УКРАЇНА

(19) UA (11) 105676 (13) C2

(51) МПК
G06F 15/18 (2006.01)
G06F 17/10 (2006.01)
G06F 19/28 (2011.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2012 06807**

(22) Дата подання заявки: **05.06.2012**

(24) Дата, з якої є чинними права на винахід: **10.06.2014**

(41) Публікація відомостей про заявку: **10.12.2013, Бюл.№ 23**

(46) Публікація відомостей про видачу патенту: **10.06.2014, Бюл.№ 11**

(72) Винахідник(и):
Дубчак Леся Орестівна (UA),
Кочан Володимир Володимирович (UA),
Васильцов Ігор Володимирович (UA),
Карпінський Микола Петрович (UA)

(73) Власник(и):
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ,
вул. Львівська, 11, м. Тернопіль, 46020 (UA)

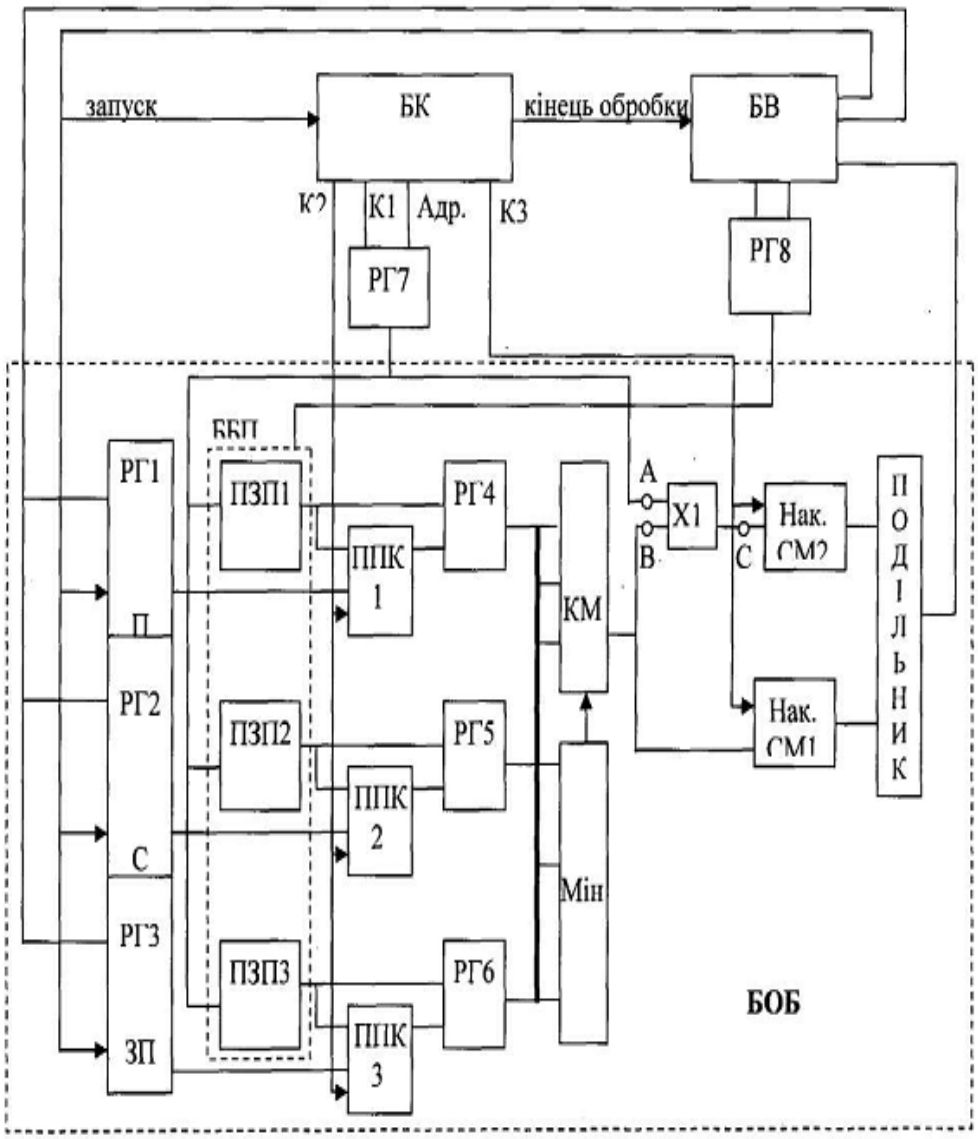
(56) Перелік документів, взятих до уваги експертизою:
Ротштейн А.П., Штовба С.Д. Нечеткая надежность алгоритмических процессов. – Винница: Континент – ПРИМ.,-1997г.-СС. 18-21; 102-107
Рогозин О.В. Метод нечеткого вывода решения в задаче подбора программного обеспечения на основе качественных характеристик этого обеспечения как объекта инвестиций.// Качество. Инновации. Образование. – 2009. - № 3.
UA 71851 A; 15.12.2004
UA 44595 U; 12.10.2009
RU 11354 U1; 16.09.1999
SU 1619252 A1; 07.01.1991
US 2008183642 A1; 31.07.2008
US 5446438 A; 29.08.1995
US 5343553 A; 30.08.1994

UA 105676 C2

(54) ПРИСТРІЙ ДЛЯ ОБРОБКИ НЕЧІТКОЇ ІНФОРМАЦІЇ

(57) Реферат:

Пристрій для обробки нечіткої інформації належить до комп'ютерних пристроїв, які використовують в комп'ютерних мережах. Пристрій містить задавальний елемент, багатоканальний блок пам'яті, багатофункціональний обчислювальний блок, блок керування та блок, що використовує результати оброблення нечіткої інформації. Багатофункціональний обчислювальний блок містить три постійні запам'ятовуючі пристрої, три пристрої порівняння кодів, вісім регістрів, блок пошуку мінімального значення коду, комутатор, перемножувач, два накопичувальних суматори та подільник. Для підвищення точності пошуку центра ваги фігури використано додатково подільник на 2, два квадратори, суматор і блок добування квадратного кореня. Блок керування пропонованим пристроєм містить тригер, ключ, два лічильники, три дешифратори і два формувачі імпульсів. За допомогою запропонованого пристрою досягається підвищення швидкодії та розширення функціональних можливостей.


