МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Західноукраїнський національний університет

Кафедра комп'ютерної інженерії

**ПЕКЕЛЬНА Вікторія Вікторівна**

**Алгоритми вибору аутентифікації користувача на основі нечіткої логіки/ Algorithms for selecting users autentification based on fuzzy logic**

спеціальність: 123 - Комп’ютерна інженерія

освітньо-професійна програма - Комп’ютерна інженерія

Кваліфікаційна робота

Виконав студент

групи КІм-21

В. В. Пекельна

Науковий керівник:

к.т.н., доцент Л.О.Дубчак

Кваліфікаційну роботу допущено

до захисту:

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л. О. Дубчак

ТЕРНОПІЛЬ – 2022

ВСТУП

**Актуальність досліджень.** Система контролю та управління доступом (СКУД) - це комплекс технічних засобів і організаційних заходів, що забезпечують контроль доступу до об'єктів СКУД та контроль за пересуванням людей по території, що охороняється. На сьогодні АСУ визнано одним із найефективніших методів вирішення складних завдань безпеки об’єктів [1].

Дивлячись на постійне зростання інтересу до СКУД і перспективи їх широкого використання в найближчому майбутньому, не можна забувати, що СКУД лише спрощує процес ідентифікації, економить час і підвищує ефективність роботи служб безпеки компанії, але в той же час , все ще потрібен людський контроль. Необхідність вибору оптимального співвідношення між людьми і технічними ресурсами системи залежить від рівня ймовірних загроз і завдань, які ставляться перед системою. Встановлення системи контролю доступу дозволить не тільки підвищити рівень загальної безпеки, але й скоротити витрати на її забезпечення, оскільки САУ не потребують великої кількості персоналу для обслуговування, вони економні у споживанні електроенергії.

**Метою даного дипломного проекту** є розробка апаратно-програмних засобів ідентифікації працівників підприємства.

Важливою особливістю захисту від несанкціонованого доступу до певних об'єктів є захист за допомогою контролю доступу.

Необхідність створення надійних і зручних систем ідентифікації зумовлена збільшенням потоків конфіденційної інформації та інформаційних систем, призначених для її аналізу та обробки, а також об’єктивною вимогою інтелектуалізації та безпеки всіх форм взаємодії користувачів автоматизованих систем. управління. система з технічними засобами.

Забезпечення конфіденційності та дистанційної роботи систем контролю доступу в різних сферах їх застосування (в авіації - диспетчери, оператори, енергетичні системи, банківська справа та інші сфери) останнім часом набуло особливого значення.

Для досягнення мети необхідно вирішити наступні **завдання**:

1) здійснити аналіз сучасних засобів аутентифікації особи;

2) здійснити розробку методики побудови захищених засобів захисту інформації на основі біомедичних даних;

3) реалізувати та здійснити експериментальне дослідження розробленого програмного засобу.

**Об’єкт дослідження** – засоби аутентифікації користувача комп’ютерної системи.

**Предмет дослідження** ‒ алгоритми вибору аутентифікації користувача на основі нечіткої логіки.

**Методами дослідження** є теорія нечіткої логіки, логічні та арифметичні операції.

Для реалізації проекту використано теорію нечіткої логіки, яка дозволяє будувати системи, що працюють в реальному часі.

**Наукова новизна** полягає у вдосконаленні алгоритму аутентифікації користувача, що базується на нечіткій логіці.

**Практичне значення** одержаних результатів полягає у розробленому методі, що може застосовуватися у будь-якій системі захисту інформації.

**Публікації та апробації результатів досліджень** здійснено на науково-практичній конференції молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі», м.Тернопіль, 2022 р. ( додаток А).

**Впровадження результатів досліджень** здійснено в системі захисту підприємства (додаток Б).

Випускна кваліфікаційна робота складається з трьох розділів.

В **першому розділі** здійснено аналіз сучасних засобів ідентифікації користувача. Крім того, досліджено сучасні засоби та методи аутентифікації.

В **другому розділі** розроблено методи аутентифікації на основі нечіткої логіки. Проведено їх аналіз та доведено актуальність впровадження з метою захисту інформації.

**В третьому розділі** розроблено та здійснено реалізацію на рівні апаратних засобів для подальшого його застосування в системах захисту інформації.

1 СУЧАСНІ АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ІДЕНТИФІКАЦІЇ СПІВРОБІТНИКІВ КОМПАНІЇ

Основним методом захисту інформації від зловмисників є інтеграція так званої системи ідентифікації та аутентифікації (SIA). При використанні SIA співробітник отримує доступ до комп'ютера або корпоративної мережі тільки після успішного проходження процедури ідентифікації та аутентифікації.

Ідентифікація полягає у впізнаванні користувача за ознакою або присвоєним розпізнавальним знаком.

Перевірка особистості представленого ним користувача здійснюється в процесі аутентифікації [2].

Апаратно-програмне забезпечення SIA включає ідентифікатори, пристрої введення-виведення (зчитувачі, контактні пристрої, адаптери тощо) та відповідне програмне забезпечення.

За типом використовуваних ідентифікаційних ознак сучасні СІА поділяються на електронні, біометричні та комбіновані (рис. 1.1).

В електронних системах ознаки ідентифікації представлені у вигляді цифрового коду, який зберігається в пам'яті ідентифікатора. Такі SIA розробляються на основі таких ідентифікаторів [2]:

- ідентифікатори iButton (інформаційна кнопка - інформаційна «таблетка»);

- смарт-карта контактна (смарт-карта - інтелектуальна карта);

- безконтактні радіочастотні ідентифікатори (системи RFID);

- безконтактні смарт-картки;

- USB-ключі або USB-жетони (жетон - пізнавальний знак, маркер).

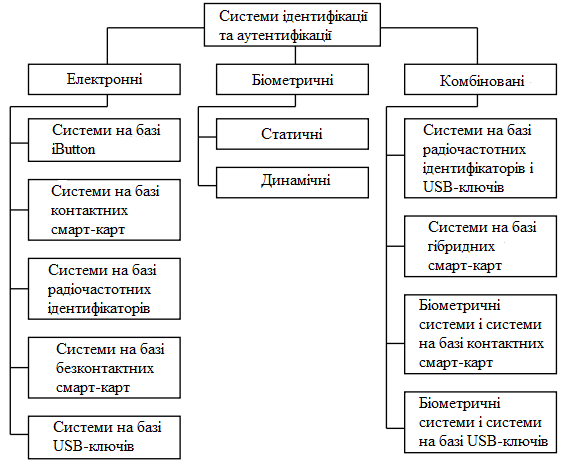


Рисунок 1.1 - Класифікація систем ідентифікації та автентифікації

У біометричних системах ідентифікаційними ознаками є індивідуальні характеристики людини, які називають біометричними. Цей тип ідентифікації та аутентифікації заснований на процедурі зчитування запропонованої користувачем біометричної ознаки та порівняння її з попередньо отриманим шаблоном.

За типом використовуваних характеристик біометричні системи поділяються на статичні та динамічні.

Статична біометрія (її також називають фізіологічною) базується на даних, отриманих у результаті вимірювання анатомічних характеристик людини (відбитки пальців, форма рук, малюнок райдужної оболонки ока, малюнок кровоносних судин обличчя, малюнок сітківки, риси обличчя, фрагменти генетичного коду тощо).

Динамічна біометрія (її ще називають поведінковою) базується на аналізі дій людини (параметрів голосу, динаміки та форми підпису).

У комбінованих системах ідентифікації одночасно використовується кілька ідентифікаційних ознак. Така інтеграція дає змогу будувати перед зловмисником додаткові перешкоди, які він не зможе подолати, а якщо й зможе, то зі значними труднощами [2].

1.1 Аналіз сучасних апаратно-програмних засобів ідентифікації працівників підприємства

В системах контролю та управління доступом (СКУД) використовується спеціальне обладнання, яке забезпечує визначення прав доступу людей і транспортних засобів на територію, що охороняється. Вони також забезпечують функції контролю за пересуванням людей і транспортних засобів по території організації. Інформація про проходження об'єкта через точки контролю доступу записується в базу даних і може бути проаналізована в подальшому.

Системи контролю доступу використовуються в офісних будівлях, бізнес-центрах, оптових компаніях, супермаркетах тощо.

У найпростішому випадку для ідентифікації особи можуть використовуватися два зчитувачі - для входу і виходу. Коли відвідувач показує картку, на моніторі супроводжуючого з'являється фотографія та коротка інформація про власника картки. Встановлення осіб та визначення переваги виконує черговий. У більш складних системах використовуються колони, що обертаються. Прохід через турнікети в обох напрямках можливий за пред'явленням картки. Над поворотними дверима можна розмістити камери відеоспостереження [3].

Для ідентифікації можна використовувати біометричні технології, в тому числі пристрої для визначення форми руки, відбитка пальця, райдужної оболонки ока та інші.

1.1.1 Біометричні засоби ідентифікації

Біометричні засоби захисту користуються заслуженою увагою фахівців завдяки високим експлуатаційним і технічним характеристикам. Ці інструменти використовуються не тільки в державних установах, які вимагають найвищого рівня захисту, а й у комерційному секторі та в повсякденному житті. Широке застосування біометричних систем є перспективою найближчого майбутнього в Україні завдяки розвитку бізнесу та прагненню країни до євроінтеграції.

Якщо досі основним стримуючим фактором була висока вартість біометричних засобів захисту, яка обмежувала їх масове використання, то нинішнє зниження цієї характеристики дозволяє прогнозувати поширення цієї технології в багатьох сферах, у тому числі й у сфері інформаційної безпеки [4].

В даний час біометрія як наука про ідентифікацію особистості має кілька практично самостійних наукових напрямів, кожен з яких має свій технічний розвиток. Тому розглянемо докладніше основні досягнення біометрії, які знайшли практичне застосування, розберемо їх недоліки, переваги та перспективи розвитку.

Сканування відбитків пальців є найдавнішою з усіх існуючих методик, але в той же час вона вважається однією з найперспективніших. Кожна людина має унікальні, незмінні відбитки пальців, що доведено судово-медичною експертизою та підтверджено професійною практикою.

У системі біометричної ідентифікації використовуються два основних способи ідентифікації людини за відбитками пальців: перший — за мініатюрними точками; другий заснований на методі кореляцій. Вони знаходяться в постійному процесі вдосконалення і мають свої переваги та недоліки. Ці методи базуються на фізіологічних властивостях структури папілярного візерунка та апаратних пристроях з відповідним програмним забезпеченням.

Дактилоскопічна ідентифікація особи, яка бажає отримати доступ до об’єкта охорони, здійснюється за допомогою телевізійної камери, яка сканує папілярний зразок одного з пальців особи та порівнює його з еталонним зображенням методом кореляції. За результатами незалежного тестування первинні похибки для систем цього класу складають від 10 до 20%, якщо врахувати несприятливі ділянки сухої шкіри і включити в групу тестування людей з недостатньо вираженим папілярним малюнком.

Результати зберігаються в базі даних для аутентифікації. Під час аутентифікації сканований відбиток пальця порівнюється з «паспортами», які зберігаються в базі даних. Зазвичай «паспорт» — це не зображення самого відбитка, а результат його розкладання на такі складові елементи, як «завиток», «бантик», «петля» тощо. (Рисунок 1.2) [5].

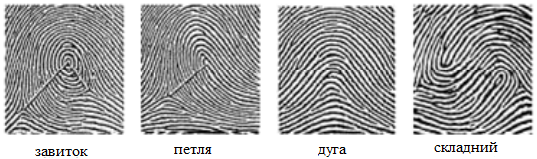


Рисунок 1.2 - Основні елементи відбитка пальця

Біометричні системи ідентифікації за відбитками пальців зазвичай мають дуже низький рівень відмови в доступі (KV - система не розпізнає справжність відбитків пальців зареєстрованого користувача), з певною ймовірністю помилкового або фальсифікованого доступу до об'єкта (KD - можливість того, що система помилково " ідентифікує» відбиток пальця користувача, який не зареєстрований у цій системі). Постачальники таких біометричних систем зазвичай вказують значення CV близько 0,01%, значення CD 0,001%, і точкою, де ці значення стають рівними, є похибка, яка становить ≈ 0,1%. В даний час активно розробляються алгоритми, стійкі до «шуму» в зображеннях відбитків пальців, що дозволяє досягти підвищення точності і швидкості розпізнавання об'єктів в реальному часі [5].

Цей спосіб ідентифікації особи набув поширення в основному в криміналістиці та системах безпеки.

Усі основні типи технологій розпізнавання облич були розроблені з метою виконання пошуку потрібного об’єкта методом «один до багатьох», тобто ідентифікації конкретного обличчя серед тисяч облич, записаних у базі даних. Якісні характеристики таких систем залежать від технологічних можливостей відеокамер, які мають роздільну здатність не менше 320x240 пікселів на дюйм при швидкості відеопотоку не менше 3-5 кадрів в секунду і об'єднані в мережу персональних комп'ютерів. Для порівняння, задовільна якість відеоконференцій вимагає швидкості відеопотоку понад 15 кадрів на секунду. Більш висока швидкість відеопотоку з кращою здатністю розпізнавання системи призводить до кращої якості отриманої ідентифікації. Відеокамери з відповідними технічними характеристиками для реалізації цієї програми коштують близько 70 доларів.

У сучасних біометричних системах сканування обличчя займає близько 20-30 секунд, в результаті чого формується кілька зображень. Для ідентифікації високоякісного зображення обличчя зазвичай потрібно близько 150-300 Кб інформації, а шаблони зображень займають близько 1300 байт інформації. Процес відеосканування обличчя заснований на створенні оригінального шаблону «вживу» в режимі реального часу та його порівнянні зі зразком файлу шаблону. Ступінь достовірності об'єктів зображення, які вимагають перевірки, являє собою певний рівень ймовірності, який може не бути однаковим для різних типів завдань або може залежати від персоналу, комп'ютерів, часу та інших факторів. При розпізнаванні обличчя на великій відстані існує значна залежність між якістю та результатом ідентифікації [5].

Існує три основні методи розпізнавання обличчя. Вони включають аналіз зображень з метою визначення відмінних рис обличчя: а) аналіз «виразних рис обличчя» - найбільш поширених і адаптованих до зміни міміки; б) аналіз на основі «нейронних мереж» — побудований на порівнянні «особливих точок», здатних ідентифікувати осіб, які перебувають у складних умовах; v) метод «автоматичної обробки зображення обличчя» - визначення співвідношення відстані та відстані між встановленими особливими рисами обличчя людини. Останній спосіб не такий ефективний, як інші, але його можна використовувати для ідентифікації зображення в слабо освітлених приміщеннях.

Основними проблемними моментами, які суттєво впливають на ефективність цих біометричних систем, є зміна освітленості, різні варіації положення обличчя під час руху, складність виділення інформативної та значної частини обличчя, в тому числі портретного, несприятливий фон, що ускладнює ідентифікацію обличчя. Частково ці проблеми можна вирішити шляхом автоматичного вибору спеціальних точок на обличчі та вимірювання відстані між ними. Таким чином, на обличчі виділяються контури очей, брів, носа, підборіддя, вух. Відстані між характерними точками цих контурів утворюють унікальний і компактний еталон певної особи, який легко піддається великомасштабному вимірюванню. Слід зазначити, що системи цього класу не розпізнають однояйцевих близнюків [5].

