С.82-96.

17. Концепція літературної освіти (затверджено наказом МОН України від 26.01.2011 №58) [Електронний ресурс]. – Режим доступу: http://shkola.ostriv.in.ua/publication/code-331EB9DAC35A0/list-9cbf2d9326.

18. Ратушняк, О.М. Формування інтерпретаційної компетентності старшокласників у процесі вивчення зарубіжної літератури : дис… канд. пед. наук : 13.00.02 [Рукопис] / Ратушняк Олександр Михайлович. — К. : Інститут педагогіки АПН України, 2009. – 231 с.

19. Ситченко, А. До поняття навчального проектування на уроках літератури [Текст] [Електронний ресурс] / А.Ситченко. – Режим доступу http://www.ukrlit.vn.ua/article1/1877.html.

20. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень : навчальний посібник. – Запоріжжя:ЗНТУ, 2008. – 341 с.

21. Рідкокаша А.А., Голдер К.К. Основи систем штучного інтелекту.Навчальний посібник. Черкаси, "ВІДЛУННЯ – ПЛЮС", 2002. – 240 с.

22. Shushura O.M. Infological modeling of information systems subject industries in solving of fuzzy control tasks. Зв'язок. 2018. № 2. С. 53–56.

23. Желдак, Тимур Анатолійович. Нечіткі множини в системах управління та прийняття рішень :навчальний посібник /Т.А. Желдак, Л.С. Коряшкіна, С.А. Ус ; за редакцією С.А. Ус .– Дніпро :НТУ ДП,2020. – 386 с.

24. Золотухіна О.А., Шушура О.М. Функціональне моделювання інформаційної системи управління ресурсами підприємства в умовах невизначеності або недостовірності даних. Зв'язок. 2017. № 6. С. 52–57.

25. Івахів, Орест Васильович. Основи побудови систем керування з нечіткою логікою :навчальний посібник /О. Івахів, М. Наконечний. – Львів :Растр-7, 2017. – 129 с.

26. Кирик В. В. Математичний апарат штучного інтелекту в електроенергетичних системах. / В. В. Кирик. − Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2019. − 224с.

27. Коротка, Лариса Іванівна. Обчислювальний інтелект : теорія нечітких множин :навчальний посібник /Коротка Л.І., Зеленцов Д.Г., Науменко Н.Ю.,Ляшенко О.А., Солодка Н.О.– Дніпро :ДВНЗ УДХТУ,2020. – 161 с.

28. Методичні вказівки до виконання лабораторних робіт з дисципліни "Нечіткі моделі і методи обчислювального інтелекту" для студентів спеціальності 8.05010102 − Системи штучного інтелекту усіх форм навчання / Уклад.: С.О. Субботін. – Запоріжжя: ЗНТУ, 2015. – 50 с.

29. Ротштейн А. П. Проектування нечітких баз знань [Текст] : лабораторний практикум та курсове проектування : [навчальний посібник] / А. П. Ротштейн, С. Д. Штовба. − Вінниця : ВДТУ, 1999. – 65 с.

30. Черняк О. І., Захарченко П. В. Інтелектуальний аналіз даних: Підручник. Київ, 2014.

31. Chetverikov G., Puzik O., Vechirska I. Multiple-valued structures of intellectual systems//Proceedings of the with Internations Computer Sciences and Information Technologies (CSIT). 2016, 7589907. -pp. 204-207.

32. Chetverikov G.G., Vechirska I.D., Leshchinsky V.A. Mathematical modeling and design of multiple-valued logic elements of digital telecommunications networks // International Conference Proceedings Crimean Microwave and Telecommunication Technology (CriMiCo).-2014, 6959429. - pp. 354-355.

33. Зайченко Ю. П. Основи проектування інтелектуальних систем / Ю. П. Зайченко. – К. : Слово, 2004. – 353 с.

34. Кондратенко В. Ю. Об’єктно-орієнтовані моделі для синтезу інтелектуальних систем з нечіткою логікою / В. Ю. Кондратенко, В. С. Яценко // Праці Одеського національного політехнічного університету. – 2006. – С. 54–60.

35. Кондратенко Ю. П. Методи обробки нечіткої лінгвістичної інформації в задачах багатокритерійного прийняття рішень / Ю. П. Кондратенко, Є. В. Сіденко // Матер. 6-ї Міжн.наук.-практ. конф. Сучасні інформаційні та інноваційні технології на транспорті MINTT-2014. – Херсон, Травень 2014. – С. 161–163.

36. Куссуль Н. М. Інтелектуальні обчислення. Навчальний посібник (навчальний посібник з грифом МОН України) / Н. М. Куссуль, А. Ю. Шелестов, А. М. Лавренюк. – К. : «Наукова думка», 2006. – 186 с.