запуск
БК
кінець обробки
БВ
К2
К1
Адр.
К3
РГ7
РГ8
ББП
РГ1
П
РГ2
С
РГ3
ЗП
ПЗП1
ПЗП2
ПЗП3
ППК 1
ППК 2
ППК 3
РГ4
РГ5
РГ6
КМ
Мін
A
B
C
X1
Нак. СМ2
Нак. СМ1
ПОДІЛЬНИК
БОБ

Фіг. 1

Пристрій призначений для оброблення нечіткої інформації в складі комп'ютерних систем, що функціонують в невизначених умовах, та його можна використати, зокрема, для вибору методу модулярного експоненціювання при розподілі доступу в комп'ютерних мережах залежно від необхідної продуктивності та стійкості комп'ютерної системи до часового аналізу, а також можливих затрат пам'яті.

Характеристикою нечіткої множини виступає функція належності. Існує понад десяток типових форм кривих для задання функцій належності, найбільш поширені трикутна та трапецеїдальна функції належності.

Основою для проведення операції нечіткого логічного висновку є база правил, що містить нечіткі висловлення у формі "Якщо-то" і функції належності для відповідних лінгвістичних термів. Процес оброблення нечіткої інформації проводиться згідно способів виводу, з яких найбільш поширеним є способи Mamdani, Tsukamoto, Sugeno s Larsen'a [1].

Спосіб Мамдані [1, 2] використовує мінімаксну композицію нечітких множин, що дозволяє побудувати залежність функції належності виходу від функцій належності входу. Процес дефазифікації (переходу до чіткого висновку) полягає у знаходженні центра ваги для фігури, яку обмежує збудована залежність функції належності виходу. Логічний висновок за способом Мамдані на прикладі двох правил R1 та R2 зображено на фіг. 1. Спочатку знаходять мінімальні площі в зображеннях функцій належності трьох змінних шляхом відсікання початкових функцій належності входу. Після чого здійснюють об'єднання усічених площ за максимальним законом і, нарешті, знаходиться центр ваги остаточної фігури, який і є висновком нечіткої системи.

Спосіб Мамдані [1, 2], його модифікації або елементи реалізують різні відомі пристрої. Відомі пристрої для обробки нечіткої інформації, що базуються на використанні блоків пам'яті для зберігання значень нечіткого параметра та відповідних значень ступеня належності згідно з заданою формою функції належності досліджуваної нечіткої множини. Прикладом таких пристроїв є пристрій для обробки нечіткої інформації [3], в якому використовується багатоканальний блок пам'яті для зберігання даних з 2N каналами, де N - потужність нечітких множин операндів, а блок вибору одного значення функції належності побудований на схемі порівняння кодів, керованих ключах, схемі АБО на два входи, багатовходових схемах І, багатовходовій схемі АБО з трьома станами по виходу та інверторі. Такий пристрій має наступні недоліки: багатоканальний блок пам'яті має бути розрахований на зберігання великих масивів інформації; введення інформації в нього вимагає значних часових витрат; низька точність обробки інформації через дискретність функції належності, що зберігається в багатоканальному блоці пам'яті; суттєве збільшення обсягів пам'яті при зменшенні кроку дискретизації.

Відомий також пристрій для обробки нечіткої інформації, що реалізує спосіб одержання якісних експертних оцінок при моделюванні економічних, соціальних, біологічних систем [4]. Цей пристрій для обробки нечіткої інформації має у своєму складі задавальний елемент для введення експертних оцінок відповідного нечіткого параметра, виконаний у вигляді потенціометричного задатчика або задатчика з покажчиком, що має можливість переміщуватись і позиціонуватись між крайніми поділками на шкалі оцінок, багатоканальний блок пам'яті для введення і зберігання даних (min і max - границь числового відрізку [min max], на якому визначається значення нечіткого параметра x, а також n - цілого значення потенційної лінгвістичної потужності числового відрізку [min max], що характеризують нечітку інформацію у вигляді нечіткого числа, наприклад, А з трикутною формою функції належності), багатофункціональний обчислювальний блок та блок відображення обробленої інформації, вихід задавального елемента та перший, другий і третій виходи багатоканального блока пам'яті з'єднані відповідно з першим, другим, третім і четвертим входами багатофункціонального обчислювального блока, вихід якого підключений до входу блока відображення обробленої інформації. Такий пристрій має наступні недоліки: обмежені функціональні можливості, оскільки пристрій забезпечує формування відповідної до задавального сигналу нечіткої множини з трикутною формою функції належності, але не формує в автоматичному режимі ступінь приналежності будь-якого заданого компонента x, що є складовою носія нечіткої множини з трикутною формою функції належності; для реалізації компонентів пристрою з відповідними взаємозв'язками застосовується ПЕОМ, що ускладнює використання такого пристрою у складі вбудованих електронних систем, які широко використовуються в бортових обчислювальних комплексах різнотипного призначення.

Найближчим до запропонованого є пристрій для обробки нечіткої інформації [5]. Цей пристрій містить задавальний елемент для введення експертних оцінок відповідного нечіткого параметра, багатоканальний блок пам'яті для введення і зберігання даних, що характеризують нечітку інформацію у вигляді нечіткої множини з трикутною формою функції належності, багатофункціональний обчислювальний блок та блок відображення обробленої інформації.