Проблеми ідентифікації людини по обличчю значно спрощуються, якщо біометричну систему спостереження перевести в дальній інфрачервоний діапазон світла. Цей метод дозволяє провести (сканувати) термографію ідентифікованого обличчя, виявивши при цьому особливу мережу кровоносних судин на обличчі, що кровопостачає шкіру. Проблеми достатнього освітлення для цього класу біометричних пристроїв не існує, оскільки вони сприймають і фіксують лише зміни температури обличчя і можуть працювати в повній темряві. При цьому на результати ідентифікації не впливають такі фактори, як перегрів або переохолодження обличчя, природне старіння шкіри обличчя, пластичні операції тощо, оскільки вони не змінюють внутрішнього розташування кровоносних судин людини. За допомогою цього методу термографії обличчя також можна розпізнати однояйцевих близнюків, оскільки кровоносні судини їх обличчя мають досить значні відмінності. Ця біометрична система ефективніша за попередню. Метод ідентифікації обличчя за геометрією руки схожий за своєю технологічною структурою та ступенем достовірності до методу ідентифікації обличчя за відбитками пальців, але поки використовується рідко. Математична модель ідентифікації людини таким чином потребує надзвичайно малої кількості інформації – лише 9 байт. Це дозволяє зберігати великий обсяг необхідної інформації про осіб, які потребують ідентифікації та швидкого пошуку. Найдосконалішим пристроєм є «Хандкі» (рис. 1.3), який за допомогою вбудованої відеокамери сканує не лише внутрішню, а й зовнішню сторону долоні. Подібні системи, але все ще рідко використовується. Математична модель ідентифікації людини таким чином потребує надзвичайно малої кількості інформації – лише 9 байт. Це дозволяє зберігати великий обсяг необхідної інформації про осіб, які потребують ідентифікації та швидкого пошуку. Найдосконалішим пристроєм є «Хандкі» (рис. 1.3), який за допомогою вбудованої відеокамери сканує не лише внутрішню, а й зовнішню сторону долоні. Подібні системи, але все ще рідко використовується. Математична модель ідентифікації людини таким чином потребує надзвичайно малої кількості інформації – лише 9 байт. Це дозволяє зберігати великий обсяг необхідної інформації про осіб, які потребують ідентифікації та швидкого пошуку. Найдосконалішим пристроєм є «Хандкі» (рис. 1.3), який за допомогою вбудованої відеокамери сканує не лише внутрішню, а й зовнішню сторону долоні. Подібні системи,



Рисунок 1.3 - Пристрій «Handkey».

Існують більш складні системи, які додатково вимірюють профіль кисті - об'єм пальців, об'єм кисті, нерівності долоні, розміщення шкірних складок на суглобах і т.д. Дані про тривимірну геометрію руки отримують за допомогою однієї телевізійної камери та інфрачервоного підсвічування руки під різними кутами. Послідовне ввімкнення кількох світлодіодів підсвічування створює тіньові версії проекцій тривимірної геометрії руки, що несе інформацію про її об’єм і відповідні індивідуальні властивості. Ці прилади досить громіздкі, оскільки вимагають переміщення джерела світла на відстань 10-15 см і відносно дорогі – коштують від 600 до 3000 доларів. Помилки ідентифікації першого та другого роду для біометричних пристроїв цього класу становлять менше 0,2%. Чисті умови для них не є обов'язковими,

Система розпізнавання райдужної оболонки використовує інфрачервоне світло низької інтенсивності, спрямоване через зіницю до кровоносних судин у задній частині ока. Сканери сітківки мають найнижчий відсоток забороненого доступу до об’єктів. Однак зображення райдужної оболонки має бути чітким.

Ця система також має певні недоліки, зумовлені фізіологічними змінами в організмі людини. З роками можливі суттєві зміни в розташуванні плям на райдужній оболонці людини, наприклад, райдужна оболонка ока дитини може з роками змінитися настільки, що біометрична система просто не зможе її розпізнати. Крім того, негативна помилка ідентифікації може виникнути при незначних травмах очей або навіть в результаті безсоння або сильного напруження очей. Зміни такого типу незначні, але система ідентифікації в таких випадках може «відкинути» райдужку. Що стосується біометричних систем сканування сітківки, то ідентифікація здійснюється за допомогою інфрачервоного світла низької інтенсивності, спрямованого через зіницю на кровоносні судини на задній стінці ока. Сканери сітківки зареєстрованих користувачів мають найнижчий відсоток відмови в доступі до об’єктів і практично не викликають помилок доступу. Однак зображення райдужної оболонки має бути чітким. З цієї причини катаракта ока може негативно вплинути на якість ідентифікації особистості.

Прилади цього класу є найдорожчими (близько 4000 доларів) і найменш популярними, оскільки користувачі впевнені, що використання приладів для інфрачервоного підсвічування зіниць шкодить їхньому здоров'ю [5].

Розпізнавання голосу – це біометрична технологія, яка дозволяє ідентифікувати людину за унікальними характеристиками її голосу. Основними перевагами цієї технології є можливість дистанційної перевірки права користувача на доступ до інформації. Цей метод активно використовується в роботі банків та інших подібних організацій. Процес реєстрації починається з того, що людина називає пароль з будь-яких трьох слів, наприклад, «мій голосовий пароль». Таким чином створюються акустичні характеристики голосу користувача, які реєструються в базі даних, а потім при перевірці досить сказати фразу пароля, щоб система ідентифікувала голос користувача з уже записаними параметрами його голосу. . в базі даних. Процес перевірки не займає багато часу і відбувається майже зі швидкістю проголошення пароля. Недоліком є ​​невелика "гнучкість"

1.1.2 Електронні засоби ідентифікації

Ідентифікаційні пристрої включають зчитувальні пристрої та ідентифікатори, які розшифровують та зчитують інформацію з ідентифікаторів різного типу, що визначає права людей, транспорту чи майна на території охоронної зони [1].

Контрольовані місця, де безпосередньо здійснюється контроль доступу, наприклад двері, турнікети, прохідні кабіни, обладнані зчитувачем, виконавчим пристроєм та іншими необхідними засобами.

Ідентифікатор - це об'єкт, який містить кодову інформацію, що підтверджує повноваження його власника. Такі інструменти мають форму підвісок, ключів, карток.

Зчитувач — це електронний пристрій, який зчитує кодову інформацію з ідентифікатора та перетворює її в стандартний формат для передачі на контролер для аналізу та прийняття рішень.

Ідентифікатор iButton відноситься до класу електронних контактних ідентифікаторів. Модельний ряд ідентифікаторів iButton досить широкий і різноманітний (більше 20 моделей). Як правило, ідентифікатор iButton являє собою мікросхему (чіп), вмонтовану в герметичний сталевий корпус. Мікросхема (чіп) живиться від мініатюрної літієвої батарейки. Корпус виглядає як стандартний акумулятор (рис. 1.4) і має діаметр 17,35 мм при висоті 5,89 мм (корпус F5) або 3,1 мм (корпус F3) [2].



Рисунок 1.4 - Ідентифікатори iButton

Корпус забезпечує високий ступінь захисту ідентифікатора від агресивних середовищ, пилу, вологи, зовнішніх електромагнітних полів, механічних ударів тощо. Ідентифікатор легко кріпиться на носій (картку, брелок).

В основі мікросхеми - мультиплексор і пам'ять. Пам'ять ідентифікатора iButton складається з наступних компонентів:

- постійний запам'ятовуючий пристрій (ПЗП);

- енергонезалежна оперативна пам'ять NV;

- супероперативна SM (пам'ять блокнота) або пам'ять ноутбука.

PZP зберігає 64-бітний код, що складається з 48-бітного унікального серійного номера (функція ідентифікації), восьмибітного коду типу ідентифікатора та восьмибітової контрольної суми.

NV RAM може використовуватися для зберігання публічної та конфіденційної інформації (криптографічних ключів, паролів доступу та інших даних).

Пам'ять SM є буфером і виконує функції пам'яті ноутбука [2].

Щоб записувати та читати дані з ідентифікатора, корпус iButton має контактувати з пристроєм для зчитування. Час контакту - не більше 5 мс, гарантована кількість контактів - кілька мільйонів.

Переваги ідентифікаторів на основі електронних ключів iButton:

- надійність, довговічність (термін збереження інформації в пам'яті ідентифікатора не менше 10 років);

- високий ступінь механічного та електромагнітного захисту;

- малий розмір;

- відносно низька ціна.

Недоліком цього пристрою є залежність його роботи від точності дотику ідентифікатора і зчитувача, що виконується вручну.

Основні характеристики пам'яті iButton наведені в таблиці 1.1 [2].

Таблиця 1.1 - Основні характеристики пам'яті ідентифікатора iButton

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Тип продукту | Ємність оперативної пам'яті NV | Ємність СМ, біт | Ємність ПЗП, байт | Примітка |
| DS1963S | 4 Кбіт (16 сторінок 256 біт) | 256 | 64 | 8 сторінок NV RAM захищені паролем. Реалізація SHA-1 |
| DS1991 | 1152 Кбіт (4 сторінки по 256 біт) | 256 | 64 | 3 блоки RAM NV захищені паролем |
| DS1992L | 1 кбіт (4 сторінки по 256 біт) | 256 | 64 | Незахищена NV RAM |
| DS1993L | 4 Кбіт (16 сторінок 256 біт) | 256 | 64 | Незахищена NV RAM |
| DS1994L | 4 Кбіт (16 сторінок 256 біт) | 256 | 64 | Незахищена NV RAM. Годинник реального часу |
| DS1995L | 16 Кбіт (64 сторінки 256 біт) | 256 | 64 | Незахищена NV RAM |
| DS1996L | 64 Кбіт (256 сторінок 256 біт) | 256 | 64 | Незахищена NV RAM |

Контактні смарт-карти належать до класу електронних ідентифікаторів контактів. Контактні смарт-карти прийнято поділяти на процесорні карти та карти пам'яті. Зазвичай вони випускаються у вигляді пластикових карт [2].

Основою внутрішньої структури сучасної процесорної смарт-карти є мікросхема, до складу якої входять центральний процесор, оперативна пам'ять, ПЗП і EEPROM (electronic erasable programmable permanent memory device - EEPROM). Як правило, в чіпі також присутній спеціалізований співпроцесор.

Оперативна пам'ять використовується для тимчасового зберігання даних, наприклад, результатів обчислень, які виконує процесор. Об'єм пам'яті становить кілька кілобайт.

Спеціалізованому процесору доручається виконання різноманітних процедур, необхідних для підвищення безпеки SIA, зокрема:

- генерація криптографічних ключів;

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

- здійснення операцій з електронним цифровим підписом (генерація та перевірка);

- здійснення операцій з ПІН-кодом тощо.

Виконуваний код процесора зберігається в PZP, RAM використовується як робоча пам'ять, ESPZP необхідний для зберігання змінних даних про власника картки.

Безконтактні радіочастотні ідентифікатори або системи RFID (радіочастотна ідентифікація) належать до класу електронних безконтактних радіочастотних пристроїв. Радіочастотні ідентифікатори типу Prokimiti випускаються у вигляді карток, кулонів, браслетів, ключів тощо. Кожен з них має свій унікальний порядковий номер [2].

Їх основними компонентами є інтегральна мікросхема, яка зв'язується зі зчитувачем, і вбудована антена. Мікросхема містить мікросхему пам'яті (або мікросхему жорсткої логіки) з допоміжними вузлами: модулем програмування, модулятором, блоком управління та іншими модулями. Обсяг пам'яті від 8 до 256 байт. У радіочастотному ідентифікаторі в основному використовується СППЗП, але зустрічається і ЕСППЗП. Пам'ять містить унікальний ідентифікаційний номер, код пристрою та службову інформацію (біти парності, початковий і кінцевий біти коду передачі тощо).

У таблиці 1.2 наведено основні характеристики безконтактних ідентифікаторів [2].

Таблиця 1.2 - Безконтактні ідентифікатори

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | Ідентифікатори близькості | Смарт-карта | |
| Стандарт ISO/IEC 14443 | Стандарт ISO/IEC 15693 |
| Частота радіоканалу | 125 кГц, 13,56 МГц | 13,56 МГц | 13,56 МГц |
| Відстань читання | До 1м | До 10 м | До 1м |
| Види вбудованих мікросхем | Мікросхема пам'яті, мікросхема жорсткої логіки | Мікросхема пам'яті, мікросхема жорсткої логіки, процесор | Мікросхема пам'яті, мікросхема жорсткої логіки |
| Функція пам'яті | Лише читання | Читати писати | Читати писати |
| Ємність пам'яті | 8-256 байт | 64 байти - 64 Кб | 256 байт - 2 Кб |
| Алгоритми шифрування та аутентифікації | За варіантами | Технології MIFARE, DES, 3DES, AES, RSA, ECC | DES, 3DES |
| Механізм проти зіткнення |  | Є | Є |

Основними перевагами радіочастотних ідентифікаторів (систем RFID) є:

- технологія безконтактного читання;

- довговічність пасивних ідентифікаторів (деякі компанії-виробники дають довічну гарантію на картки);

- точність, надійність і зручність зчитування розпізнавальних знаків.

До недоліків систем RFID можна віднести слабкий електромагнітний захист і відносно високу вартість, враховуючи вартість зчитувача.

Ідентифікатори на основі USB-ключів належать до класу електронних контактних пристроїв. Ідентифікатори цього типу не потребують дорогих апаратних зчитувачів. Ідентифікатор під назвою USB-ключ підключається до USB-порту безпосередньо або за допомогою з’єднувального кабелю.

Ключі USB можуть включати:

- процесор - управління та обробка даних;

- криптографічний процесор - реалізація алгоритмів ГОСТ 28147 - 89, DES, 3-DES, RSA, DSA​​, MD5, SHA-1 та інших криптографічних перетворень;

- USB контролер - забезпечує інтерфейс з USB портом комп'ютера;

- RAM - зберігання змінних даних;

- ЕСППЗП - зберігання ключів шифрування, паролів, сертифікатів та інших важливих даних;

- PZP - зберігання команд і констант.

У таблиці 1.3 представлені деякі характеристики USB-ключів [2].

Таблиця 1.3 - Характеристики USB-ключів

|  |  |  |  |
| --- | --- | --- | --- |
| Продукт | Ємність пам'яті | Цифра серійного номера | Алгоритм шифрування |
| ІКЕА 20кк | 8/32 | 64 | DES, 3DES, RC2, RC4, MDS, RSA-1024/2048 |
| eToken R2 | 16/32/64 | 32 | ДЕСКИ (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 |

Перевагами ідентифікаторів на основі USB-ключів є відсутність апаратного зчитувача, малий розмір і зручність зберігання ідентифікатора, а також простота підключення ідентифікатора до USB-порту. До недоліків можна віднести відносно високу вартість і слабкий механічний захист брелока [2].

1.1.3 Комбіновані засоби ідентифікації

Останнім часом підвищену увагу та інтерес викликають середовища двофакторної аутентифікації, які ефективно вирішують завдання забезпечення безпечного доступу до інформаційних ресурсів своїх компаній. Такі засоби автентифікації можна отримати за допомогою комбінованих SIA [2].

Впровадження комбінованих СІА в корпоративну систему захисту інформації дозволяє збільшити кількість використовуваних ідентифікаційних ознак (факторів).

В даний час використовуються наступні типи комбінованих систем ідентифікації та автентифікації:

- системи на основі радіочастотних ідентифікаторів та USB-ключів;

- системи на основі гібридних смарт-карт;

- біоелектронні системи.