37. Ямпольський Л. С. Системи штучного інтелекту в плануванні, моделюванні та управлінні / Л. С. Ямпольський, Б. П. Ткач, О. І. Лісовиченко. – Київ : ДП «Видавничий дім «Персонал», 2011. – 544 с.

38. Fuzzy Logic Toolbox. User’s Guide. The MathWorks, Inc., 1999. – 134 p.

39. Kaufmann, A., Gupta, M. : Introduction to Fuzzy Arithmetic: Theory and Applications.Van Nostrand Reinhold Company, New York (1985).

40. Kondratenko, G., Kondratenko, Y., Sidenko, I.: Fuzzy Decision Making System for Model-Oriented Academia/Industry Cooperation: University Preferences. In : C. Berger-Vachon (ed.), Complex Systems: Solutions and Challenges in Economics, Management and Engineering 125, pp. 109–124. Springer, Cham (2018) DOI: 10.1007/978-3-319-69989-9_7.

41. Kondratenko, Y., Kondratenko, V. : Soft Computing Algorithm for Arithmetic Multiplication of Fuzzy Sets Based on Universal Analytic Models. In book:

V. Ermolayev et al. (eds.), Information and Communication Technologies in Education, Research, and Industrial Application. Communications in Computer and Information Science 469, ICTERI'2014, pp. 49–77. Springer International Publishing, Switzerland (2014) DOI: 10.1007/978-3-319-13206-8_3.

42. Kondratenko, Y., Kondratenko, N. : Real-Time Fuzzy Data Processing Based on a Computational Library of Analytic Models. DATA 3(4), 1–9 (2018).

43. Kondratenko, Y., Kondratenko, N. : Universal Direct Analytic Models for the Minimum of Triangular Fuzzy Numbers. In : V. Ermolaev et al. (eds.), ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. CEUR Workshop Proceedings. Volume II: Workshops, pp. 100–115. Kyiv, Ukraine (2018) CEUR-WS.org/Vol-2104/paper_208.pdf.

44. Kondratenko, Y. P., Kondratenko, N. Y. : Reduced Library of the Soft Computing Analytic Models for Arithmetic Operations with Asymmetrical Fuzzy Numbers. Int. J. of Computer Research 23(4), 349–370 (2016).

45. Kondratenko, Y. P., Kondratenko, N. Y. : Soft Computing Analytic Models foκ Increasing Efficiency of Fuzzy Information Processing in Decision Support Systems. Chapter in book: R. Hudson (ed.), Decision Making: Processes, Behavioral Influences and Role in Business Management, pp. 41–78. Nova Science Publishers, New York (2015).

46. Kondratenko, Y. P., Sidenko, E.V. : Correction of the Knowledge Database of Fuzzy Decision Support System with Variable Structure of the Input Data. In: International Conference on Modeling and Simulation MS'2012, pp. 56–61. Minsk, Belarus (2012).

47. Kondratenko, Y. P., Sidenko, I. V. : Decision-Making Based on Fuzzy Estimation of Quality Level for Cargo Delivery. In: L. Zadeh et al. (eds.), Recent Developments and New Directions in Soft Computing. Studies in Fuzziness and Soft Computing 317, pp. 331–344. Springer, Cham (2014). DOI : 10.1007/978-3-319-06323-2_21.

48. Kondratenko, Y. P., Sidenko, Ie.V. : Decision-Making and Fuzzy Estimation of Quality Level for Cargo Delivery. In: 2nd World Conference on Soft Computing, pp. 418–423. Baku, Azerbaijan (2012).

49. Kondratenko, Y. P., Sidenko, Ie. V. : Design and Reconfiguration of Intelligent Knowledge-Based System for Fuzzy Multi-Criterion Decision Making in Transport Logisticts. Journal of Computational Optimization in Economics and Finance. 6(3), 229–242 (2014).

50. Kondratenko, Y. P., Sidenko, Ie. V. : Method of Actual Correction of the Knowledge Database of Fuzzy Decision Support System with Flexible Hierarchical Structure. Journal of Computational Optimization in Economics and Finance. 4(2), 57–76 (2012).

51. Kondratenko, Y. P., Simon, D. : Structural and Parametric Optimization of Fuzzy Control and Decision Making Systems. In : L. Zadeh et al. (eds.), Recent Developments and the New Direction in Soft-Computing Foundations and Applications, Studies in Fuzziness and Soft Computing 361, pp. 273–289. Springer, Cham (2018) DOI: 10.1007/978-3-319-75408-6_22.

52. Березький О.М., Мельник Г.М. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Магістр”. Спеціальність: 123 - Комп’ютерна інженерія. Магістерська програма - Комп’ютерна інженерія". Тернопіль: ЗУНУ, 2024. 32 с.