Багатофункціональний обчислювальний блок виконаний у вигляді арифметико-логічного пристрою. Багатоканальний блок пам'яті містить сім суматорів, чотири керовані ключі, три порогові елементи, два елементи І, два блоки ділення, а також два елементи НІ. Перший прямий вхід першого суматора підключений до першого входу багатофункціонального обчислювального, блока і до інформаційних входів першого та другого керованих ключів, другий інвертований вхід - до першого виходу багатоканального блока пам'яті та до першого інвертованого входу четвертого суматора, а вихід - до першого входу (ділене) першого блока ділення і до входу першого порогового елемента. Вихід першого порогового елемента з'єднаний з першим входом першого елемента І та з керованим входом першого керованого ключа, вихід якого підключений до першого прямого входу другого суматора. Другий інвертований вхід другого суматора з'єднаний з другим виходом багатоканального блока пам'яті, з другим прямим входом четвертого суматора і з першим інвертованим входом п'ятого суматора, а вихід - з входом другого порогового елемента. Вихід другого порогового елемента з'єднаний з першим входом другого елемента І, з входом першого елемента НІ та з керованим входом другого керованого ключа. Вихід другого керованого ключа підключений до першого прямого входу третього суматора, другий інвертований вхід якого з'єднаний з третім виходом багатоканального блока пам'яті і з другим прямим входом п'ятого суматора, а вихід - з першим входом (ділене) другого блока ділення і з входом третього порогового елемента. Вихід третього порогового елемента з'єднаний через другий елемент НІ з другим входом другого елемента І, вихід якого підключений до керованого входу четвертого керованого ключа. Інформаційний вхід четвертого керованого ключа підключений до виходу другого блока ділення, а вихід - до другого інвертованого входу шостого суматора. Вихід шостого суматора з'єднаний з виходом багатофункціонального обчислювального блока, перший прямий вхід шостого суматора через третій керований ключ підключений до виходу першого елемента І, другий вхід якого підключений до виходу першого елемента НІ. Вихід п'ятого суматора з'єднаний з другим входам (подільник) другого блока ділення, а вихід четвертого суматора - з другим входом (подільник) першого блока ділення, вихід якого підключений до керованого входу третього керованого ключа. Цей пристрій має наступні недоліки: функція належності задана лише трикутної форми, велику складність та малу швидкодію.

Задачею винаходу є підвищення швидкодії способу, а також розширення функціональних можливостей пристрою на його основі (функція належності може бути довільної форми) і спрощення схеми пристрою.

Суть винаходу полягає в тому, що пристрій для обробки нечіткої інформації має у своєму складі задавальний елемент для введення експертних оцінок відповідного нечіткого параметра, виконаний у вигляді першого, другого і третього регістрів пам'яті, багатоканальний блок пам'яті для введення і зберігання даних, що характеризують нечітку інформацію у вигляді нечіткої множини з трикутною (або довільною іншою) формою функції належності, багатофункціональний обчислювальний блок, блок керування та блок, який використовує результати оброблення нечіткої інформації. Перший, другий і третій виходи даних та сигнал "запуск" блоку, який використовує результати оброблення нечіткої інформації, підключено до першого, другого, третього входів задавального елемента, а сигнал "запуск" підключено також до входу блока керування. Вихід "кінець обробки" блоку керування підключено до відповідного входу блока, який використовує результати оброблення нечіткої інформації, а виходи керування - до входів багатофункціонального обчислювального блока. Виходи задавального елемента підключені до входів багатофункціонального обчислювального блока, вихід якого підключено до входів блока, який використовує результати оброблення нечіткої інформації. Пропонований пристрій відрізняється тим, що багатофункціональний обчислювальний блок виконаний у вигляді арифметико-логічного пристрою, що містить перший, другий і третій пристрої порівняння кодів, обидва входи яких підключено відповідно до виходів задавального елемента та багатоканального блока пам'яті. Виходи багатоканального блока пам'яті підключені до інформаційних входів четвертого, п'ятого і шостого регістрів пам'яті, керуючі входи яких підключені до виходів першого, другого і третього пристроїв порівняння. Виходи регістрів пам'яті підключені до входів блока пошуку мінімального значення коду та інформаційних входів комутатора. Входи керування комутатора підключено до виходів блока пошуку мінімального значення коду. Вихід комутатора підключено до входу першого накопичувального суматора та першого входу перемножувала, другий вхід підключений до виходу сьомого регістра пам'яті та входів адреси багатоканального блоку пам'яті, а вихід - до входу другого накопичувального суматора, вихід якого підключено до першого входу подільника. Другий вхід подільника підключено до виходу першого накопичувального суматора, а вихід - до входу блока, який використовує результати оброблення нечіткої інформації. Причому перший вихід блока

керування підключено до керуючих входів першого, другого і третього пристроїв порівняння кодів, другий вихід - до керуючого входу сьомого регістра пам'яті. А інформаційний вхід сьомого регістра пам'яті підключено до виходу адреси блока керування. Третій вихід блока керування підключено до керуючих входів обох накопичувальних суматорів, а до виходу блока, який використовує результати оброблення нечіткої інформації, підключено керуючий вхід і вхід даних восьмого регістра. Вихід восьмого регістра підключено до адрес задання тих областей пам'яті багатоканального блоку пам'яті, де зберігаються значення функцій належності виходу, відповідних до кожного правила нечіткого висновку.

Для підвищення точності пошуку центра ваги фігури, який є висновком нечіткої системи, між виходом комутатора та першим входом перемножувача, ввімкненого по схемі квадратора, введено подільник на 2, між виходом перемножувача та входом другого накопичувального суматора введено послідовно з'єднані другий суматор і блок добування квадратного кореня. При цьому другий вхід другого суматора через квадратор підключено до виходу сьомого регістра пам'яті.