Крім того, деякі види таких систем здатні управляти і контролювати фізичний доступ до будівлі і приміщень.

Апаратна інтеграція USB-ключів і радіочастотних ідентифікаторів передбачає, що антена і мікросхема, що підтримує безконтактний інтерфейс, вбудовані в корпус брелока. Це дозволяє керувати доступом як до комп'ютера, так і до офісного приміщення за допомогою єдиного ідентифікатора. Для входу в офіс працівник використовує свій ID як безконтактну картку, а при доступі до захищених комп’ютерних даних – як USB-ключ. Крім того, при виході з кімнати він витягує ідентифікатор з USB-роз’єму (для повторного введення пізніше) і таким чином автоматично блокує комп’ютер.

Для прикладу візьмемо ідентифікатор RFiKey, який є ключем USB - iKey із вбудованим чіпом Prokimity. Продукт RFiKey підтримує інтерфейс USB 1.1/2.0 і працює зі зчитувачами HID Corporation [2].

До основних можливостей RFiKey відносяться наступні індикатори:

- робоча частота радіочастотного ідентифікатора Прокіміти – 125 кГц;

- тактова частота процесора - 12 МГц;

- реалізовані криптографічні алгоритми - MD5, RSA, DES, 3 - DES, RC2, RC4, RC5;

- наявність апаратного датчика випадкових чисел;

- підтримувані стандарти - PKCS # 11, MS Cripto API, PC/SC;

- файлова система з трьома рівнями доступу до даних;

- підтримувані операційні системи - Windows 95/98/ME/NT4 (SP3) / 2000/XP.

Гібридні смарт-карти містять різні чіпи, які не з’єднані між собою. Один чіп підтримує контактний інтерфейс, інший (Proximity, ISO14443 / 15693) - безконтактний. Як і у випадку з інтеграцією USB-ключів і радіочастотних ідентифікаторів, SIA на основі гібридних смарт-карт вирішують подвійне завдання: захист від несанкціонованого доступу до комп’ютерів і приміщень компанії, де вони зберігаються. Крім того, на смарт-картці розміщується фото працівника, що дозволяє його візуально ідентифікувати.

Аналіз витрат при переході на використання гібридних смарт-карт, як і у випадку поєднання радіочастотних ідентифікаторів і USB-ключів, ще раз підтверджує торжество принципу «два в одному». Якщо на посвідчення нанести фото працівника, цей принцип трансформується в «три в одному».

Інтеграція з електронними системами на основі безконтактних смарт-карт в основному використовується в системах контролю фізичного доступу.

Прикладом такої інтеграції є продукти Precise 100 MC компанії Precise Biometrijs AB. Щоб отримати доступ до інформаційних ресурсів комп'ютера за допомогою таких засобів, користувачеві необхідно вставити смарт-карту в зчитувач і прикласти палець до сканера. Шаблони відбитків пальців зберігаються в зашифрованому вигляді в захищеній пам'яті смарт-карти. Якщо зображення відбитка пальця відповідає шаблону, доступ до комп’ютера дозволено.

Продукт Precise 100 MC — це пристрій USB, який працює в середовищі Windows. Зчитувач смарт-карт підтримує всі типи мікропроцесорних карт, які відповідають стандарту ISO 7816-3 (протоколи T=0, T=1). Сканер відбитків пальців – це сканер ємнісного типу зі швидкістю сканування 4 відбитки пальців за секунду [2].

1.2 Вибір методів ідентифікації в компанії

1.2.1 Біометрична ідентифікація обличчя

Системи розпізнавання облич — це вбудовані комп’ютерні програми, які аналізують зображення облич людей для їх ідентифікації. Програма робить знімок обличчя та вимірює його характеристики, такі як відстань між очима, довжина носа, кут щелепи, на основі чого створюється унікальний файл під назвою «шаблон». Використовуючи шаблони, програма порівнює дане зображення з іншими зображеннями, а потім оцінює, наскільки зображення схожі одне на одне. Звичайними джерелами зображень, які використовуються для розпізнавання обличчя, є сигнали з телекамер і раніше отримані фотографії, наприклад ті, що зберігаються в базі даних водійських прав. Але згідно з дослідженнями, зернисті зображення або старі фотографії, такі як ті, що зберігаються в особистих файлах, не будуть корисними.

На практиці, коли системи розпізнавання обличчя використовуються як частина стандартних електронних систем безпеки, передбачається, що особа, яку потрібно ідентифікувати, дивиться прямо в камеру. Тому система працює з відносно простим двовимірним зображенням, що значно спрощує алгоритми та знижує інтенсивність обчислень. Але навіть у цьому випадку завдання розпізнавання все одно нетривіальна, оскільки алгоритми повинні враховувати можливість зміни рівня освітленості, виразу обличчя, наявність або відсутність макіяжу чи окулярів.

Обсяг баз даних при використанні стандартних персональних комп'ютерів не перевищує 10000 зображень.

На даний момент існує чотири основні методи розпізнавання обличчя [6]:  
1) «Фізичні особи»;

2) аналіз «відмітних характеристик»;

3) аналіз на основі «нейронних мереж»;

4) метод «автоматичної обробки зображення обличчя».

Всі ці способи відрізняються складністю реалізації та метою застосування.

«Eigenface» можна перекласти як «власне обличчя». Ця технологія використовує двовимірні зображення в градаціях сірого, які представляють характерні риси зображення обличчя. Метод «власного обличчя» часто використовується як основа для інших методів розпізнавання обличчя.

Під час реєстрації «конкретне обличчя» кожної конкретної людини представляється у вигляді певної кількості коефіцієнтів. Для режиму автентифікації, в якому зображення використовується для перевірки особистості, «живий» шаблон порівнюється з уже зареєстрованим шаблоном для визначення коефіцієнта різниці. Ступінь відмінності між візерунками визначає факт ідентифікації. Технологія «eigenface» оптимальна при використанні в добре освітлених приміщеннях, коли є можливість сканувати обличчя попереду.

Метод аналізу «відмітних ознак» є найбільш поширеною технологією ідентифікації. Ця технологія схожа на техніку «Eigenface», але більш адаптована до зміни зовнішнього вигляду або виразу обличчя людини (усміхнене чи похмуре обличчя). Технологія «виразні риси» використовує десятки характерних ознак різних ділянок обличчя з урахуванням їх взаємного розташування. Індивідуальне поєднання цих параметрів визначає особливості кожної особистості. Обличчя людини унікальне, але досить динамічне, адже людина може посміхатися, відрощувати бороду та вуса, носити окуляри – все це підвищує складність процесу ідентифікації. Так, наприклад, коли ви посміхаєтеся, відбувається певний рух частин обличчя, розташованих біля рота, що в свою чергу викличе такий же рух прилеглих частин. Враховуючи такі зміни, можна однозначно ідентифікувати людину навіть за різними змінами обличчя. Враховуючи те, що цей аналіз розглядає локальні поверхні обличчя, допустимі відхилення можуть становити до 25° в горизонтальній площині та приблизно до 15° у вертикальній площині та вимагають досить потужного та дорогого обладнання, яке відповідно зменшує ступінь розширення. цього методу [6].

«Нейронні мережі» використовують алгоритм, який зіставляє унікальні параметри людини з параметрами шаблону, знайденого в базі даних, використовуючи максимально можливу кількість параметрів. Під час порівняння виявляються невідповідності між тестованим і шаблоном з бази даних, потім запускається механізм, який за допомогою відповідних вагових коефіцієнтів визначає ступінь відповідності тестованого шаблону з бази даних. Цей метод підвищує якість ідентифікації обличчя в складних умовах.

Метод «автоматичної обробки зображення обличчя» — це найпростіша технологія, яка використовує відстані та співвідношення між легко визначеними точками обличчя, такими як очі, кінчик носа та куточки губ. Хоча цей метод не такий потужний, як «власні грані» або «нейронна мережа», його можна досить ефективно використовувати в умовах слабкого освітлення.

Надійність системи розпізнавання обличчя значною мірою залежить від кількох факторів:

1) якість зображення. Імовірність безпомилкової роботи системи значно знижується, якщо особа, яку ми намагаємося ідентифікувати, не дивиться прямо в камеру або фотографується при поганому освітленні;

2)актуальність фотографії, внесеної в базу даних;

3) розмір бази даних.

Технології розпізнавання облич добре працюють зі стандартними відеокамерами, які передають дані та керуються персональним комп’ютером і вимагають роздільної здатності 320x240 пікселів на дюйм із швидкістю відеопотоку не менше 3–5 кадрів на секунду. Для порівняння, прийнятна якість для відеоконференцій вимагає швидкості відеопотоку 15 кадрів на секунду. Вища швидкість відеопотоку при більшому розширенні призводить до покращення якості ідентифікації. При розпізнаванні людей на великій відстані існує сильна залежність між якістю відеокамери та результатами ідентифікації [6].

1.2.2 Ідентифікація за карткою Prokimiti

Системи контролю доступу на основі пластикових безконтактних безконтактних карток (рисунок 1.5) широко використовуються в різних компаніях і установах. Картки призначені для доступу до будь-яких типів приміщень, що охороняються, тобто по суті є електронними ключами. Карти належать до класу пасивних, оскільки не мають власного внутрішнього джерела живлення, що забезпечує їм практично необмежений термін служби [7].



Малюнок 1.5 - Картка Prokimiti

Кожна картка доступу має свій індивідуальний код доступу та серійний номер. Він складається з двох пластикових частин, між якими розташована антена і мініатюрний чіп. Панелі герметично склеєні в заводських умовах. Чіп складається з передавача, приймача і процесора, в пам'яті якого знаходиться ідентифікаційний код карти (записаний на заводі при виробництві). Процес зчитування та розпізнавання коду картки заснований на технології безконтактної радіочастотної ідентифікації. Зчитувач постійно випромінює радіосигнал на частоті 125 кГц, коли він потрапляє в його діапазон, карта генерує і починає випромінювати відповідний сигнал через вбудовану антену. Антена пристрою для зчитування карток приймає сигнал, потім демодулює його та витягує з нього код доступу, який потім надсилається до контролера системи доступу. Після ідентифікації система або підтверджує, або видає сигнал про помилку.

За співвідношенням ціна-якість картки прокіміт економічно вигідніше традиційних металевих ключів, особливо якщо на підприємстві висока плинність кадрів. Крім того, безконтактні картки дозволяють отримати доступ до приміщень набагато швидше, ніж традиційні ключі. Якщо картка містить ідентифікаційні дані працівника (фото, ім'я, прізвище та посада), вона може бути використана як перепустка у разі відсутності зчитувального пристрою або його несправності.

При виборі моделі зчитувального пристрою необхідно звертати увагу не тільки на ціну (цей фактор досить важливий), але і на відстань, на якій карта працює і може передати ідентифікаційний код. Також важливий тип інтерфейсу, через який зчитувач передає код карти на контролер системи доступу. Не менш важливим є вміння працювати з вуличними та внутрішніми зчитувачами, а також зчитувачами для доступу до комп’ютерної мережі [7].

Картки Prokimit бувають різних форматів, але найбільш поширеними є [8]:

– Em-Marine – чи не найпоширеніший стандарт безконтактних проксімі-карт. Карти формату Em - marine заслужили своє широке поширення завдяки своїй невисокій вартості;

- HID - формат, розроблений американською компанією HID Corp. Вона більш захищена, але на ринку є не тільки оригінальні, а й аналогові безконтактні прокіміти (prokimiti) картки такого формату. Набагато дорожче карт Em – Marine;

- Mifare - ці безконтактні проксіміті (proximity) карти набули широкого поширення в галузях, пов'язаних з оплатою послуг (міський, міський наземний транспорт, курорти, спортивні центри і т.д.). Картки дозволяють не тільки отримувати доступ, але й зберігати записану на них інформацію.

Для прикладу візьмемо прокім-карту формату Em-Marine і опишемо її технологію.

Безконтактна карта доступу Em Marine складається з мікросхеми з фіксованим (EM Marine) або перепрограмованим кодом (HID, Indala), котушки індуктивності та конденсатора, який є резонансним коливальним контуром. Стандарт Em Marine, найпростіший і доступний, розроблений швейцарською компанією EM Microelectronic - Marin SA. Пластикові картки EM Marine завоювали популярність завдяки необмеженому терміну служби, відсутності помилок при передачі ідентифікаційного коду та невибагливості до умов експлуатації.

Пластикові картки EM-Marine на основі технології радіочастотної ідентифікації. Радіочастотна карта EM-Marine передає дані від ідентифікатора на зчитувач в радіочастотному діапазоні. Пластикові картки EM-Marine для доступу в приміщення поєднують в собі переваги безконтактних proximity і смарт-карт. Запис і зчитування інформації з мікросхеми здійснюється безконтактним способом. Карта Prokimiti EM-Marine є пасивним пристроєм, тобто не має вбудованого джерела живлення. Живлення мікросхеми під час обміну інформацією здійснюється за рахунок змінного електромагнітного поля, створюваного зчитувальним пристроєм [9].

Програмована карта ST-PC020EM торгової марки Smartec (рисунок 1.6) використовує технологію proximity і призначена для ідентифікації персоналу в системах контролю доступу та вимірювання часу. Електронна перепустка у вигляді пластикової картки має 64-бітну пам'ять, розраховану на зчитування без перезапису, і може передавати ідентифікаційний код необмежену кількість разів. Така прокіміті-карта працює разом зі зчитувачами стандарту Em Marine на частоті 125 кГц, при цьому відстань зчитування коду становить до 10 см. ST-PC020EM має стандартні розміри 85х54 мм, але характеризується тонким корпусом - 0,8 мм [ 10].



Рисунок 1.6 – Програмована карта ST-PC020EM

ID card ST-PC020EM відноситься до пасивного класу стандарту Em Marine, тому що не має вбудованого джерела живлення. Передача коду здійснюється за технологією prokimiti, коли зчитувач карт доступу постійно випромінює сигнал на частоті 125 кГц, а карта, яка знаходиться в його зоні дії, отримує енергію і генерує радіосигнал з кодом. Ця технологія реалізована на основі вбудованого в прокіміті-карту мініатюрного чіпа, який включає передавач, приймач, процесор і антену. Запрограмований в заводських умовах унікальний ідентифікаційний код зберігається в пам'яті процесора.

У порівнянні з RFID-ідентифікаторами Prokimity, Mifare або iClass стандартні картки Em Marine мають найнижчу ціну при однаковій функціональності. Представлена ​​прокімітна карта має достатню механічну міцність, стійка до вигинів, ударів, не боїться вологи та бруду, виготовлена ​​з високоміцного ПВХ пластику та має необмежений термін служби. Тому ST-PC020EM можна використовувати в різних кліматичних умовах в діапазоні робочих температур від -25°С до +85°С при відносній вологості повітря 90% [10].

Як і всі пластикові ідентифікаційні картки, ST-PC020EM виготовляється шляхом термічного пресування двох пластикових пластин, між якими попередньо вставляються смарт-чіп Em-Marine і антена. При цьому карта prokimiti дозволяє наносити на обидві поверхні будь-яке зображення: написи, фотографії, логотипи та ін. метод прямого друку: це може бути сублімація, офсетний друк або трафаретний друк.

Картковий процесор Smartec виготовлений за технологією CMOS (CMOS - complementary metal-oxide-conductor structure), має ємність пам'яті 64 біт і захищений від статичної електрики та електромагнітних полів. При передачі радіосигналу на безконтактний зчитувач карта серії ST-PC020EM використовує 3 типи модуляції: Манчестерський код, Двофазний код і PSK-код, які відрізняються кількістю імпульсів на один біт. Основні характеристики ST-PC020EM представлені в таблиці 1.4 [10].