Блок керування пропонованим пристроєм містить послідовно з'єднані тригер, ключ, перший лічильник, другий лічильник і формувач імпульсів, вихід якого підключено до входу скидання згаданого тригера. На вхід встановлення цього тригера підключено сигнал "запуск" з виходу блока, який використовує результати обробки нечіткої інформації, а вихід підключено до виходу "кінець обробки" блока керування. До входу згаданого ключа підключено генератор тактових імпульсів. При цьому входи першого, другого і третього дешифраторів підключені до виходів першого лічильника таким чином, щоби отримати на їх виходах імпульси керування зсунуті в часі на тривалість спрацювання відповідних елементів схеми багатофункціонального обчислювального блока. Тому виходи цих дешифраторів підключені до першого, другого та третього виходів блока керування, які підключені до входів керування цих елементів схеми багатофункціонального обчислювального блока. Крім того, виходи другого лічильника підключені до виходу адреси блока керування, яка поступає на сьомий регістр багатофункціонального обчислювального блока.

Під час експлуатації швидкодія пропонованого пристрою принципово підвищується шляхом зменшення кількості операцій за рахунок виконання перших операцій способу Мамдані під час навчання пристрою, до його експлуатації. Крім того, пропонований пристрій має більш регулярну структуру, а тому краще за відомі пристрої реалізується на програмованих логічних матрицях, внутрішні логічні елементи яких мають значно вищу швидкодію за окремі логічні елементи. Функціональні можливості пристрою розширено за рахунок того, що функції належності можуть бути довільної форми, а також можуть змінюватися згідно результатів навчання комп'ютерної системи. Спрощення схеми пристрою досягається зменшенням кількості елементів, необхідних для виконання тих функцій, які реалізує найближчий аналог (слід визнати, що найближчий аналог не проводить останню операцію - дефазифікацію результатів оброблення нечіткої інформації, тобто не знаходить координату центру ваги остаточної фігури, який і є висновком нечіткої системи).

Робота пристрою оброблення нечіткої інформації пояснюється фіг. 1-5. На фіг. 1 представлено структурну схему пропонованого пристрою, який визначає центр ваги за спрощеною схемою, яка має знижену точність (їй притаманна методична похибка). Фіг. 2 ілюструє принцип роботи схеми фіг. 1 під час визначення центра ваги. На фіг. 3 представлено структурну схему пропонованого пристрою, який визначає центр ваги за схемою, яка має високу точність (методична похибка їй не притаманна). Фіг. 4 ілюструє принцип роботи схеми фіг. 3 під час визначення центра ваги. На фіг. 5 представлено структурну схему блока керування, що входить до складу схеми фіг. 1.

Представлена на фіг. 1 структурна схема пропонованого пристрою, який визначає центр ваги за спрощеною схемою, складається з задавального елемента (ЗЕ) для введення експертних оцінок відповідного нечіткого параметра, виконаного у вигляді першого (РГ1), другого (РГ2) і третього (РГ3) регістрів пам'яті, багатоканального блока пам'яті (ББП) для введення і зберігання даних, виконаного у вигляді першого (ПЗП1), другого (ПЗП2) і третього (ПЗП3) постійних запам'ятовуючих пристроїв (можна використати Flash-пам'ять, яка перезаписується після етапу навчання, або оперативну пам'ять), блоку керування (БК), блоку, який використовує результати оброблення нечіткої інформації (БВ), та багатофункціонального обчислювального блока (БОБ). БОБ в свою чергу складається з першого (ППК1), другого (ППК2) і третього (ППК3) пристроїв порівняння кодів, четвертого (РГ4), п'ятого (РГ5), і шостого (РГ6) регістрів пам'яті, блока пошуку мінімального значення коду Мін і керованого ним комутатора (КМ), перемножувача (Х1), першого (СМ1) і другого (СМ2) накопичувальних суматорів і подільника ПОДІЛЬНИК. В склад пристрою також входять сьомий (РГ7) і восьмий (РГ8) регістри.

Роботу пристрою розглянемо на прикладі багатоканальної обробки нечіткої інформації для знаходження методу модулярного експоненціювання відповідно до заданих значень продуктивності системи захисту інформації (яку реалізує блок БВ, який використовує результати оброблення нечіткої інформації), стійкості цієї системи захисту інформації до часового аналізу та допустимих затрат пам'яті системи на реалізацію алгоритмів захисту інформації.

В процесі навчання пристрою для обробки нечіткої інформації у визначені області ПЗП1 … ПЗП3 записуються функції належності виходу для кожного з правил. Для цього, згідно механізму нечіткого висновку Мамдані, порівнюють вхідні дані зі значеннями функцій належності входів, знаходять найменше значення функцій належності входів щодо кожного з входів, які відповідають базі правил і таким чином знаходять відповідні значення функцій належності виходу, згідно яких під час експлуатації будемо відсікати необхідні області функцій належності виходу.

В процесі експлуатації пристрою для обробки нечіткої інформації блок БВ, який використовує результати обробленню (Нечіткої інформації, формуючи сигнал "запуск", записує у перший РГ1, другий РГ2 і третій РГ3 регістри пам'яті значення продуктивності, стійкості та допустимих затрат пам'яті відповідно. Ці значення є результатами попередньої обробки, яка проведена під час згаданого етапу навчання пристрою. Сигнал "запуск" запускає також блок керування БК. Крім того, в регістр РГ8 записується адреса (старші розряди адреси) області ПЗП1 … ПЗП3, яка відповідає даному каналу (визначає характерні для даного каналу функції належності виходу).