Таблиця 1.4 - Технічні характеристики прокімітних карт ST-PC020EM

|  |  |
| --- | --- |
| Параметри | Значення |
| Робоча частота | 100-150 кГц |
| Чіп | N-4100 |
| Тип пам'яті | Лише для читання |
| Обсяг пам'яті | 64 біти |
| Відстань читання | 0,1 м |
| Максимальна кількість відтворень | Це не обмежено |
| Розмір картки | 85,4 x 54,0 x 0,8 мм |
| матеріал | Полівініл хлорид |
| Вологість | 90% |
| Діапазон робочих температур | -25°C ... +85°C |
| Температура зберігання | -40°C...+70°C |

1.3 Розбір технічного завдання та формулювання завдання

У даній роботі розроблено апаратно-програмну систему ідентифікації співробітників компанії на основі фазової логіки. Пропонується для полегшення доступу співробітників до компанії. Ідентифікація, як і контроль доступу, забезпечує технологію безпеки, яка дозволяє або забороняє доступ до певних об'єктів.

Розроблена система ідентифікації забезпечить легкий та зручний доступ на об’єкт, а також захистить від несанкціонованого проникнення.

Ця програмно-апаратна система буде розроблена на основі нечіткої логіки, оскільки в наш час нечітка логіка привертає все більше уваги фахівців, які розробляють різні системи. На відміну від булевої алгебри, в якій існує тільки два значення (0 і 1, істина або хибність), у фазовій логіці також є перехідні значення (стани).

В останні роки значення нечіткої логіки стрімко зростає у світі високих технологій, тому розробка системи на її основі буде актуальною.

Розроблений апаратно-програмний комплекс засобів ідентифікації співробітників буде реалізований за допомогою програмного забезпечення Simulink, яке вбудовано в пакет програм Matlab.

MATLAB — це набір програм для числового аналізу та мова програмування, яка використовується в цьому наборі. Система є зручним інструментом для роботи з математичними матрицями, малювання функцій, роботи з алгоритмами, створення робочих оболонок (інтерфейсів користувача) з програмами на інших мовах програмування.

MATLAB надає користувачеві велику кількість функцій аналізу даних, які охоплюють майже всі області математики, включаючи:

- матриці та лінійна алгебра — матрична алгебра, лінійні рівняння, власні значення та вектори, сингулярності, матрична факторізація тощо;

- поліноми та інтерполяція — корені многочленів, операції над поліномами та їх диференціювання, інтерполяція та екстраполяція кривих;

- математична статистика та аналіз даних — статистичні функції, статистична регресія, цифрова фільтрація, швидке перетворення Фур'є та ін.;

- обробка даних — набір спеціальних функцій, включаючи побудову графіків, оптимізацію, пошук нулів, числове інтегрування та інші;

- диференціальні рівняння — розв’язування диференціальних та диференціально-алгебраїчних рівнянь, рівнянь із зв’язками, рівнянь у частинних похідних тощо;

- розріджені матриці — спеціальний клас даних пакету MATLAB, що використовується в спеціалізованих програмах;

- цілочисельна арифметика — виконання цілочисельних арифметичних операцій у середовищі MATLAB [11].

Simulink — це інтерактивний інструмент для моделювання, симуляції та аналізу динамічних систем, включаючи дискретні, безперервні та гібридні, нелінійні та розривні системи. Він дозволяє створювати графічні блок-схеми, моделювати динамічні системи, досліджувати продуктивність системи та покращувати проекти.

Ключовими особливостями Simulink є [12]:

- інтерактивне графічне середовище для побудови блок-схем;

- розширювана бібліотека готових блоків;

- засоби побудови багаторівневих ієрархічних багатокомпонентних моделей;

- засоби навігації та налаштування параметрів складних моделей - Model Explorer;

- засоби інтеграції в модель готових алгоритмів C/C++, FORTRAN, ADA та MATLAB, взаємодія із зовнішніми програмами моделювання;

- сучасні засоби розв'язування диференціальних рівнянь для неперервних, дискретних, лінійних і нелінійних об'єктів (включаючи гістерезис і розриви);

- імітаційне моделювання нестаціонарних систем за допомогою вирішувачів зі змінним і постійним кроком або кероване пакетне моделювання MATLAB;

- інтерактивна візуалізація вихідних сигналів, засоби налаштування та призначення вхідних впливів;

- інструмент для налагодження та аналізу моделі;

- повна інтеграція з MATLAB, включаючи численні методи, візуалізацію, аналіз даних і графічні інтерфейси.

Дерево рішень розробленої системи ідентифікації побудовано на основі нечіткої логіки (рисунок 1.7).

Перший етап включає аналіз системи. На цьому етапі вибираються властивості системи розробки та її основні властивості.

Після цього необхідно провести постановки. Тут описано саме завдання та виділено цілі системи розробки.

На третьому етапі обирається метод проектування. Для дизайну була обрана нечітка логіка.

Четвертий етап передбачає вибір системи автоматизованого проектування (САПР). В якості САПР був обраний Matlab, тобто пакет, що входить до нього - Simulink.

Останній п'ятий етап - перевірка системи розробки. На цьому етапі система перевіряється на тестах. У результаті випробувань стає очевидним, чи відповідають очікувані результати, отримані при постановці задачі, результатам випробувань, отриманим під час перевірки.



Рисунок 1.7 – Дерево рішень

2 РОЗРОБКА ТА ДОСЛІДЖЕННЯ ПРИСТРОЮ

2.1 Створення структурної схеми пристрою

Термін «нечітка логіка» почав використовуватися в кінці 60-х років 20 століття. Спочатку це означало будь-яку логіку, яка мала більше двох значень істинності.

В даний час термін «нечітка логіка» використовується в двох різних значеннях.

У більш вузькому розумінні нечітка логіка - це логічна система, яка є розширенням багатозначної логіки. Однак навіть для нечіткої логіки у вужчому розумінні перелік базових операцій сильно відрізняється як за формою, так і за змістом від списку основних операцій для багатозначних логічних систем. Нечітка логіка у вужчому розумінні — це спеціальна багатозначна логіка, яка має на меті забезпечити формальні основи градуйованого підходу до невизначеності. Поступовий підхід — це загальний принцип людського мислення, який використовується, коли намагається з’ясувати, чи має об’єкт властивість повністю чи лише частково, оскільки дана властивість незрозуміла. Наприклад, «практично біла точка», «дуже потужний двигун» і т.д. У всіх випадках ми стикаємося з прихованими ступенями інтенсивності властивостей, що розглядаються.

Нечітка логіка в широкому сенсі є розширенням нечіткої логіки у вужчому значенні та спрямована на створення математичної моделі природних людських міркувань, у якій природна мова відіграє фундаментальну роль. У цьому сенсі нечітка логіка еквівалентна теорії нечітких множин, тобто класів з неточними, розмитими межами [13].

Загалом, нечітка логіка є результатом поступового підходу до формальних логічних схем. Важливо зазначити, що це не результат нескінченних марних узагальнень. Завдяки поступовому підходу нечітка логіка забезпечує вирішення деяких класично нерозв’язних задач [14]. Наприклад, добре відомі стародавні парадокси сорит (купа) і фалакрос (лиса людина).

Парадокс купи: з одного пшеничного зерна купи не стає. Те саме стосується двох зерен, трьох і т.д. Тому натовпу не існує.

Парадокс лисого: лисий - це людина без волосся або з одним волоссям. Те саме стосується людини з двома волосками тощо. Отже, всі люди лисі.

Згадані парадокси виникають тоді, коли властивості «бути натовпом» і «бути лисим» точно розуміються, тобто виключається їх невизначеність. Класична бінарна логіка не може з ними впоратися.

Таким парадоксам не місце в нечіткій логіці. Рішення, запропоноване нечіткою логікою, полягає в тому, щоб припустити, що імплікація F(k)=>F(k+1), де F(k) означає, наприклад, твердження «k зерен не утворюють купи», вірна лише частково. , який близький до 1, скажімо, 1–ɛ, де ɛ>0. За такого припущення парадокс натовпу, як і парадокс лисого, зникає.

Фази логічної операції засновані на звичайній булевій логіці, де два твердження A і B можуть бути істинними або хибними, тобто приймати значення «1» або «0». Для цих двох висловлювань існує загалом =16 різних логічних операцій, з яких лише п’ять мають змістовну інтерпретацію: І (˄), АБО (˅), виключне АБО (\oplus), імплікація (⇒) та еквівалентність (⬄). Таблиці істинності для цих операцій наведено в таблиці 2.1 [15].

Таблиця 2.1 - Таблиці істинності булевої логіки

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| я | IN | A ˄ V | A ˅ V | я\oplusIN | А ⇒ Б | я⬄IN |
| 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 - це тип багатозначної логіки, в якій значення істинності задані лінгвістичними змінними або термінами лінгвістичної змінної «істина». Правила виконання нечітких логічних операцій отримані з булевих логічних операцій за допомогою принципу узагальнення [15].

Основними перевагами нечітких систем перед іншими є:

- можливість роботи з нечітко заданими вхідними даними, наприклад, значеннями, які постійно змінюються в часі (динамічні завдання);

- можливість нечіткої формалізації критеріїв оцінки та порівняння;

- можливість проведення оцінки якості як вхідних даних, так і вихідних результатів, оскільки система працює не тільки за реальними значеннями даних, а й за ступенем їх вірогідності та розподілом;

- можливість швидкого моделювання складних динамічних систем та їх порівняльного аналізу із заданим ступенем точності: оперуючи принципами поведінки системи, що описуються нечіткими методами, по-перше, не витрачається багато часу на знаходження точних значень змінних і складання рівнянь, що їх описують, по-друге, є можливість оцінити різні варіанти вихідних значень [16].

В даний час розвиток нечіткої логіки ще далекий від завершення, незважаючи на те, що роботи з розробки її математичних основ ведуться досить активно. Це пояснюється тим, що нечітка логіка має певну програму, яка тісно пов'язана з моделюванням деяких частин природної мови, що дозволяє будувати різні її рішення.

Підхід до формалізації поняття нечіткої множини полягає в узагальненні поняття приналежності. У звичайній теорії множин існує кілька способів специфікації множини. Одним з них є присвоювання за допомогою характеристичної функції.

Нехай U — універсальна множина, k — елемент U, а R — деяка властивість.

Регулярна (точна) підмножина A універсальної множини U, елементи якої задовольняють властивість R, визначається як множина впорядкованих пар, де характеристична функція приймає значення 1, якщо k задовольняє властивість R, і 0 в іншому випадку [14] .

Розглянемо множину Ks усіх чисел від 0 до 10. Визначимо підмножину A множини Ks усіх дійсних чисел від 5 до 8: A = [5,8].

Покажемо функцію належності множини A. Ця функція присвоює номер 1 і 0 кожному елементу в X залежно від того, належить цей елемент до підмножини A чи ні. Результат показано на рисунку 2.1.

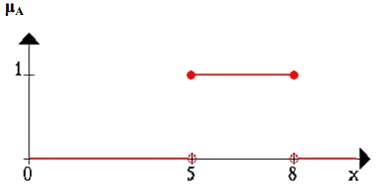


Рисунок 2.1 - Функція належності множини А

Ми можемо інтерпретувати елементи, що відповідають 1, як елементи множини A, а елементи, що відповідають 0, як елементи, що не належать до множини A.

Це поняття використовується в багатьох сферах. Але є ситуації, коли цій концепції бракує гнучкості.

Нечітка підмножина відрізняється від звичайної тим, що для елементів k з U немає однозначної відповіді «так-ні» щодо властивості R . У зв'язку з цим нечітка підмножина A універсальної множини U визначається як множина впорядкованих пар, де - характерна функція приналежності (або просто функція приналежності), яка приймає значення в деякій повністю впорядкованій множині M, зазвичай M = [0,1]. Функція належності вказує ступінь (або рівень) елемента k, який належить до підмножини A . Множину M називають множиною належності. Якщо M = {0,1}, то нечітку підмножину A можна вважати нормальною або нечіткою множиною. Таким чином, з точки зору характеристичної функції, нечіткі множини є природним узагальненням звичайних множин, коли двійковий характер характеристичної функції відмовляється і приймається

Опишемо багато молодих людей. Формально це можна записати так: V = {група молодих людей}.

Оскільки вік зазвичай починається з 0, нижня межа цього набору має дорівнювати нулю. Верхню межу визначити складніше. Спочатку встановимо верхню межу, наприклад, 20 років. Отже, ми маємо B як чітко обмежений інтервал, B = [0,20]. Виникає питання: чому хтось молодий у 20 років, а не завтра? Очевидно, це структурна проблема, і якщо ви перемістите верхню межу в іншу точку, ви можете поставити те саме запитання.

Більш природний спосіб створення множини B — послаблення суворого поділу на молодих і немолодих. Ми зробимо це, роблячи не тільки чіткі судження «Так, він належить багатьом молодим людям» або «Ні, він належить не багатьом молодим людям», а й гнучкі формулювання «Так, він належить до досить молодих людей» або « Ні, він не дуже молодий».

Представимо цю ідею більш формально. У першому прикладі всі елементи міркування закодовані за допомогою 0 або 1. Простий спосіб узагальнити цю концепцію полягає в тому, щоб ввести значення між 0 і 1. Реально, можна навіть припустити нескінченну кількість значень між 0 і 1 .

Інтерпретація чисел із співвідношенням усіх елементів міркувань тепер ускладнюється. Звичайно, число 1 знову відповідає елементу, що належить до множини B, а 0 означає, що елемент точно не належить до множини B. Всі інші значення визначають ступінь приналежності до множини B.

На рисунку 2.2 наведено приклад характеристичної функції множини молодих людей [14].

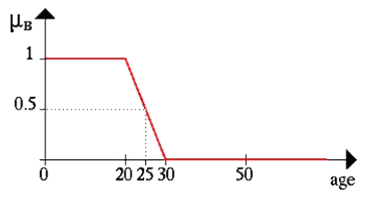


Рисунок 2.2 – Функція приналежності молоді

Наведемо інший приклад нечіткої множини.

Формалізуємо неправильне визначення поняття «гарячий чай». Температурна шкала за Цельсієм діятиме як U (зона оцінки). Очевидно, що вона буде варіюватися від 0 до 100 градусів. Ми створили нечіткий набір для концепції «гарячий чай» наступним чином:

*я*= {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}.

Так, чай з температурою 60°C належить до множини «Гаряче» зі ступенем належності 0,80. Чай при температурі 60 на одну людину°C може бути гарячим, але не дуже гарячим для іншого. Саме в цьому проявляється нечіткість завдання відповідного набору.

Множину А також можна записати у вигляді:

*я*= 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.

або:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Елемент множини А | 0 | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
|  | 0 | 0 | 0 | 0,15 | 0,30 | 0,60 | 0,80 | 0,90 | 1 | 1 | 1 |

Функція приналежності не є ймовірністю, оскільки функція розподілу невідома, повторів експериментів немає. Отже, якщо взяти як приклад розгляд прогнозу погоди, який полягає у визначенні однієї з двох взаємовиключних подій: буде дощ і не буде, і присвоїти їм якісь ранги, то сума цих рангів не обов'язково буде дорівнювати 1, але якщо рівність все ще існує, то нечітка множина буде вважатися нормалізованою. Значення функції приналежності можуть бути взяті тільки з апріорних знань, експертних опитувань.