Блок керування БК працює циклічно. На початку кожного циклу БК своїм сигналом К1 записує в регістр РГ7 початкову адресу області ПЗП1 … ПЗП3 (молодші розряди адреси, які визначають абсцису функцій належності виходу, значення яких записано в тій області ПЗП1 … ПЗП3, яка визначається старшими розрядами адреси). На вихід ПЗП1 … ПЗП3 надходять коди значень функцій належності вихрду, які відповідають записаній в РГ7 адресі. Їх значення порівнюються (з допомогою пристроїв порівняння кодів ППК1 … ППК3) зі значеннями значення продуктивності, стійкості та допустимих затрат пам'яті, записаними в РГ1 … РГ3. Якщо якісь із значень, що надходять з РГ1 … РГ3, більші за відповідні значення, що надходять з ПЗП1 … ПЗП3, то останні записуються у регістри РГ4 … РГ6. Якщо якісь із значень, що надходять з РГ1 … РГ3, менші за відповідні значення, що надходять з ПЗП1 … ПЗП3, то запис у регістри РГ4 … РГ6 не проводиться, в них залишаються значення, які були не більші за значення, що надходять з РГ1 … РГ3. Запис в регістри РГ4 … РГ6 проводиться згідно керуючого сигналу К2, який дозволяє роботу ППК1 … ППК3. В результаті на виходах РГ4 … РГ6 маємо відсічені по осі ординат функції належності виходу.

Далі блок пошуку мінімального значення коду Мін знаходить серед значень відсічених функцій належності виходу, які знаходяться в регістрах РГ4 … РГ6, ті, що мають мінімальну амплітуду. Відповідно до знайденого мінімуму блок Мін вмикає відповідний канал комутатора КМ і отримане мінімальне значення надходить на подальшу обробку. На цьому закінчується один цикл роботи пристрою. Наступні цикли відрізняються лише зміною адреси, яка записується в регістр РГ7.

Подальша обробка нечіткої інформації полягає у знаходженні абсциси центра ваги фігури, отриманої шляхом перебору всіх адрес в регістрі РГ7 (опитування всієї області, яка відповідає правилам згідно механізму нечіткого висновку Мамдані).

Процес спрощеного пошуку центра ваги фігури, яка збудована в результаті перебору всіх адрес в регістрі РГ7, зображено на фіг. 2. Він ведеться на базі формули [6]:

$$r_{цв} = \frac{\sum r_i m_i}{\sum m_i}, \qquad (1)$$

де $r_{цв}$ - координата центра ваги; r_i - координата центра ваги і-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти; m_i - маса і-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти.

Для реалізації пошуку абсциси центра ваги $r_{цв}$ перемножувач Х1 обчислює чисельник формули (1) шляхом перемноження адреси, записаної в регістрі РГ7 (умовне значення абсциси центра ваги і-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти) на значення функції належності виходу (умовне значення маси і-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти). Значення адреси, записаної в регістрі РГ7, та функції належності виходу є умовними в тому сенсі, що вони відображають розміри отриманої фігури з відповідним масштабом.

Накопичувальні суматори СМ1 і СМ2 проводять сумування отриманих значень чисельника і знаменника (1), а подільник знаходить частку, яка відповідає умовній абсцисі центра ваги.

Синхронізація роботи суматорів СМ1 і СМ2 здійснюється сигналом К3 блока керування БК. Цей сигнал повинен бути затриманим відносно сигналу К2 на час, який визначається затримкою блоків Мін, КМ і Х1.

Після перебору всіх адрес, які записуються в регістр РГ7, блок керування БК формує сигнал "кінець обробки", який надходить на блок БВ. Блок БВ зчитує з виходу подільника приблизне значення абсциси центра ваги фігури, отриманої в результаті нечіткої обробки. Отримане значення є приблизним тому, що координата r_i центра ваги і-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти, не враховує висоти і-того прямокутника, тобто значення функції належності виходу.

Для підвищення точності визначення координат центра ваги отриманої фігури за рахунок врахування висоти і-тих прямокутників пропонується замість перемножувача Х1 (див. фіг. 1) ввімкнути схему, представлену на фіг. 3. Ця схема складається з подільника на два 1/2, перемножувача Х1 (ввімкненого по схемі квадратора, для чого на обидва входи надходить той самий код), суматора СМ3, блоку добування квадратного кореня БДКК, а також перемножувача Х2 (теж ввімкненого по схемі квадратора, для чого на обидва входи надходить той самий код). Вона реалізує обчислення векторів r_i за теоремою Піфагора. Для цього перемножувачі Х1, Х2 та суматор СМ3 знаходять суму квадратів катетів (див. фіг. 4), а блок БДКК знаходить дійсне значення довжини вектора r_i центра ваги і-того прямокутника. Далі робота пристрою не відрізняється від роботи схеми, представленої на фіг. 1.

Блоки перемножувачів Х1 та Х2, добування квадратного кореня БДКК, а також ПОДІЛЬНИК можна реалізувати на основі постійних запам'ятовуючих пристроїв. При цьому на входи адреси подають вхідні коди, а в комірках постійних запам'ятовуючих пристроїв записують коди, що відповідають дійсним результатам виконання відповідних арифметичних дій. Така реалізація перелічених вище блоків дозволяє отримати їх максимальну швидкодію під час експлуатації, бо всі необхідні обчислення проведені ще на етапі створення пристрою. Крім того, ділення на два (блок 1/2) можна виконати просто зсуваючи входи перемножувача Х1 на один розряд вправо (в сторону менших розрядів).

Структурна схема блоку керування БК представлена на фіг. 5. Вона складається з тригера Тг, генератора тактових імпульсів Ген., ключа Кл, лічильників Ліч.1 та Ліч.2 та формувачів Ф1 і Ф2. До виходів лічильника Ліч. 1 підключені входи трьох дешифраторів, які формують сигнали керування К1, К2, К3 (див. фіг 1). У початковому стані тригер Тг знаходиться в такому стані, що ключ Кл запертий і не пропускає на вхід лічильника Ліч. 1 тактових імпульсів з генератора Ген. Після приходу імпульсу запуску перекидається тригер Тг. При цьому фронт його вихідного імпульсу, виділений формувачем Ф2, скидає в нуль лічильники Ліч.1 та Ліч.2. Одночасно на ключ Кл надходить дозвіл на проходження тактових імпульсів генератора Ген. на вхід лічильника Ліч.1. Крім того, вихід тригера Тг знімає сигнал "кінець обробки". Це означає, що пристрій обробки нечіткої інформації власне зайнятий її обробкою.