Існує два методи побудови функцій належності [14].

Зазвичай використовуються прямі методи, коли експерт або просто задає значення для кожного h U, або визначає функцію належності аналітично, тобто за допомогою формул. Як правило, прямі методи завдання функцій приналежності використовуються для вимірювання таких понять, як швидкість, час, відстань, тиск, температура і т.д., або при виділенні полярних величин.

При прямих методах застосовують також групові прямі методи, коли, наприклад, групі експертів демонструють певне обличчя і кожен повинен дати одну з двох відповідей: «ця людина лиса» або «ця людина не лиса», тоді кількість ствердних відповідей, поділена на загальну кількість експертів, дасть оцінку (даної людини).

На практиці існує суб’єктивна схильність експертів оцінювати об’єкти за кінцями оціночної шкали, тому прямі методи, засновані на прямому визначенні значення функції приналежності, зазвичай використовують лише тоді, коли такі помилки є незначними або малоймовірними.

Непрямі методи визначення значення функції приналежності застосовуються у випадках, коли відсутні елементарні вимірювальні властивості, за допомогою яких визначається нечітка множина. Наприклад, поняття «КРАСА», яке, на відміну від понять «ДОВЖИНА» і «ВИСОТА», складніше і важко формалізується. У таких випадках рангові показники використовуються в попарному порівнянні об’єктів, коли порівнюються всі можливі пари для визначення переваг об’єктів.

У непрямих методах значення функції належності вибираються так, щоб вони задовольняли сформульованим раніше умовам. Експертна інформація – це лише необроблені дані для подальшої обробки. Додаткові умови можуть стосуватися як типу отриманої інформації, так і процедури обробки. Прикладами додаткових умов можуть бути наступні: функція приналежності має відображати близькість до попередньо призначеного еталонного показника; об'єкти множини U є точками в просторі параметрів; результатом процедури обробки має бути функція належності, яка задовольняє умови інтервальної шкали.

Непрямі методи більш трудомісткі, ніж прямі, але їх перевагою є стабільність по відношенню до спотворень відгуку.

Непрямі методи, як і прямі, можуть бути як для одного експерта, так і для групи експертів [14].

Основою для операції нечіткого логічного висновку є база правил, яка містить нечіткі твердження виду «Якщо щось» і функції приналежності для відповідних лінгвістичних термінів. При цьому необхідно дотримуватися наступних умов:

1) існує принаймні одне правило для кожного лінгвістичного терміна вихідної змінної;

2) для будь-якого терміна вхідної змінної існує хоча б одне правило, в якому цей термін використовується як передумова (ліва частина правила).

Загалом механізм логічних міркувань включає чотири етапи: введення неоднозначності (фазифікація), нечіткий висновок, композиція та доведення до ясності, або дефазифікація (рис. 2.3) [17].



Рисунок 2.3 – Система нечіткого логічного висновку

Алгоритми нечіткого висновку в основному відрізняються типом використовуваних правил, логічними операціями та типом методу дефазифікації. Розроблено моделі нечіткого висновку Мамдані, Сугено, Ларсена та Цукамото.

Розглянемо нечіткий висновок докладніше на прикладі механізму Мамдані. Це найпоширеніший метод логічних міркувань у нечітких системах. Він використовує мінімаксну композицію нечітких множин. Цей механізм включає наступний ряд дій [18]:

1) процедура фазифікації: визначаються ступені істинності, тобто значення функцій належності для лівих частин кожного правила (передумови). Для бази правил із m правил ми позначаємо ступінь істинності як

*Аi.k*(X*k*), i=1…..m, k=1…..n; (2.1)

2) нечіткий висновок. Спочатку визначаються «порогові» рівні для лівої частини кожного правила:

альфа*і* = min(A*i.k*(X*k*)) (2,2)

*і*

Далі є «скорочені» вихідні функції належності:

Bi\*(i)= min(альфа*і*, Б*і*(i)); (2.3)

*і*

3) композиція, тобто об’єднання отриманих скорочених функцій, для якого використовується максимальна композиція нечітких множин:

*MF*(i)= (Bi\*(i)), (2.4)

*і*

де MF (i) – функція належності скінченної нечіткої множини;

4) затьмарення або доведення до ясності. Існує кілька методів дефазифікації. Наприклад, метод середнього центру або метод центру:

*MF*(i)= max (Bi\*(i)), (2.5)

*і*

Геометричне значення цієї величини є центром ваги для кривої MF (i). На малюнку 2.4 графічно показано процес нечіткого висновку Мамдані для двох вхідних змінних і двох нечітких правил R1 і R2 [18].

Основним недоліком нечіткого висновку на основі класичного механізму Мамдані є те, що для будь-яких вхідних даних необхідно обробляти всю базу правил, тобто виконувати три кроки (визначення значення функцій належності для вхідних змінних, мінімаксну композицію та дефазифікацію). Такий спосіб обробки нечітких даних знижує швидкість роботи системи та вимагає витрат пам'яті [16].

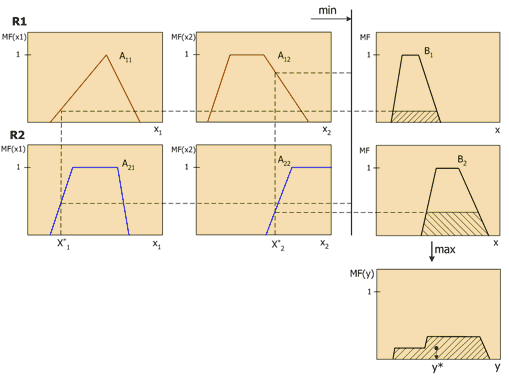


Рисунок 2.4 - Схема нечіткого висновку Мамдан

Суть обробки нечітких даних на основі методу Мамдані полягає в тому, що процес обробки нечіткої вхідної інформації поділяється на етапи навчання та експлуатації. Під час навчання блоку обробки нечітких даних визначаються області вихідних функцій належності для кожного з правил. Під час роботи вхідні дані спочатку порівнюються зі значеннями вихідних функцій належності в областях пам’яті, визначених базою правил, де зберігаються значення вказаних вихідних функцій належності, що відповідають кожному правилу нечіткого логічного висновку. Тоді значення вихідних функцій належності, що перевищують вхідні дані, відсікаються. Потім вибираються мінімальні значення функцій належності виходів, отриманих після відсікання, і з них будується відповідна фігура. Останньою операцією обробки нечітких даних є знаходження центру тяжіння фігури, отримані в результаті додавання усічених вихідних функцій належності. На рисунку 2.5 наведена схема алгоритму реалізації запропонованого методу обробки нечіткої інформації [16].

Реалізація методу модульної оцінки

Кінець

Початок

Визначення площі

функції членства

виходить

Вчитись

Введіть значення вхідних змінних для навчання

Введення поточних значень

критерії

Порівняння вхідних даних зі значеннями вихідної функції належності

Перетин осей і вихідних функцій належності у відповідних областях

Вибір мінімальних поверхонь різу

Побудова фігури з нарізних поверхонь

Знаходження центру ваги отриманої фігури

Операція

Рисунок 2.5 - Схема алгоритму обробки нечітких даних на основі методу Мамдані

Запропонований метод обробки нечітких даних на основі механізму Мамдані дозволяє підвищити швидкодію системи, що розв’язує прикладні інженерні задачі, шляхом поділу процесу її впровадження на фази навчання та експлуатації.

Пропонована система ідентифікації співробітників складається з підсистеми ідентифікації клієнта, командної підсистеми та блоку обробки інформації (рисунок 2.6).

Підсистема

і

ідентифікації

Команда

підсистема

Блок обробки

інформації

Рисунок 2.6 Структура системи ідентифікації

Підсистема ідентифікації надає дані про задіяний блок обробки інформації.

Отже, якщо працівник є новим у даній системі або має дуже низький рівень довіри, то необхідний рівень стійкості має бути максимальним, тобто дорівнювати 1. І навпаки, для працівника з дуже високим рівнем довіри значення відмовостійкості може відразу перейти до 0, що забезпечить збільшення швидкості системи.

Блок обробки інформації обробляє отриману інформацію та подає в командну підсистему висновок про надання доступу до підприємства-працівника.

Розроблена система ідентифікації в середовищі Matlab буде мати такий вигляд (рис. 2.7):

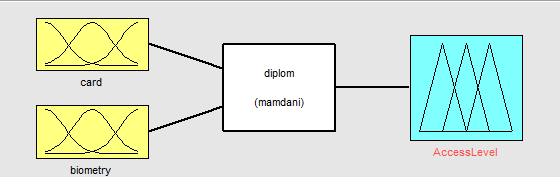


Рисунок 2.7 - Структурна схема засобу ідентифікації співробітників

де Sard, біометричні дані - це входи, що вказують на зчитування з карти та біометрику обличчя відповідно;

AccessLevel - вихід, знаходиться в двох станах: надати доступ або заборонити.

2.2 Реалізація проекту за допомогою MATLAB

Fuzzy Logic Toolbox — це пакет розширення MATLAB, який містить інструменти для проектування систем нечіткої логіки.

Пакет дозволяє створювати експертні системи на основі нечіткої логіки, виконувати кластеризацію за допомогою нечітких алгоритмів і проектувати нечіткі нейронні мережі.

Пакет містить графічний інтерфейс для інтерактивного покрокового проектування нечітких систем, функції командного рядка для розробки програм, а також спеціальні блоки для побудови нечітких логічних систем у Simulink.

Усі функції пакету написані на відкритій мові MATLAB, що дозволяє контролювати виконання алгоритмів, модифікувати вихідний код, а також створювати власні функції та процедури [19].

Основною концепцією Fuzzy Logic Toolbox є структура FIS – система нечіткого логічного висновку (Fuzzy Inference System). FIS-структура містить усі необхідні дані для реалізації функціонального відображення «вхід-вихід» на основі нечіткого логічного висновку за схемою, зображеною на рисунку 2.8 [20].

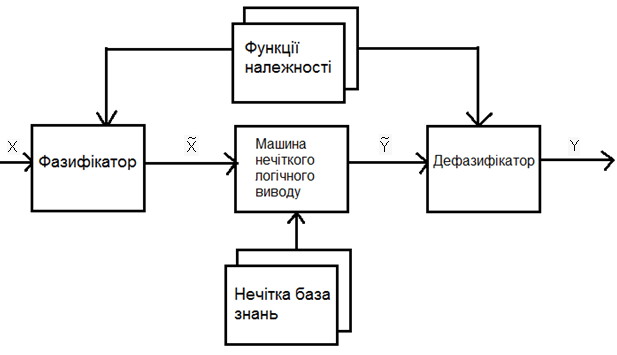


Рисунок 2.8 - Нечіткий логічний висновок

– вхідний інший вектор;

- вектор нечітких множин, відповідний вхідному вектору Ks;

- результат логічного висновку у вигляді вектора нечітких множин;

є вихідним відмінним вектором.

Основними перевагами використання Fuzzy Logic Toolbox є:

- графічний інтерфейс для інтерактивного, покрокового проектування нечітких систем;

- функції створення експертних систем на основі нечіткої логіки;

- підтримка логіки AND, OR та NOT у настроюваних правилах;

- стандартні типи експертних систем нечіткої логіки (Mamdani, Sugeno);

- функції нейроадаптивної та нечіткої кластеризації з навчанням;

- включення нечітких систем у модель Simulink;

- генерація C-коду та незалежних додатків, які реалізують системи нечіткої логіки.

За допомогою Fuzzy Logic Toolbox середовища MATLAB 7.9.0 (R2009b) можна побудувати систему нечіткої ідентифікації в залежності від вартості картки (карти) та біометричних даних (біометрії).

В якості вхідних даних вибираються значення, які будуть зчитуватися з картки співробітника, а також біометричні дані особи. Сукупність цих вихідних даних дозволить більш точно визначити рівень доступу до підприємства. Це буде або повний доступ, або доступ буде заборонено.

Значення функцій належності можуть визначатися різними функціями: трапецієподібної, дзвоноподібної, трикутної та ін. Розглянемо дзвоноподібну та трикутну функції, оскільки вони будуть використані в подальшій роботі.

Дзвоноподібна функція належності [21].

Синтаксис:

*і*= gbellmf (k, параметри) (2.5)

Функція gbellmf визначає функцію належності як симетричну криву у формі дзвона. Ця функція задана формулою

, (2.6)

параметри якого геометрично інтерпретуються наступним чином:

*a*- коефіцієнт концентрації функції належності;

*b*- коефіцієнт нахилу функції належності;

*в*- координата максимуму функції належності.

Функція gbellmf використовується для визначення гладких симетричних функцій належності. Функція gbellmf має два вхідних аргументи:

1) k – вектор, для координат якого необхідно обчислити ступені приналежності;

2) params – вектор параметрів функції належності. Порядок налаштування параметрів [abc].

Функція gbellmf повертає вихідний аргумент i, що містить ступені приналежності координат вектора k.

приклад:

k = 0:0,1:10;

i1 = gbellmf (k, [3 1 5]);

i2 = gbellmf (k, [3 2 5]);

i3 = gbellmf (k, [3 3 5]);

графік (k, [i1; i2; i3])

заголовок ('gbellmf, a=3, b=1,…,3, c=5')

legend('b=1', 'b=2', 'b=3')

2.9 показано приклад побудови дзвоноподібних графіків функцій приналежності з різними коефіцієнтами нахилу [21].

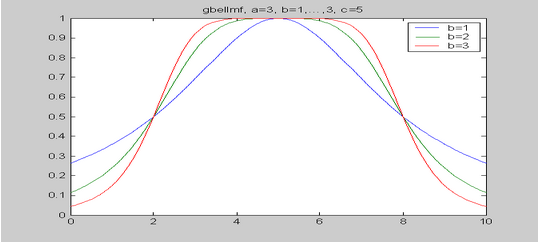


Рисунок 2.9 – Дзвоноподібні графіки функцій належності з різними коефіцієнтами нахилу

Трикутна функція належності [22].

Синтаксис:

*і*= trimf (k, параметри) (2.7)

Функція trimf задає функцію належності у формі трикутника. Це проста і широко використовувана функція членства. Трикутна функція належності задана такою аналітичною формулою

(2,8)

Параметри трикутної функції належності зазвичай інтерпретуються як:

[a, c] - змінний діапазон зміни;

*b*- максимально можливе значення змінної.

Функція trimf має два вхідних аргументи:

1) h – вектор, для координат якого необхідно обчислити ступінь приналежності;

2) params – вектор параметрів функції належності. Порядок призначення параметрів [abc]. Параметри функції належності повинні задовольняти умову .

Функція trimf повертає вихідний аргумент i, який містить ступінь приналежності координат вектора k [22].

приклад:

k = 0:0,1:10;

i1 = trimf (k, [0 0 10]);

i2 = trimf (k, [0 3 10]);

i3 = trimf (k, [0 7 10]);

графік (k, [i1; i2; i3])

заголовок (' trimf, a=0, b=0...7, c=10')

легенда ('b=0', 'b=3', 'b=7')

Значення функцій приналежності вхідних змінних і біометричної картки задається дзвоноподібною функцією, заданою чотирма числами (a, b, c, d), які позначають абсциси піків дзвоника.

Вихід функції належності1 задається трикутною формою, яка залежить від трьох змінних (a, b, c) (абсцис вершин трикутника).

Моделювання нечіткого висновку здійснюється відповідно до типу Мамдані, описаного вище.