Лічильник (Ліч.1) керує роботою багатофункціонального обчислювального блока БОБ. Для цього він формує імпульсні сигнали керування К1, К2, К3. Дешифратори дозволяють таким чином розподілити в часі сигнали керування К1, К2, К3, що інтервал між К1 і К2 відповідає сумарному часу запису адреси в регістр РГ7 та вибірки значень, записаних в ПЗП1 … ПЗП3. Інтервал між К2 і К3 значно довший, він повинен відповідати часу обробки даних (точніше - проходження даних) від регістрів РГ4 … РГ6 до накопичувальних суматорів СМ1 і СМ2. Формування К1, К2, К3 з допомогою дешифраторів дозволяє отримати відповідні інтервали та їх змінювати під час налагодження пристрою. Сумарний період роботи лічильника Ліч.1 задає один цикл роботи БОБ. Цей період повинен відповідати сумарній затримці всіх блоків, які входять в БОБ.

Лічильник (Ліч.2) формує адреси Адр. опитування ПЗП1 … ПЗП3, в яких розміщено значення ординат функцій належності виходу для всіх відповідних областей багатоканального блока пам'ять Кількість станів Ліч.2 повинна відповідати максимальному об'єму ПЗП1 … ПЗП3. Період роботи Ліч.2 відповідає добутку тривалості один цикл роботи БОБ на максимальний об'єм ПЗП1 … ПЗП3. Після закінчення перебору всіх адрес Адр. формувач Ф1 скидає тригер Тг в початковий стан. Тг закриває ключ Кл і, тим самим, забороняє проходження імпульсів генератора Ген. на лічильники. Також Тг встановлює вихідний сигнал "кінець обробки", сигналізуючи БВ про закінчення обробки нечіткої інформації.

Пропонований спосіб обробки нечіткої інформації та пристрій для його реалізації можуть бути використані в банківській системі при здійсненні, наприклад, інтернет-банкінгу через комп'ютерну мережу. При цьому до сервера комп'ютерної системи банку надходять запити від користувачів, які ідентифікуються своїми IP-адресами.

Неможливо чітко визначити чи здійснюється атака зловмисника (зокрема, часова атака, яка є пасивною і її неможливо виявити) на канал передачі даних кожного з користувачів. Проте існують користувачі, які мають позитивний стаж (з точки зору захисту від часової атаки) користування мережею банку. Таким чином, кожній IP-адресі клієнта банку відповідає свій рівень ймовірності ризику виникнення атаки (тобто значення стійкості до часової атаки). Крім того, під час опрацювання інформації сервером необхідно врахувати необхідний рівень продуктивності системи захисту інформації та можливі затрати пам'яті (необхідно забезпечити прийнятний компроміс між часом обслуговування клієнтів та ресурсами системи, які використовуються для захисту системи).

На сучасному етапі для захисту інформації використовуються, як правило, асиметричні криптоалгоритми, основною операцією в яких є модулярне експоненціювання. Вибір методу модулярного експоненціювання залежно від значень продуктивності, стійкості до часового аналізу та допустимих затрат пам'яті в описаних умовах невизначеності може реалізовуватись запропонованим пристроєм обробки нечіткої інформації. Це дозволить реконфігурувати систему захисту інформації банку в кожному конкретному випадку здійснення запиту клієнтами, що підвищить захищеність системи в цілому та правильність розподілу доступу користувачів. При цьому підвищена продуктивність пропонованого способу забезпечить менший час доступу для клієнта.

Перевагою апаратної реалізації є те, що зловмисник, шляхом впровадження відповідної програми у виконуваний комп'ютерною системою комплекс програм, може порушувати роботу системи захисту інформації таким чином, що це порушення важко виявити (наприклад, встановлює однаковий для всіх випадків крипто алгоритм з відомими зловмиснику хоча би деякими параметрами, що значно полегшує його злам). Заборонити порушення роботи апаратного пристрою програмним чином значно легше, наприклад, вводячи механічне вимикання доступу до задання параметрів системи захисту (в нашому випадку відключивши вихід регістра РГ8 від входу ББП або хоча би заблокувавши механічно сигнал запису в регістр РГ8).

Джерела інформації:

1. Рогозин О.В. Метод нечеткого вивода решения в задаче подбора программного обеспечения на основе качественных характеристик этого обеспечения как объекта инвестиций. //Качество Инновации Образование. - 2009. - №3.

2. Ротштейн А.П., Штовба С.Д. "Нечёткая надёжность алгоритмических процессов". - Винница: Континент - ПРИМ., - 1997. - 142 с.

3. Патент України № 22731 Пристрій для обробки нечіткої інформації. МПК G06F 15/00, G06F 7/06 / А.А. Рідкокаша, К.К. Голдер, М.М. Рахман. - опубл. 07.04.1998, бюл. № 3.

4. Патент України № 44595 Пристрій для обробки нечіткої інформації. МПК G06F 17/00/ В.Ю. Кондратенко, Ю.П. Кондратенко. - опубл. 12.10.2009, бюл. № 19.

5. Патент України № 71851 Спосіб одержання якісних експертних оцінок при моделюванні економічних, соціальних, біологічних систем. МПК G06Q 99/00, G06N 7/00/ Л.О. Коршевнюк, Д.О. Коршевнюк, М.Ю. Мінін. - опубл. 15.12.2004, бюл. № 12.