Функції приналежності для картки та біометричних змінних показано на малюнках 2.10 і 2.11 відповідно. Вони поділені на три інтервали.

Змінні використовуються для вказівки інформації про картку,і.

Пропонуються змінні для вказівки біометричних даних обличчя,і, що відповідає низькому, середньому та високому рівням.

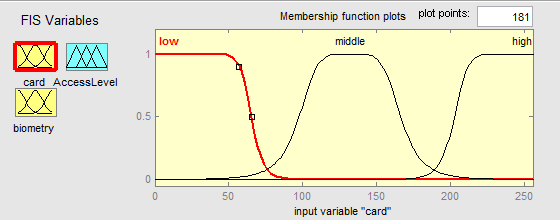


Рисунок 2.10 – Функції приналежності змінної картки

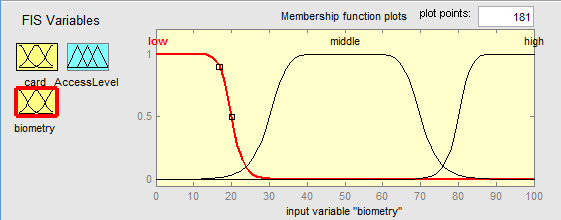


Рисунок 2.11 - Функції належності змінної біометрії

Функції належності для вихідної змінної output1 показано на малюнку 2.12. Вони позначені однаковими інтервалами на осі ординат з метою точного визначення центру ваги, що свідчить про нечіткий висновок системи [23].

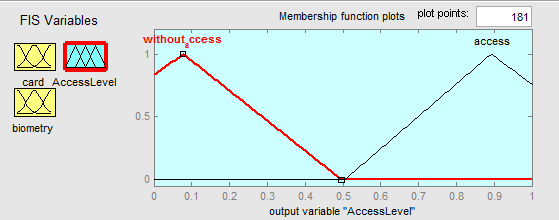


Рисунок 2.12 – Функції належності змінної AccessLevel

no\_access означає, що доступ не надано, access означає, що доступ надано.

База знань для побудови цієї нечіткої моделі складається з правил якщо-тоді, усі вхідні змінні мають три нечіткі стани та інший стан без, коли значення вхідної змінної не вказано системою. Випадок, коли не задані значення всіх вхідних змінних, на практиці неможливий, тому кількість правил нечіткого виведення досліджуваної системи дорівнює.

Система правил нечіткого виведення для розробленої системи виглядає так:

1. Якщо (картка низька) і (біометрія низька), то (вихід1 — no\_access)

2. Якщо (картка має низький рівень) і (біометрія має середній рівень), то (вихід 1 — no\_access)

3. Якщо (картка маленька) і (біометричний показник високий), то (вихід 1 – це доступ)

4. Якщо (картка низька), то (вихід1 — no\_access)

5. Якщо (картка середня) і (біометрія низька), то (вихід1 — no\_access)

6. Якщо (карта посередині) і (біометрія посередині), то (вихід 1 – доступ)

7. Якщо (картка середня) і (біометричний показник високий), то (вихід 1 – доступ)

8. Якщо (табуляція посередині), то (вихід1 — no\_access)

9. Якщо (картка має високий рівень) і (біометричний показник низький), то (вихід1 — no\_access)

10. Якщо (картка має високий рівень) і (біометричний показник є середнім), то (вихід 1 – це доступ)

11. Якщо (картка має високий рівень) і (біометричний показник високий), то (вихід 1 – це доступ)

12. Якщо (картка має високий рівень), то (вихід1 — no\_access)

13. Якщо (біометричний показник низький), то (вихід1 — no\_access)

14. Якщо (біометричний показник середній), то (вихід1 — відсутність\_доступу)

15. Якщо (біометричний показник високий), то (вихід 1 — доступ)

2.3 Функціональне моделювання проекту

Фазовий висновок моделі на основі заданих 15 правил з поточними значеннями змінних картки, біометрії та рівня доступу має вигляд, показаний на рисунку 2.13.

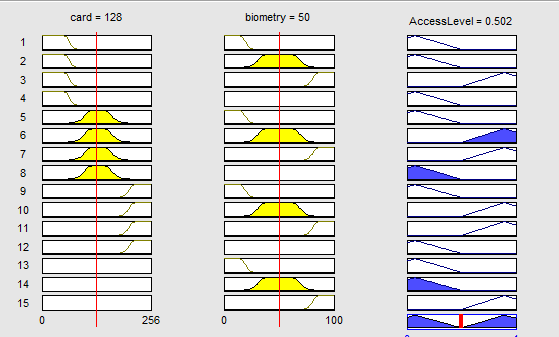


Рисунок 2.13 – Вихід нечіткої моделі

Переміщаючи шкалу на входах системи від меншого до більшого і навпаки, можна перевірити правильність роботи розробленого пристрою (табл. 2.2).

Таблиця 2.2 - Термін дії правил

|  |  |  |
| --- | --- | --- |
| картка | Біометрія | Рівень доступу |
| 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 |

Перелік побудованої моделі за класичним механізмом Мамдані, розробленої за допомогою засобів MATLAB, представлено в Додатку А.

Поверхня значень нечіткої системи на основі механізму Мамдані показана на рисунку 2.14. Це підтверджує правильність побудови бази правил нечіткого висновку.

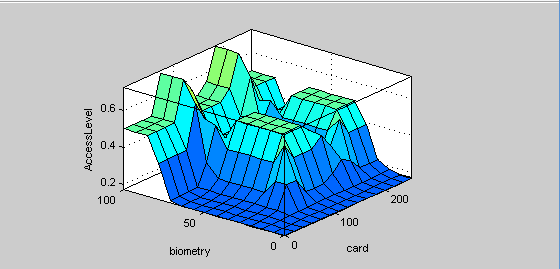


Рисунок 2.14 - Поверхня вихідних значень нечіткої системи на основі механізму Мамдані

Основним недоліком нечіткого висновку, заснованого на класичному механізмі Мамдані, є те, що для будь-яких вхідних даних необхідно обробляти всю базу правил, тобто виконувати три кроки. Однак головною перевагою є просте розширення фазової системи через входи та її робота в реальному часі.

3 ВПРОВАДЖЕННЯ ПРОЕКТУ БЕЗПЕКИ ДОСТУПУ В КОМПАНІЇ

3.1 Модель розробленого нечіткого контролера з використанням Simulink

Розробка інструментів для забезпечення доступу в компанії буде здійснюватися в пакеті програм Matlab, який описаний в пункті 1.3. Для роботи використовується Matlab версії 7.9.0, яка має такі системні вимоги (мінімальні):

- Операційна система: Windows XP (SP2) / 2003 (SP2) / Vista (SP1);

- Процесор: Celeron (SSE2) / Pentium 4 / Xeon / Athlon 64 (SSE2) / Opteron 1,4 ГГц;

- Пам'ять: 512 Мб;

- Відеокарта: 128 MB, 16 bit, OpenGL;

- Вільне місце на залізниці: 680 Мб.

Особливості цієї версії програми включають наступне:

- версія для роботи тільки в середовищі Windows (є версія з такою ж назвою продукту для систем UNIX: Linux, Solaris, Mac);

- математика та розрахунки;

- розробка алгоритмів;

- візуалізація даних;

- зовнішні інтерфейси;

- MEKS - файли;

- набори інструментів.

Пакет Matlab 7.9.0 містить ряд функцій для побудови графіків, включаючи тривимірний, візуальний аналіз даних і створення анімаційних відео.

Головне вікно Matlab виглядає так (рис. 3.1).

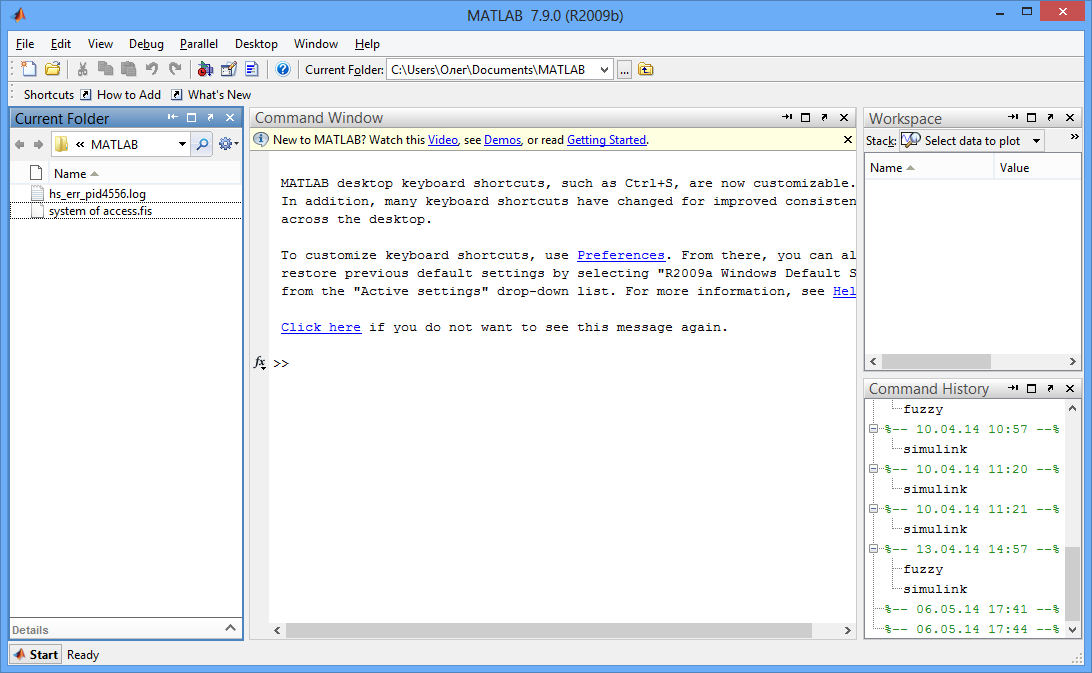


Рисунок 3.1 – Головне вікно Matlab 7.9.0

Вбудоване середовище розробки дозволяє створювати графічний інтерфейс користувача з різними елементами керування, такими як кнопки, поля введення тощо. За допомогою компонента MATLAB Compiler ці графічні інтерфейси можна перетворити на незалежні програми, які потребують інсталяції бібліотеки MATLAB Component Runtime для роботи на інших комп’ютерах.

Інструмент Simulink, що входить до пакету програм Matlab, використовується для побудови моделі інструменту ідентифікації співробітників компанії. Це дозволяє моделювати динамічні властивості системи та бачити результати після початку моделювання. Щоб гарантувати задану швидкість і точність моделювання, Simulink надає вирішувачі ODE з фіксованим і змінним кроком, графічний налагоджувач і програму для оцінки часу виконання окремих функцій моделі [25].

Щоб запустити Simulink, введіть simulink у робочому середовищі Matlab і натисніть Enter. Після цього з’явиться вікно Simulink Library (Simulink Library Browser) (рис. 3.2).

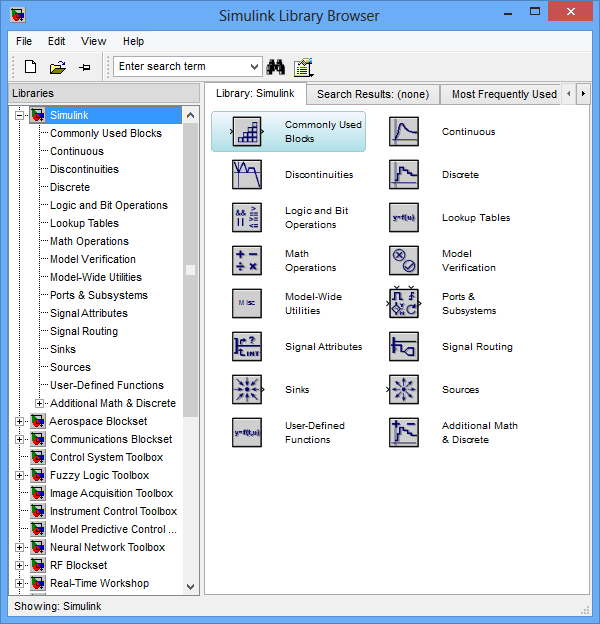


Рисунок 3.2 – Браузер бібліотеки Simulink

Переглядач бібліотек Simulink містить бібліотеку блоків широко використовуваних систем моделювання [25].

Ця бібліотека включає:

- блоки неперервної та дискретної динаміки, такі як Integrator та Unit Delay;

- алгоритмічні блоки, такі як Sum, Product, Lookup Table;

- структурні блоки, такі як Мук (Multiplexer), Перемикач (Svitch), Селектор шин (Bus Selector).

Для побудови моделі створюється новий проект (New Model), після чого відкривається робоча область, в яку переміщуються необхідні об'єкти. Ця система вимагає наступного (рис. 3.3):

а) генератор випадкових чисел (Random Number);

б) осцилограф (Scope);

в) мультиплексор (Мук);

г) нечіткий контролер (Fuzzy Logic Controller).

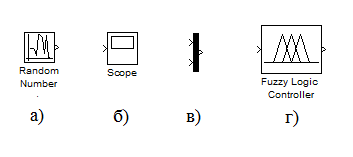


Рисунок 3.3 – Об’єкти побудови моделі доступу

Оскільки система працюватиме на основі даних зчитування карток і біометрії, модель складатиметься з:

- два генератори випадкових чисел, для яких вказана картка з іменами та біометрією;

- три осцилографи - два на вхід (картка1 і біометричний1) і один на вихід (доступ);

- один мультиплексор для підключення двох входів;

- нечіткий контролер (Fuzzy Logic Controller).

Fuzzy Logic Controller — це нечіткий контролер, побудований на основі нечіткої логіки. Його реалізація вимагає [26]:

1) визначити вхідні лінгвістичні змінні. Наприклад, «час ділового візиту» та «частота ділового візиту» для аналізу ділового візиту;

2) визначте мовну змінну, яку потрібно отримати. У цьому випадку це буде лінгвістична змінна «відвідуваність»;

3) визначити правила побудови результуючої змінної з вхідних даних.

Сфери практичного застосування:

- використовується самостійно для виконання функцій лінійного перетворювача з автоматичним керуванням;

- використовуються при вирішенні завдань алгоритмічної обробки інформації від досліджуваного об'єкта (задачі фільтрації);

- в системах з нечіткою послідовністю процедур перевірки статистичних гіпотез.

Ця модель нечіткого висновку працює відповідно до класичного механізму Мамдані, описаного в розділі 2.1, показаного на малюнку 3.4.

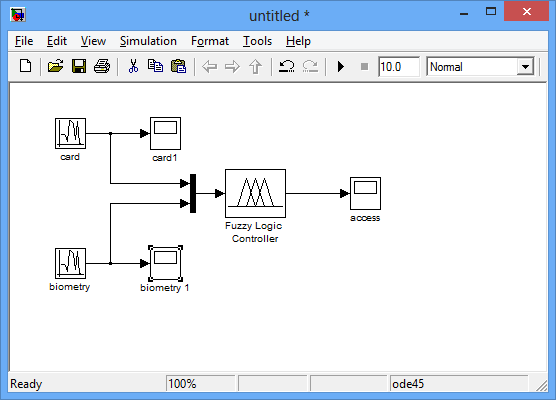


Рисунок 3.4 – Модель розробленого інструменту

Входами нечіткого контролера (Fuzzy Logic Controller), який працює за механізмом Мамдані, є значення карти (card) і біометрії (biometrics), а виходом - рівень безпеки доступу, описаний в таблиці 2.2. . .

Щоб запустити симуляцію, ви повинні спочатку встановити шлях до нашої системи в контролері нечіткої логіки. Для цього подвійним клацанням миші відкривається вікно параметрів Fuzzy Logic Controller, де вводиться шлях до нашої системи (рис. 3.5).

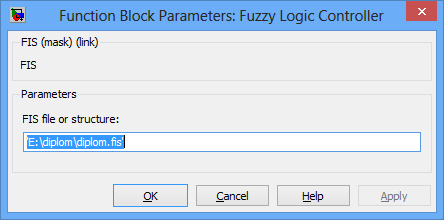


Рисунок 3.5 – Параметри контролера Fuzzy Logic

Після виконання дій можна побачити значення, які виводить осцилограф. Для цього спочатку клацніть правою кнопкою миші на картці осцилографа та виберіть «Подивитися під маскою». Така ж операція виконується з осцилографом, який відповідає за біометрію. В результаті моделювання значення даних осцилографа показані на малюнках 3.6 і 3.7 відповідно.

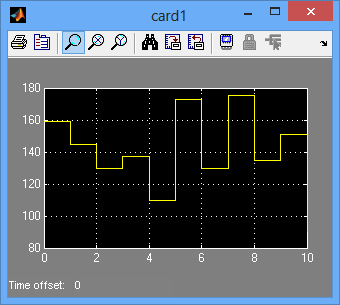


Рисунок 3.6 - Плата осцилографа

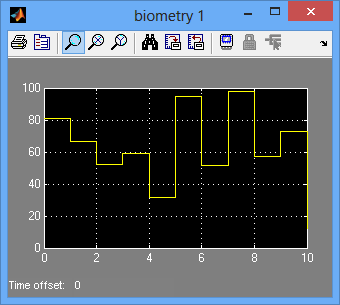


Рисунок 3.7 - Біометричний осцилограф

Як видно на малюнках 3.6 і 3.7, значення обох карток і біометрії не перевищують значення, які були спочатку встановлені (256, 100 відповідно).

На рисунку 3.8 показано фрагмент схеми нечіткого контролера для ідентифікації співробітників компанії. Загальна схема нечіткого контролера наведена в Додатку Б.

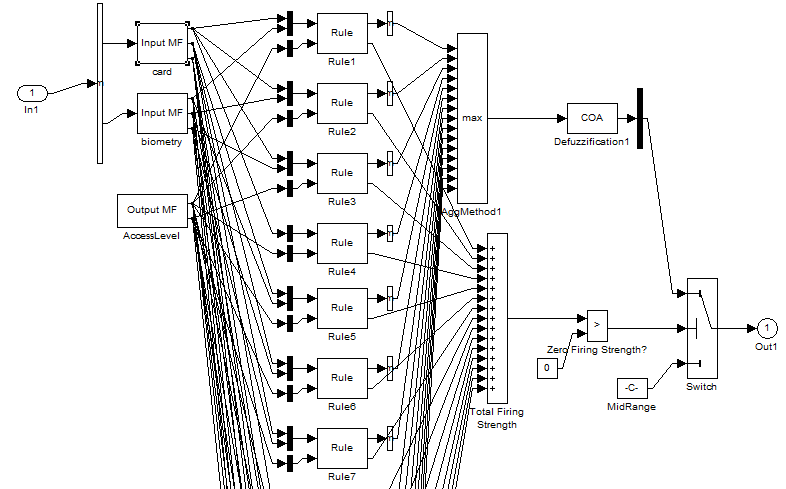


Рисунок 3.8 - Фрагмент схеми фазорегулятора

Розроблена схема нечіткого контролера складається з трьох блоків опису функцій належності вхідних змінних (Input MF blocks), блоку опису вихідних функцій належності (Output MF), виходи яких подаються на вхід. з 15 правил (блоки Правило 1 ... 15).

3.2 Перевірка правильності роботи нечіткого контролера

Схема розрахунку функцій належності вхідних і вихідних змінних, побудована системою Simulink, наведена на рисунку 3.9 і 3.10 відповідно.

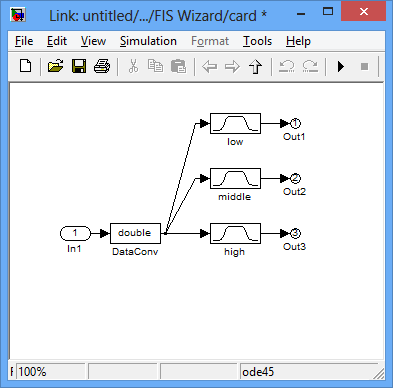


Рисунок 3.9 – Схема розрахунку функцій, що належать вхідним змінам

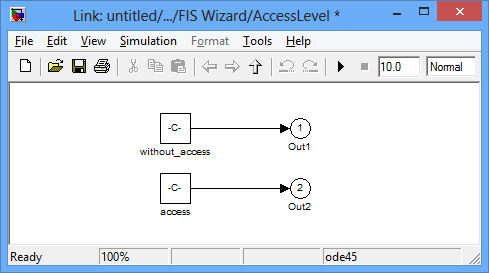
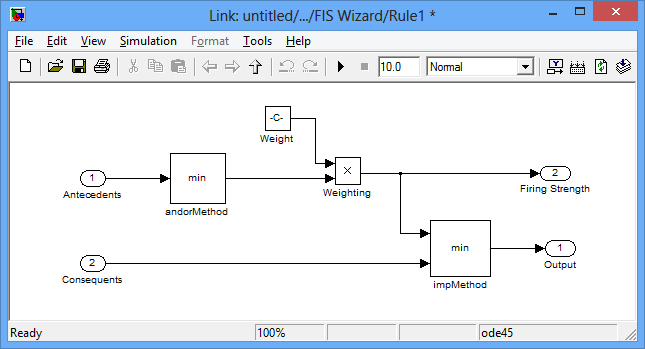


Рисунок 3.10 – Схема розрахунку функції належності вихідної змінної

Побудова кінцевої фігури для знаходження центру тяжіння та обробки нечітких змінних виконується згідно з механізмом Мамдані, який описано в пункті 2.1, схему якого показано на малюнку 2.4.

Щоб обробляти правила з бази знань, Simulink бере до уваги оцінку, яка представлена ​​константою ваги. На рисунку 3.11 показана схема обробки нечітких значень. Блок-схема правила «якщо щось» наведена в Додатку D.



Малюнок 3.11 -Схема обробки нечітких вхідних значень за правилом «якщо щось».

Значення вхідних змінних картки та біометричних даних є входами до правил і відповідають входу 1, а вхід 2 відповідає за рівень доступу, який буде надано при заданій умові. Блок Min відповідає за обробку даних, яка відбувається за законом мінімуму. Значення функції належності виходу AccessLevel (вихід 1) і послідовність, що представляє інтервал налаштування цього виходу (вихід 2), є виходами цієї схеми.

Щоб знайти центр ваги кінцевої фігури, яка утворилася в результаті підсумовування виходу 15 правил, тобто зробити висновок за механізмом Мамдані, нечіткий контролер виконує дефазифікацію. Схема дефазифікації показана на рисунку 3.12.

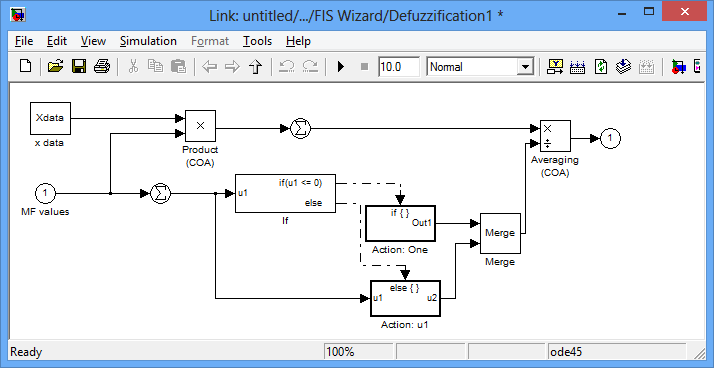


Рисунок 3.12 – Схема дефазифікації нечіткого висновку

Дефазифікація виконується за такою формулою:

(3.1)

декількість прямокутників, на які ділиться кінцева фігура,

значення абсцис,

значення ординати-ї фігури.

Структурна схема дефазифікації нечіткого висновку наведена в додатку D.

Результатом роботи моделі з вхідними значеннями картки та біометрії (див. рис. 3.6, 3.7) є значення центру ваги, наведене на рис. 3.13.

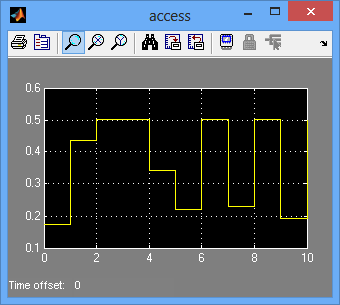


Рисунок 3.13 – Результати розробленої нечіткої моделі

Тестові значення вхідних і вихідних змінних системи нечіткої ідентифікації співробітників компанії наведені в таблиці 3.1.

Таблиця 3.1 - Тестові значення змінних системи нечіткої ідентифікації співробітників компанії

|  |  |  |  |
| --- | --- | --- | --- |
| ні | картка | Біометрія | Рівень доступу |
| 1 | 2 | 3 | 4 |
| 1 | 160 | 81 | 0,18 |
| 2 | 147 | 68 | 0,44 |
| 1 | 2 | 3 | 4 |
| 3 | 130 | 56 | 0,5 |
| 4 | 139 | 60 | 0,5 |
| 1 | 2 | 3 | 4 |
| 5 | 111 | 33 | 0,34 |
| 6 | 176 | 96 | 0,23 |
| 7 | 129 | 52 | 0,5 |
| 8 | 178 | 98 | 0,24 |
| 9 | 138 | 58 | 0,5 |
| 10 | 152 | 76 | 0,19 |

Аналізуючи таблицю 3.1, можна констатувати, що середнє відхилення результатів системи від значення нечіткого регулятора, що працює за механізмом Мамдані, становить не менше 0,1. Ці дані підтверджують правильність роботи та ефективність системи.

3.3 Захист розробленої нечіткої системи

Заходи захисту, пов’язані з нечіткою системою ідентифікації працівників у компанії, повинні:

- відповіді на погрози;

- розроблятися таким чином, щоб врахувати можливу шкоду від їх реалізації;

- забезпечити ефективність захисту нечіткої системи ідентифікації працівників компанії протягом визначеного періоду часу.

Нечітка система ідентифікації співробітників компанії у вигляді контролера може бути реалізована на програмованих логічних матрицях (PLM) або програмованих логічних інтегральних схемах (PLC).

Система з контролером нечіткої ідентифікації співробітників дозволяє зберегти конфіденційність, цілісність і приватність даних, до яких буде здійснюватися доступ. Такі контролери виготовляються як готові апаратні вироби.

Основними недоліками програмних засобів захисту в порівнянні з апаратними є їх недостатня стійкість до злому і низька продуктивність при обробці великих потоків даних, що в більшості випадків призводить до повного виходу системи з ладу.

Сучасні апаратні контролери та системи контролю доступу традиційно реалізуються на базі універсальних програмованих логічних інтегральних схем (ПЛК).

Програмована логічна інтегральна схема (ПЛК) — електронний продукт, який поєднує конструктивні особливості перепрограмованих пристроїв і дискретної логіки. ПЛІС складається з логічних блоків, які з’єднані між собою вентильною схемою та матрицею переходів [27].

FPGA мають багато переваг перед звичайною дискретною логікою та перепрограмованими пристроями, такими як мікроконтролери. У мікроконтролерах реалізовано принцип конвеєрної обробки інформації, що викликає затримки у виконанні команд. У деяких випадках навіть невелика затримка у виконанні команд неприпустима, наприклад, при застосуванні на важливих штучних об'єктах.

ПЛІС не мають характерної для мікроконтролерів затримки при виконанні команд, тому що вони працюють за принципами дискретної логічної організації і мають можливість багаторазового програмування завдяки особливій конструкції матриці переходів (внутрішніх зв'язків).

Особливістю FPGA є процес програмування. Коли сигнали програмування подаються на відповідні висновки мікросхеми, матриця переходу переходить у режим програмування. У цьому режимі послідовність виконуваних блоків задається послідовністю імпульсів. Іншими словами, користувач програмує ПЛІС залежно від власних потреб, враховуючи характеристики обладнання, з яким ПЛІС спілкується. Можливість багаторазового програмування і простота комбінування логічних блоків робить процес проектування більш продуктивним і підвищує надійність виробу [27].

FPGA використовувалися протягом кількох десятиліть для побудови різних інтерфейсних вузлів, пристроїв керування та моніторингу тощо. З появою високошвидкісних FPGA надвисокої інтеграції, які працюють на високих тактових частотах, їх ніша на світовому ринку значно розширилася.

До основних переваг ПЛІС можна віднести наступне:

- при створенні логічних пристроїв програміст має в своєму розпорядженні існуючу елементну базу, яка містить все необхідне для проектування, від найпростіших логічних елементів до мікропроцесорів;

- використання ПЛІС загалом дозволяє зменшити розмір апаратного забезпечення порівняно з пристроями, реалізованими на великих інтегральних схемах (ІС);

- програміст, не вдаючись до сторонньої допомоги, може коригувати свою схему скільки завгодно разів, не вносячи змін у друковану плату. Цей спрощений процес налагодження дозволяє скоротити період розгортання пристроїв на основі PLIM.

Апаратні засоби захисту більш стійкі до злому, ніж програмні. Основними перевагами фурнітури є:

- неможливість фізичного доступу до системи забезпечує захист від несанкціонованого доступу;

- стійкість до атак на відмову в обслуговуванні;

- неможливість дистанційної зміни алгоритму системи;

- автономність.

Для нормального функціонування апаратної системи необхідно дотримуватися певних правил її експлуатації - забезпечувати постійне безперебійне електропостачання, підтримувати відповідні умови зовнішнього середовища (вологість, температура тощо), захищати систему від зовнішнього впливу. впливи - фізичні пошкодження, електромагнітне випромінювання та ін.

Враховуючи те, що розробляється програмно-апаратна система ідентифікації співробітників компанії, крім апаратного захисту необхідний і програмний захист для запобігання несанкціонованому доступу. Захист здійснюватиметься шляхом ідентифікації користувача.

При запуску програми ідентифікації користувача з'явиться діалогове вікно, в якому необхідно ввести свою особисту інформацію: ім'я користувача та пароль. Якщо ці дії виконані успішно, користувач авторизується в системі.

Після входу в систему користувач може працювати з певним набором об'єктів, але якщо він спробує використати об'єкт, до якого він не має прав доступу, з'явиться повідомлення «Доступ заборонено».

Інструменти адміністрування, які дозволяють розподіляти доступ при роботі в мережі персональних комп’ютерів, а також для вирішення завдань інтеграції, розташовані в додатку «Керування комп’ютером» (рис. 3.14). Щоб отримати доступ до цієї програми, необхідно виконати наступну послідовність дій:

Панель управління - Адміністрування - Управління комп'ютером. Після цього відкриється необхідне вікно.