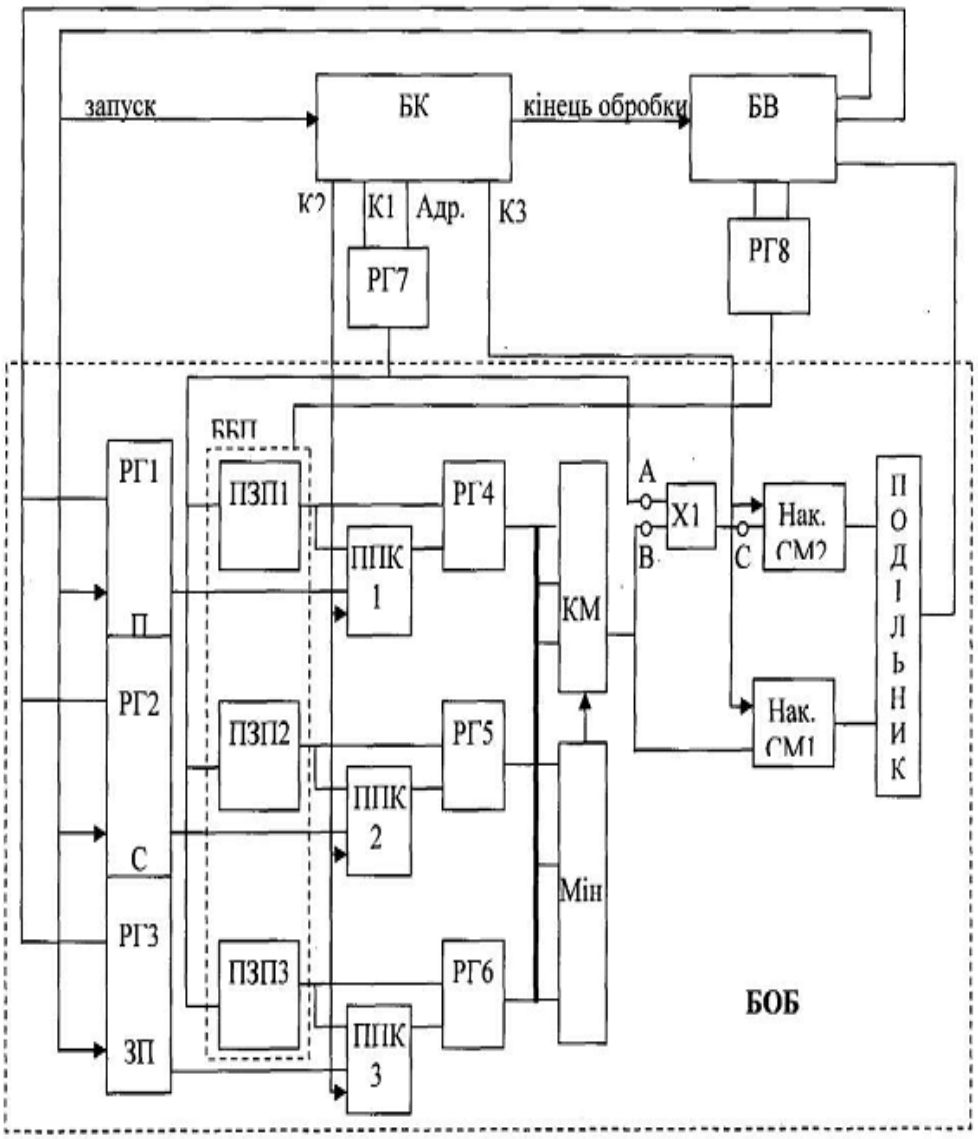
6. Яворский Б.М., Детлаф А.А. Физика для школьников старших классов и поступающих в вузы, - М.: Академия, 2008. - 720 с.

ФОРМУЛА ВИНАХОДУ

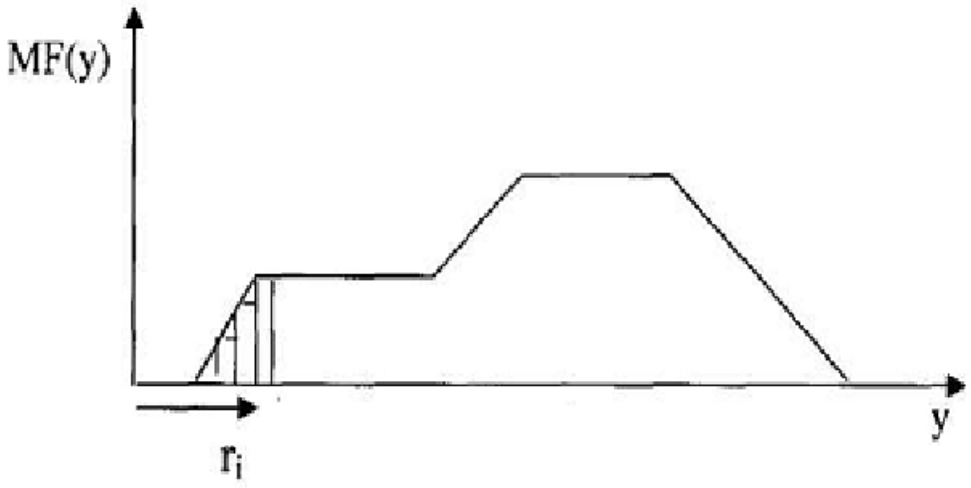
1. Пристрій для обробки нечіткої інформації, що складається із задавального елемента для введення експертних оцінок відповідного нечіткого параметра, виконаного у вигляді першого, другого і третього регістрів пам'яті, багатоканального блока пам'яті для введення і зберігання даних, що характеризують нечітку інформацію у вигляді нечіткої множини з трикутною або іншою формою функції належності, багатофункціонального обчислювального блока, блока керування та блока, який використовує результати оброблення нечіткої інформації, перший, другий і третій виходи даних та сигнал "запуск" якого підключено до першого, другого, третього входів задавального елемента, сигнал "запуск" підключено також до входу блока керування, вихід "кінець обробки" якого підключено до відповідного входу блока, який використовує результати оброблення нечіткої інформації, а виходи керування - до входів багатофункціонального обчислювального блока, причому виходи задавального елемента підключені до входів багатофункціонального обчислювального блока, вихід якого підключено до входів блока, який використовує результати оброблення нечіткої інформації, який **відрізняється** тим, що багатофункціональний обчислювальний блок виконаний у вигляді арифметико-логічного пристрою, що містить перший, другий і третій пристрої порівняння кодів,

обидва входи яких підключено відповідно до виходів задавального елемента та багатоканального блока пам'яті, виходи якого підключені також до інформаційних входів четвертого, п'ятого і шостого регістрів пам'яті, керуючі входи яких підключені до виходів першого, другого і третього пристроїв порівняння кодів, а виходи - до входів блока пошуку мінімального значення коду і керованого ним комутатора, вихід якого підключено до входу першого накопичувального суматора та першого входу перемножувача, другий вхід якого підключений до виходу сьомого регістра пам'яті та входів адреси багатоканального блоку пам'яті, а вихід - до входу другого накопичувального суматора, вихід якого підключено до першого входу подільника, другий вхід якого підключено до виходу першого накопичувального суматора, а вихід - до входу блока, який використовує результати оброблення нечіткої інформації, причому перший вихід блока керування підключено до керуючих входів першого, другого і третього пристроїв порівняння кодів, другий вихід блока керування підключено до керуючого входу сьомого регістра пам'яті, інформаційний вхід якого підключено до виходу адреси блока керування, третій вихід блока керування підключено до керуючих входів обох накопичувальних суматорів, а до виходу блока, який використовує результати оброблення нечіткої інформації, підключено керуючий вхід і вхід даних восьмого регістра, вихід якого підключено до входів адрес задання тих області пам'яті багатоканального блоку пам'яті, де зберігаються значення функцій належності виходу, відповідних до кожного правила нечіткого висновку.

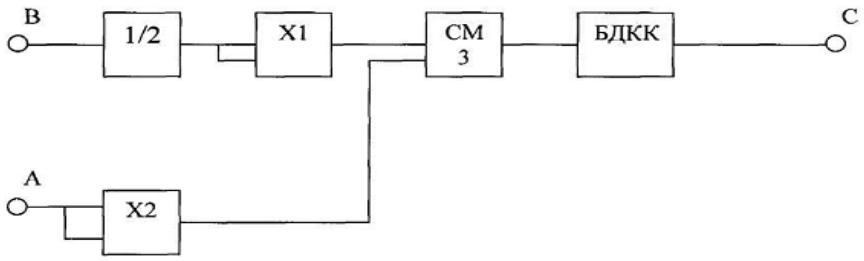
2. Пристрій для обробки нечіткої інформації за п. 1, який **відрізняється** тим, що між виходом комутатора та першим входом перемножувача, ввімкненого по схемі квадратора, введено подільник на 2, між виходом перемножувача та входом другого накопичувального суматора введено послідовно з'єднані другий суматор і блок добування квадратного кореня, причому другий вхід другого суматора через квадратор підключено до виходу сьомого регістра пам'яті.


запуск
БК
кінець обробки
БВ
К2
К1
Адр.
К3
РГ7
РГ8
ББП
РГ1
П
РГ2
С
РГ3
ЗП
ПЗП1
ПЗП2
ПЗП3
ППК 1
ППК 2
ППК 3
РГ4
РГ5
РГ6
КМ
Мін
А
В
Х1
С
Нак. СМ2
Нак. СМ1
ПОДІЛЬНИК
БОБ

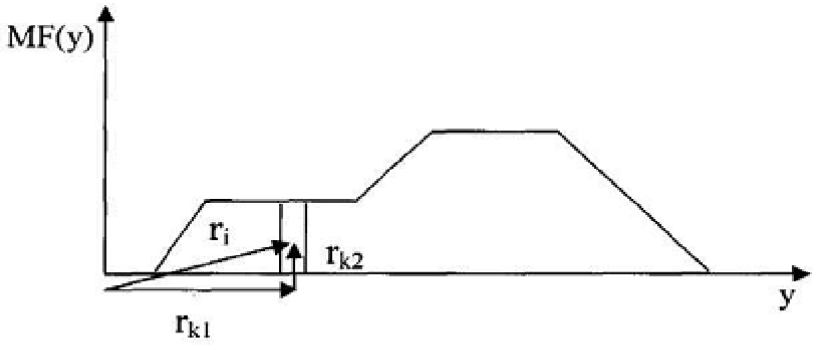
Фіг. 1


MF(y)
y
r_i

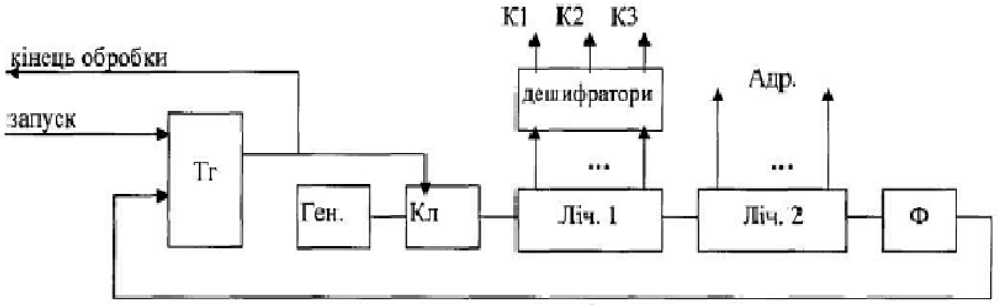
Фіг. 2



Фіг. 3



Фіг. 4



Фіг. 5

Комп'ютерна верстка С. Чулій

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601