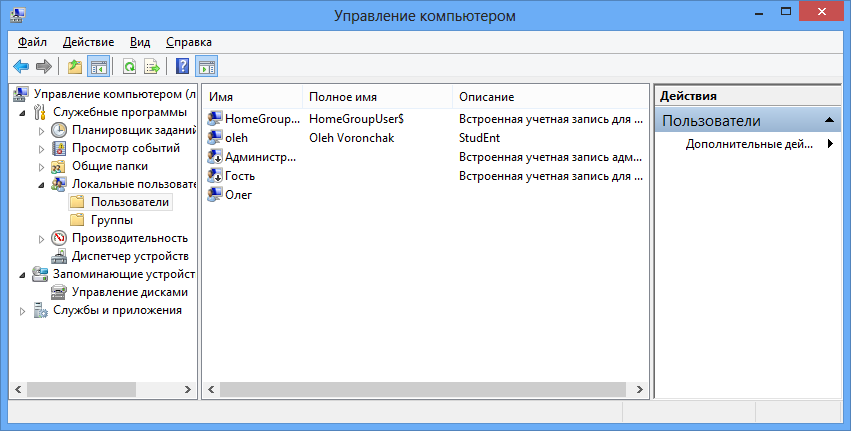


Рисунок 3.14 – Вікно керування комп’ютером.

Головне вікно програми містить усі основні елементи, необхідні для керування системою.

При вході користувача в систему виконується така послідовність дій:

1) перевірка наявності користувача із заданими параметрами;

2) ідентифікуються паролі;

3) перевіряються права доступу користувачів до об'єктів системи.

У додатку «Керування комп’ютером» ви можете виконувати різні дії із записами користувачів, наданими в системі. Найпростіший спосіб - це створити нового користувача. Для цього в меню Користувачі необхідно вибрати пункт Новий користувач, після чого з’явиться вікно створення нового користувача (рис. 3.15).

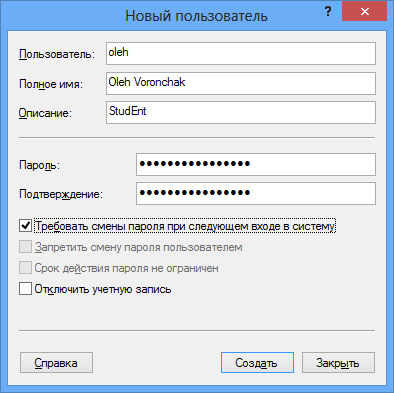


Рисунок 3.15 – Вікно для створення нового користувача

Коли ви створюєте нового користувача, вам може знадобитися заповнити деяку коротку інформацію (ім’я, короткий опис). Після цього пропонується призначити пароль, який після входу необхідно ввести повторно, щоб перевірити його правильність.

Якщо при створенні користувача поставити позначку «Вимагати зміни пароля при наступному вході», то при першому вході користувач спочатку введе поточний пароль, після чого йому доведеться змінити його на новий, і тільки після цього він зможе щоб увійти.

Як тільки буде створено нового користувача, його можна буде видалити. Для цього в меню створеного користувача виберіть пункт Видалити (рис. 3.16).

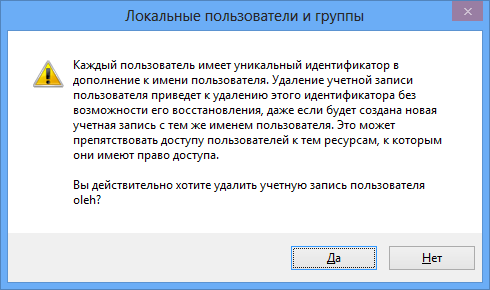


Рисунок 3.16 – Видалення користувача oleh

Є досить важливий параметр, який надає користувачам статус адміністратора. Справа в тому, що навіть якщо користувач не має прав доступу до тих чи інших програмних об'єктів, з опцією «адміністративний доступ», це означає, що незалежно від того, які групи прав доступу до певних програмних об'єктів, з опцією «адміністративний доступ» позначено « Адміністративний доступ» отримає повний доступ (рис. 3.17).

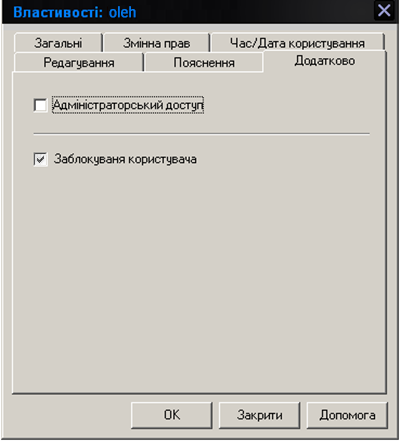


Рисунок 3.17 – Надання адміністративного доступу/блокування користувачів

У цьому ж вікні ви можете заблокувати доступ до системи. Для цього потрібно поставити галочку навпроти Блокувати користувача. Користувач буде заблоковано, доки адміністратор не розблокує його. Перевагою є те, що користувача не потрібно видаляти, а потім створювати заново. Цю операцію слід використовувати, коли є необхідність позбавити прав певного користувача.

Незалежно від кількості створених користувачів, для кожного з них можна встановити параметри, які обмежуватимуть час перебування в системі. Для цього необхідно викликати меню Властивості та встановити час перебування користувача в системі (рисунок 3.18).

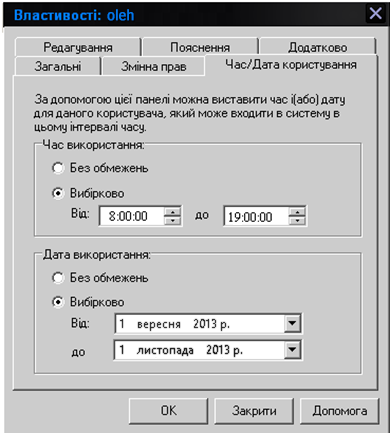


Рисунок 3.18 - Параметри користувача (час роботи)

У випадку, коли необхідно запровадити обмеження роботи на тривалий час, можливе запровадження обмежень за датою.

Захист програмного забезпечення, де примусово дотримуються права доступу користувачів, є досить надійним від несанкціонованого доступу. Його можна використовувати в будь-якій комп'ютерній системі.

ВИСНОВКИ

Під час роботи над дослідженням було виконано:

1) проведено аналіз наявних апаратно-програмних засобів ідентифікації працівників. Аналіз сучасних систем ідентифікації свідчить про очевидний рух у бік біометричних систем, оскільки цей вид розпізнавання є зручним і надійним з точки зору аналізу відповідності контрольного біометричного ключа (символу) конкретному користувачеві;

2) проведено аналіз технічного завдання та постановку завдання;

3) проведено розробку апаратно-програмних засобів ідентифікації на основі фазової логіки. Розроблено структурну схему пристрою, здійснено реалізацію засобами Matlab та проведено функціональне моделювання;

4) проведено реалізацію створеного проекту. За допомогою Simulink розроблено модель нечіткого контролера, перевірено правильність його роботи;

5) дослідження надійності розробленого технічного та програмного забезпечення від несанкціонованого доступу;

Дані, отримані під час функціонального моделювання пристрою, близькі до значень, знайдених під час верифікації нечіткого контролера за допомогою Simulink. На підставі цих даних можна стверджувати, що розроблений апаратно-програмний засіб правильно розроблений і функціонує коректно.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Датчик: веб-сайт. URL: <http://l2u.su/qcui> (дата звернення: 12.02.22).
2. Бурштинський М.В., Хай М.В., Харчишин М.Б. Давачі: навчальний посібник. Львів, 2014. 198 с.
3. Гаврилюк М.О. Давачі систем автоматики: навчальний посібник. Львів, 2010. 180с.
4. Аш Ж.Л. Датчики измерительных систем. Москва, 2008. 904 с.
5. Гуманюк Н.М. Датчики в автоматике. Москва, 2015. 264 с.
6. Іванов А.О. Теорія автоматичного керування: підручник. Дніпропетровськ, 2008. 250 с.
7. Тесленко В.А. Датчики в системах сбора данных и управления. Київ, 2006. 318 с.
8. Novаk V., Perfilieva I., Mockor J. Mathematical principles of fuzzy logic – M: Kluwer Academic Publishers,1999. – P. 15.
9. Щоденник [Електронний ресурс] / Режим доступу до ресурсу: http://company.shodennik.ua/functions/.
10. Zadeh L. Real-Life Applications of Fuzzy Logic // Fuzzy logic now and then – M: Hindawi, 2013. – P. 125.
11. Cintula P. Fuzzy Logics as the Logics of Chains // Fuzzy Sets and Systems – M: Libor, 2006. – P. 606.
12. Godo L. Fuzzy Sets and Systems // Monoidal T-Norm Based Logic: Towards a Logic for Left-Continuous T-Norms – M: Waweland, 2001. – P. 25.
13. Zimmerman H. Fuzzy set theory and its applications // Fuzzy logic intoduction – M: Kluwer, 1991. – P. 315.
14. MathWorks (What Is Fuzzy Logic?) [Електронний ресурс] / Режим доступу до ресурсу: https://www.mathworks.com/help/fuzzy/what-is-fuzzy-logic.html.
15. Yager R. Fuzzy Sets and Applications // Introduction – M: Wiley, 1987. – P. 8.
16. A semantics-driven, fuzzy logic-based approach to knowledge representation and inference [Електронний ресурс] / Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0957417407006276.
17. Expert diagnosis of computer systems using neuro-fuzzy knowledge base [Електронний ресурс] / Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7807669/metrics#metrics.
18. The neuro-fuzzy diagnostic model synthesis with hashed transformation in the sequence and parallel mode [Електронний ресурс] / Режим доступу до ресурсу: https://ric.zntu.edu.ua/article/view/101022/96247.
19. Usability Determination Using Multistage Fuzzy System [Електронний ресурс] / Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S1877050916000442.
20. A novel fuzzy decision-making system for CPU scheduling algorithm [Електронний ресурс] / Режим доступу до ресурсу: https://link.springer.com/article/10.1007/s00521-015-1987-8.
21. Network-based output tracking control for T-S fuzzy systems using an event-triggered communication scheme(Article) [Електронний ресурс] / Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0165011415000032.
22. Expert evaluation model of the computer system diagnostic features [Електронний ресурс] / Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7027101/metrics#metrics.
23. Diagnosing computer hardware failures using expert system (rule-based technique) [Електронний ресурс] / Режим доступу до ресурсу: https://www.researchgate.net/publication/279205502\_DIAGNOSING\_COMPUTER\_HARDWARE\_FAILURES\_USING\_EXPERT\_SYSTEM\_RULEBASED\_TECHNIQUE.
24. Computer Aided Development of Fuzzy, Neural and Neuro-Fuzzy Systems [Електронний ресурс] / Режим доступу до ресурсу: https://www.researchgate.net/publication/312590719\_Computer\_Aided\_Development\_of\_Fuzzy\_Neural\_and\_Neuro-Fuzzy\_Systems.
25. A fuzzy expert system for automatic seismic signal classification [Електронний ресурс] / Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0957417414005053.
26. Classification of Network Traffic Using Fuzzy Clustering for Network Security [Електронний ресурс] / Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-319-62701-4\_22.
27. Mamdani E. Application of fuzzy algorithms for the control of a simple dynamic plant // Proc. IEEE 121, 1974. – P. 1585-1588.
28. Мирончук Ю., Купріненко О. Побудова функцій належності нечітких множин, які відповідають кількісним експертним оцінкам фізичних величин // Системи обробки інформації. — 2017. — № 1. — С. 93-97.
29. Блюмин С., Шуйкова И., Сараев П. Нечеткая логика: алгебраические основы и приложения: Монография – К.:ЛЭГИ, 2002. – 113 с..
30. Cordon O., Herrera F. A General study on genetic fuzzy systems // Genetic Algorithms in computer science – M:Tante, 1995. – P. 33.
31. Леоненков А. Нечеткое моделирование в MATLAB и fuzzyTECH – СПб.: БХВ-Петербург, 2005. – 736 с.
32. Abadeh M., Habibi J., Lucas C. Intrusion Detection Using a Fuzzy Genetics-Based Learning Algorithm // Journal of Network and Computer Applications. – 2007. – №30. – P. 414-418.
33. Koo T. Analysis of a Class of Fuzzy Controllers, in Proc. 1st Asian Fuzzy Systems Sump – Singapore: Way, 1998. – P. 35-38.
34. Дубчак Л. Метод обробки нечітких даних на основі механізму Мамдані / Л. Дубчак // Системи обробки інформації. – 2012. – №7(105). – 131с.
35. Passino K., Yurkovich S. Fuzzy Control – California: Addison-Wesley, 2001. – 53 P.
36. Iancu I. Extended Mamdani Fuzzy Logic Controller – California: ACTA Press, 2001. – P. 143-149.
37. Лозинський А., Демків Л. Дослідження впливу вигляду функції належності на динамічні показники системи при багатокритеріальній оптимізації зі змінними ваговими коефіцієнтами // Електротехнічні та комп’ютерні системи. - 2012. - № 5. - С. 137-144.
38. Ротштейн А., Штовба С. Идентификация нелинейной зависимости нечеткой базой знаний с нечеткой обучающей выборкой // Кибернетика и системный анализ. – 2006. – №2. – C. 17–24.
39. MathWorks (Simulation and Model-Based Design) [Електронний ресурс] / Режим доступу до ресурсу: https://www.mathworks.com/products/ simulink.html.
40. Рутковская Д., Пилинский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы – М.: Горячая линия – Телеком, 2004. – 452 с.
41. Expert evaluation model of the computer system diagnostic features/ Модель експертної оцінки діагностичних особливостей комп'ютерної системи G. Krivoulya ; A. Shkil ; D. Kucherenko ; A. Lipchansky ; Ye. Shereme, 2016
42. A fuzzy expert system for automatic seismic signal classification/ Нечітка експертна система класифікації автоматичних сейсмічних сигналів, El HassanAit Laasria Es-Saïd Akhouayria Dris Agliza Daniele Zontab Abderrahman Atmania, 2015
43. A semantics-driven, fuzzy logic-based approach to knowledge representation and inference/ Семантико-керований нечіткий логічний підхід до представлення знань, Rodrigo Martínez-Béjara Jose M.Cadenasa Hossein Shirazib Paul Comptonc,2016
44. Computer Aided Development of Fuzzy, Neural and Neuro-Fuzzy Systems / Автоматизована розробка нечітких, нейронних та нейро-нечіткі системи, Priti Srinivas Sajja, 2017
45. Network-based output tracking control for T-S fuzzy systems using an event-triggered communication scheme(Article) / Мережеве керування вихідним відстеженням для нечітких систем T-S з використанням схеми зв'язку, викликаної події, Zhang, D., Han, Q.-L., Jia, X, 2016
46. Николайчук Я.М., Яцків В.В., Гринчишин Т.М. Перспективи створення телефонних ліній на основі відкритого оптичного каналу зв’язку // Вісник Технологічного університету Поділля. – 2002. Т2– №3. – С. 47 – 50.
47. Вильям Столлингс. Криптография и защита сетей: принципы и практика: Пер. с англ. – М.: Издательский дом “Вильямс”, 2001. – 672 с.
48. Рябенький В.М., Жуйков В.Я., Гулий В.Д. Цифрова схемотехніка: Навч. Посібник. - Львів: Видавництво «Новий світ 2000», 2009.-736с.
49. Папушин В. А. Основи автоматизації виробництва / В. А. Папушин, В.С. Білецький. – Донецьк: Східний видавничий дім, 2007. – 168 с.
50. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику: веб-сайт. URL: http://matlab.exponenta.ru/fuzzylogic/book1/ (дата звернення 25.12.2021)